



SAMSUNG TECHWIN

SAMSUNG PoE Switch SPN-12080P / SPN-14240P

USER MANUAL



REV. 2.00
Nov 2014

SAMSUNGTECHWIN.CO.,LTD

Table of Contents

Table of Contents	i
About This Guide.....	1
Terms/Usage.....	1
Copyright and Trademarks	1
1 Product Introduction	2
SPN-12080P	3
Front Panel.....	3
Rear Panel.....	3
SPN-14240P	4
Front Panel.....	4
Rear Panel.....	4
2 Hardware Installation	5
Step 1: Unpacking.....	5
Step 2: Switch Installation.....	5
Desktop or Shelf Installation.....	5
Rack Installation	5
Step 3 – Plugging in the AC Power Cord.....	6
Power Failure	7
3 Getting Started.....	8
Management Options.....	8
Using Web-based Management	8
Supported Web Browsers	8
Connecting to the Switch.....	8
Login Web-based Management	8
Smart Wizard	9
Web-based Management.....	9
4 Configuration	10
Smart Wizard Configuration	10
IP Information	10
Password.....	10
SNMP	11
Web-based Management.....	12
Tool Bar > Save Menu	13
Save Configuration	13
Save Log	13
Tool Bar > Tool Menu	13
Reset	13
Reset System	13
Reboot Device	13
Configuration Backup and Restore	14
Firmware Backup and Upgrade.....	14
Tool Bar > Smart Wizard.....	15
Function Tree	16
Device Information.....	16
System > System Settings	17
System > IPv6 System Settings	18
System > IPv6 Route Settings	18

System > IPv6 Neighbor Settings	19
System > Password.....	19
System > Port Settings.....	20
System > DHCP Auto Configuration	20
System > SysLog Host.....	21
System > Time Profile	21
System > Power Saving	22
System > IEEE802.3az EEE Settings	22
VLAN > 802.1Q VLAN.....	23
VLAN > 802.1Q VLAN PVID	24
VLAN > 802.1Q Management VLAN.....	24
VLAN > Voice VLAN > Voice VLAN Global Settings	24
VLAN > Voice VLAN > Voice VLAN Port Settings	26
VLAN > Voice VLAN > Voice Device List.....	26
VLAN > Auto Surveillance VLAN Settings	26
L2 Functions > Jumbo Frame	27
L2 Functions > Port Mirroring	28
L2 Functions > Loopback Detection.....	28
L2 Functions > MAC Address Table > Static MAC	29
L2 Functions > MAC Address Table > Dynamic Forwarding Table	29
L2 Functions > Spanning Tree > STP Global Settings	29
L2 Functions > Spanning Tree > STP Port Settings	31
L2 Functions > Link Aggregation > Port Trunking.....	32
L2 Functions > Link Aggregation > LACP Port Settings	32
L2 Functions > Multicast > IGMP Snooping	33
L2 Functions > Multicast > Multicast Forwarding.....	34
L2 Functions > Multicast > Multicast Filtering Mode	35
L2 Functions > SNTP > Time Settings	35
L2 Functions > SNTP > TimeZone Settings.....	36
L2 Functions > LLDP > LLDP Global Settings	37
L2 Functions > LLDP > LLDP MED Settings	37
L2 Functions > LLDP > LLDP Port Settings.....	38
L2 Functions > LLDP > 802.1 Extension TLV	39
L2 Functions > LLDP > 802.3 Extension TLV	39
L2 Functions > LLDP > LLDP Management Address Settings	40
L2 Functions > LLDP > LLDP Management Address Table	40
L2 Functions > LLDP > LLDP Local Port Table	41
L2 Functions > LLDP > LLDP Remote Port Table	42
L2 Functions > LLDP > LLDP Statistics	43
QoS > Bandwidth Control.....	44
QoS > 802.1p/DSCP/ToS.....	45
QoS > IPv6 Traffic Class Priority Settings.....	46
QoS > TCP/UDP Port Priority Settings	46
Security > Trusted Host.....	46
Security > Port Security.....	47
Security > Traffic Segmentation	47
Security > Safeguard Engine.....	48
Security > Storm Control	48
Security > ARP Spoofing Prevention	48

Security > DHCP Server Screening	49
Security > SSL Settings.....	49
Security > Smart Binding > Smart Binding Settings.....	50
Security > Smart Binding > Smart Binding	51
Security > Smart Binding > White List.....	51
Security > Smart Binding > Black List	52
AAA > 802.1X > 802.1X Settings	52
ACL > ACL Wizard	54
ACL > ACL Profile List.....	55
ACL > ACL Finder	66
PoE > PoE Global Settings (SPN-12080P/28P only).....	66
PoE > PoE Port Settings (SPN-12080P/28P only)	67
SNMP > Trap to SmartConsole Utility	68
SNMP > SNMP > SNMP Global Settings	69
SNMP > SNMP > SNMP User	69
SNMP > SNMP > SNMP Group Table	70
SNMP > SNMP > SNMP View	71
SNMP > SNMP > SNMP Community.....	71
SNMP > SNMP > SNMP Host.....	72
SNMP > SNMP > SNMP Engine ID	72
SNMP > RMON > RMON Global Settings	72
SNMP > RMON > RMON Statistics	72
SNMP > RMON > RMON History.....	73
SNMP > RMON > RMON Alarm Settings	73
SNMP > RMON > RMON Event.....	74
Monitoring > Port Statistics.....	74
Monitoring > Cable Diagnostics	75
Monitoring > System Log.....	76
6 Command Line Interface.....	77
To connect a switch via TELNET:.....	77
Logging on to the Command Line Interface:.....	77
CLI Commands:	77
?	78
download	78
upload	79
config ipif system	80
config ipif system	81
logout.....	81
ping	81
ping6.....	82
reboot	82
reset config	83
show ipif.....	83
show switch	84
config account admin password	84
save	85
debug info.....	85
Appendix A - Ethernet Technology.....	87
Gigabit Ethernet Technology	87

Fast Ethernet Technology	87
Switching Technology	87
Appendix B - Technical Specifications	88
Hardware Specifications	88
Key Components / Performance	88
Port Functions	88
Physical & Environment	88
Emission (EMI) Certifications	88
Safety Certifications	88
Features	88
L2 Features	88
VLAN	88
QoS (Quality of Service)	88
Security	89
OAM	89
Management	89
Green Technology	89
Appendix C – Rack mount Instructions	90

About This Guide

This guide provides instructions to install the SAMSUNG PoE Switch SPN-12080P/SPN-14240P, how to configure Web-based Management step-by-step.



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

This guide is mainly divided into four 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 PoE 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 SAMSUNG TECHWIN CO., LTD. All rights reserved.

Reproduction in any manner whatsoever without the written permission of SAMSUNG TECHWIN CO., LTD. is strictly forbidden.

Trademarks used in this text: SAMSUNG and the SAMSUNG logo are trademarks of SAMSUNG TECHWIN CO., LTD.; 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. SAMSUNG TECHWIN CO., LTD. disclaims any proprietary interest in trademarks and trade names other than its own.

1 Product Introduction

Thank you and congratulations on your purchase of SAMSUNG PoE Switch Products.

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

Flexible Port Configurations. The SPN-12080P and SPN-14240P are the new generation of PoE Switches. These series offer 2 PoE models with 8 10/100/1000Mbps PoE ports plus 2 SFP ports and 24 10/100/1000Mbps PoE ports plus 4 SFP ports.

The first 4 ports of SPN-14240P also support up to 30 watts PoE power for the connections of PoE + Power Devices, allowing them to be deployed at difficult places such as on high walls and ceilings, where AC power outlets are not readily available.

Green Technology. Green devices are about providing eco-friendly alternatives without compromising performance. Green Technology includes a number of innovations to reduce energy consumption on SPN-12080P and SPN-14240P such as shutting down a port, or turning off some LED indicators, or adjusting the power usage according to the Ethernet cable connected to it. For PoE model such as SPN-12080P and SPN-14240P, Green Technology offers Time-based PoE feature to shut down per port power off working hours.

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

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

Network Security. Safeguard Engine function protects the switches against traffic flooding caused by virus attacks. Additional features like 802.1X port-based authentication provide access control of the network with external RADIUS servers. ACL is a powerful tool to screen unwanted IP or MAC traffic. Storm Control can help to keep the network from being overwhelmed by abnormal traffic. Port Security is another simple but useful authentication method to maintain the network device integrity.

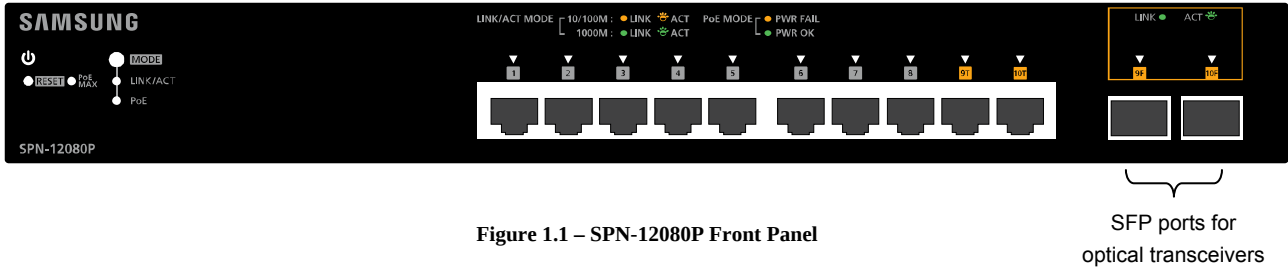
Versatile Management. The new generation of SAMSUNG PoE Switches provides growing businesses with a simple and easy management of their network, using a Web-Based management interface that allows administrators to remotely control their network down to the port level.

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

In addition, users can utilize the SNMP MIB (*Management Information Base*) to poll the switches for information about the status, or send out traps of abnormal events. SNMP support allows users to integrate the switches with other third-party devices for management in an SNMP-enabled environment.

SPN-12080P

8-Port 10/100/1000Mbps plus 2 combo ports of 1000Base-T/SFP ports Web Smart PoE Switch.

Front Panel

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

PoE Max: The PoE 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 78 Watts.

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

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

Port Link/Act/Speed LED (1-8, 9T, 10T 9F, 10F): When mode LED lights up in Link/Act mode, the port LEDs indicate a network link through the corresponding port. Blinking indicates the Switch is either sending or receiving data to the port. When the port LED glows in amber, it indicates the port is running on 10M or 100M. When the port LED glows in green, it is running on 1000Mbps.



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



CAUTION: The ITE is to be connected only to PoE networks without routing to the outside plant.

Port PoE LED (1-8): When mode LED lights up in PoE mode, the port LEDs indicate powering status over the corresponding port. SPN-12080P can supply up to 30W on port 1- 4, which are marked with black background color on front panel, for IEEE802.3at compliance PDs.

Rear Panel

Figure 1.2 – SPN-12080P Rear Panel

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

SPN-14240P

24-Port 10/100/1000Mbps plus 4 SFP ports Web Smart PoE Switch.

Front Panel

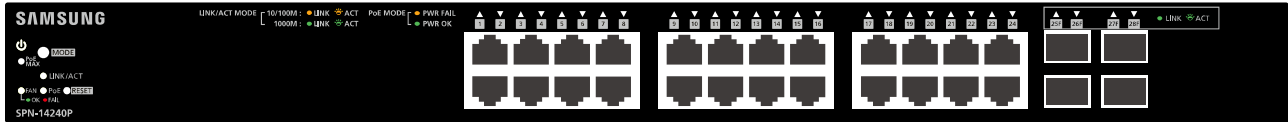


Figure 2.7 – SPN-14240P Front Panel

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

PoE Max: The PoE 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 185 Watts.

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

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

Port Link/Act/Speed LED (1-24, 25F, 26F, 27F, 28F): When mode LED lights up in Link/Act mode, the port LEDs indicate a network link through the corresponding port. Blinking indicates the Switch is either sending or receiving data to the port. When the port LED glows in amber, it indicates the port is running on 10M or 100M. When the port LED glows in green, it is running on 1000Mbps.

Fan: The Fan LED lights green when fans work well, and lights red when fans fail.



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



CAUTION: The ITE is to be connected only to PoE networks without routing to the outside plant.

Port PoE LED (1-24): When mode LED lights up in PoE mode, the port LEDs indicate powering status over the corresponding port. SPN-14240P can supply up to 30W on port 1- 4, which are marked with black background color on front panel, for IEEE802.3at compliance PDs.

Rear Panel



Figure 1.8 – SPN-14240P Rear Panel

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

2 Hardware Installation

This chapter provides unpacking and installation information for the SAMSUNG PoE Switch.

Step 1: Unpacking

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

- One SAMSUNG PoE Switch
- One AC power cord
- Four rubber feet
- Screws and two mounting brackets
- One Multi-lingual Getting Started Guide
- One CD with User Manual

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.

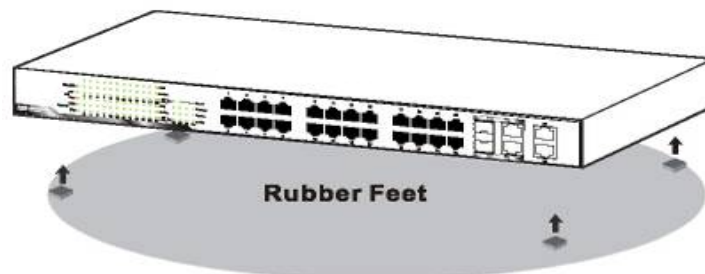


Figure 2.1 – Attach the adhesive rubber pads to the bottom

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).

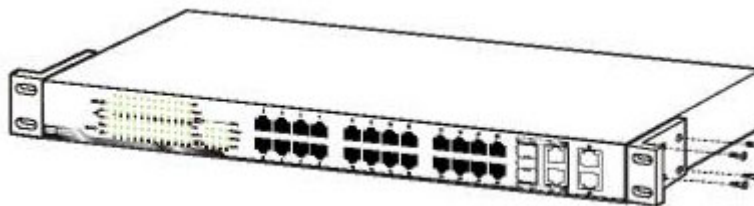


Figure 2.2 – Attach the mounting brackets to the Switch

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

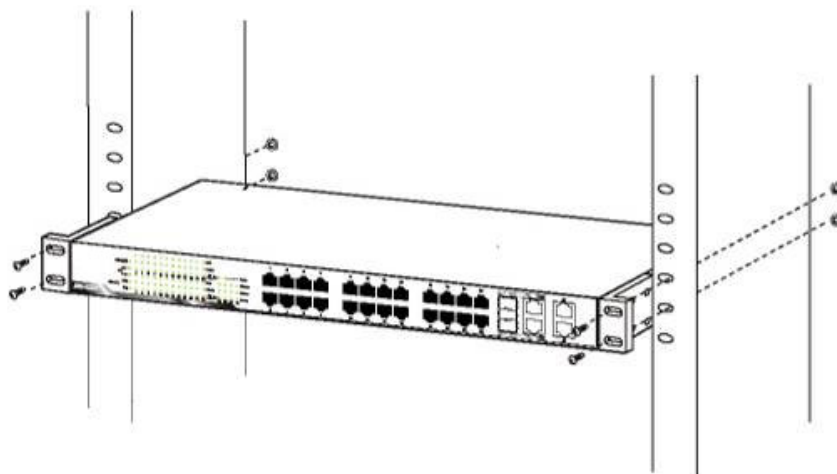


Figure 2.3 – Mount the Switch in the rack or chassis

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

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

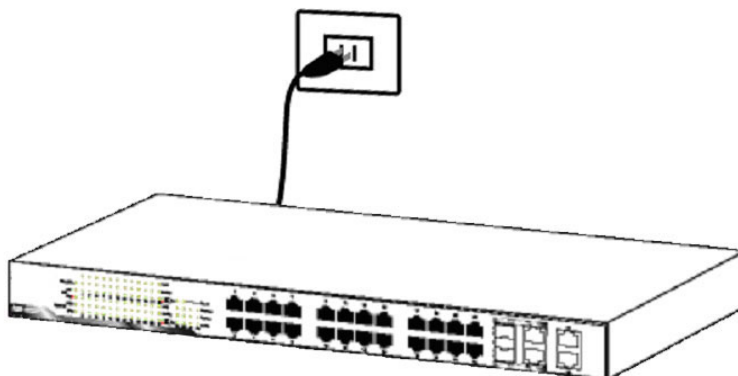


Figure 2.4 –Plugging the switch into an outlet

Power Failure

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

3 Getting Started

This chapter introduces the management interface of SAMSUNG PoE Switch.

Management Options

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

Each switch must be assigned its own IP Address, which is used for communication with the Web-Based Management or a SNMP network manager. The PC should have an IP address in the same range as the switch. Each switch can allow up to four users to access the Web-Based Management concurrently.

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

Using Web-based Management

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

Supported Web Browsers

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

- Internet Explorer 6 or later version
- Netscape 8 or later version
- Firefox 3.0 or later version
- Chrome 5.0 or later version
- Safari 4.0 or later version
- Opera 10 or later version

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.

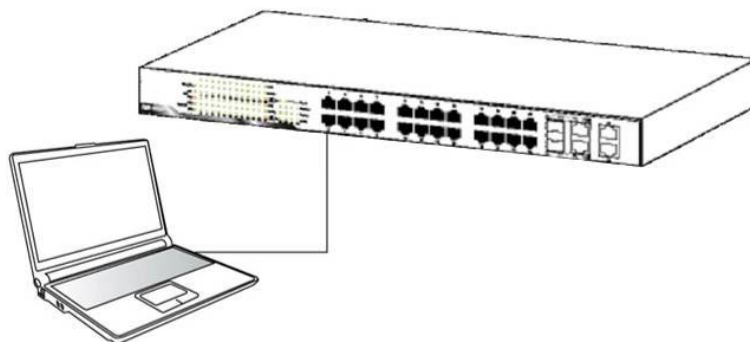


Figure 3.1 – Connected Ethernet cable

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

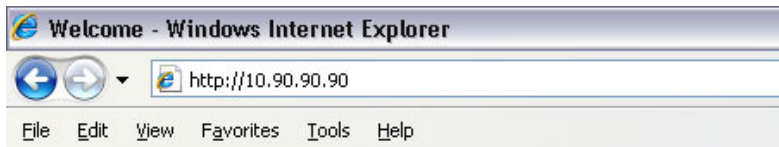


Figure 3.2 –Enter the IP address 10.90.90.90 in the web browser



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

Smart Wizard

After a successful login, the Smart Wizard will guide you through essential settings of the SAMSUNG PoE Switch. Please refer to the Smart Wizard Configuration section for details.

Web-based Management

By clicking the **Exit** button in the Smart Wizard, you will enter the Web-based Management interface. Please refer to Chapter 5 [Configuration](#) for detailed instructions.

4 Configuration

The features and functions of the SAMSUNG PoE 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 SAMSUNG PoE 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.

Figure 5.1 – IP Information in Smart Wizard



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

Password

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.

Welcome to Smart Wizard

Step 2 of 3: Set up the password for authorized access.

Password

Password:
Confirm Password:
.....

☐ Ignore the wizard next time

Exit Back Next

Figure 5.2 – Password in Smart Wizard

SNMP

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.

Welcome to Smart Wizard

Step 3 of 3: Enable SNMP for management.

SNMP

SNMP: ☐ Enabled ☒ Disabled

☐ Ignore the wizard next time

Exit Back Next Apply

Figure 5.3 – SNMP in Smart Wizard



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

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

Web-based Management

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

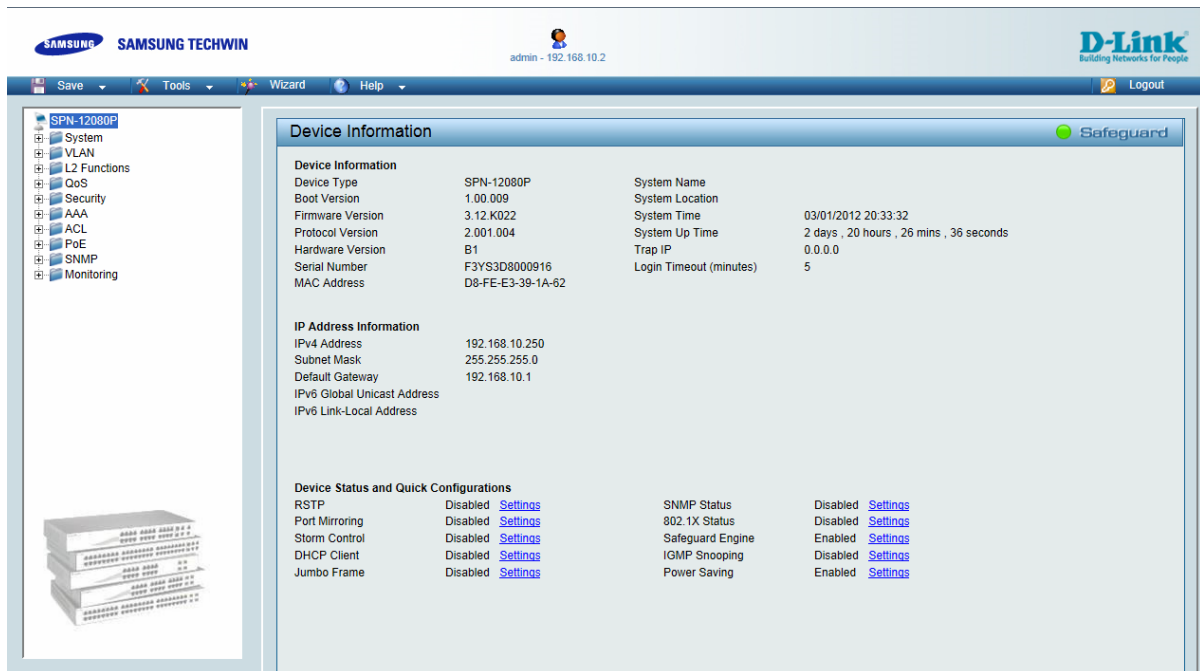


Figure 5.5 – Web-based Management

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

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

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

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

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



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

Tool Bar > Save Menu

The Save Menu provides Save Configuration and Save Log functions.

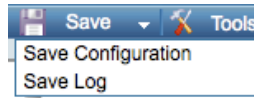


Figure 5.6 – Save Menu

Save Configuration

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

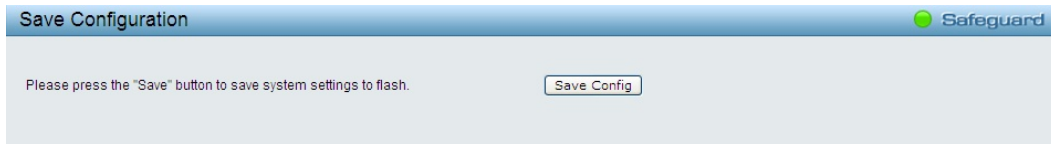


Figure 5.7 – Save Configuration

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).

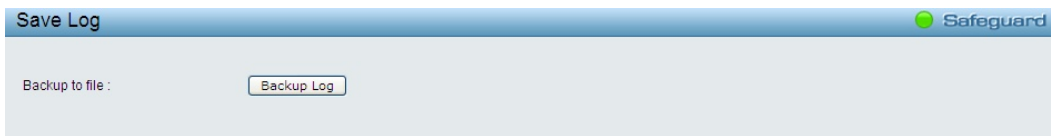


Figure 5.8 – Save Log

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.

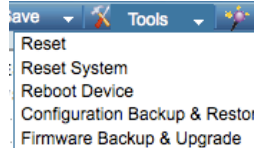


Figure 5.9 – Tool Menu

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.

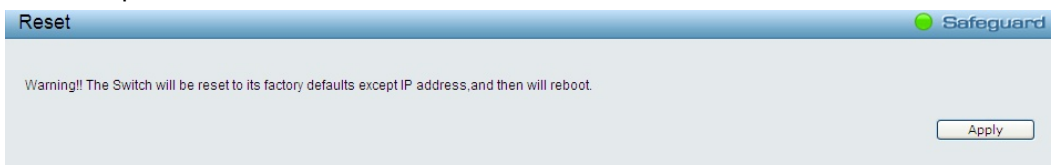


Figure 5.10 – Tool Menu > Reset

Reset System

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

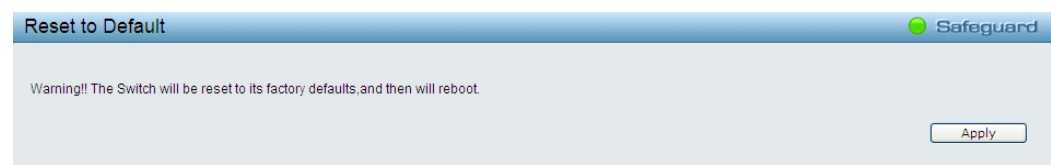


Figure 5.11 – Tool Menu > Reset System

Reboot Device

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

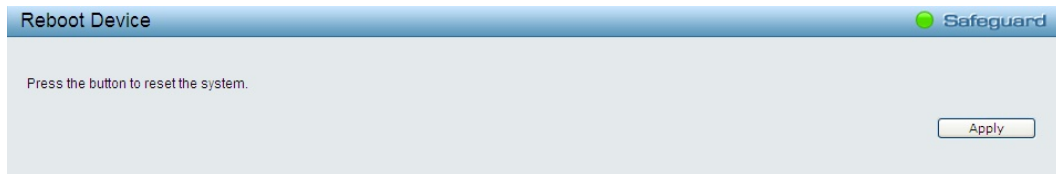


Figure 5.12 – Tool Menu > Reboot Device

Configuration Backup and Restore

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

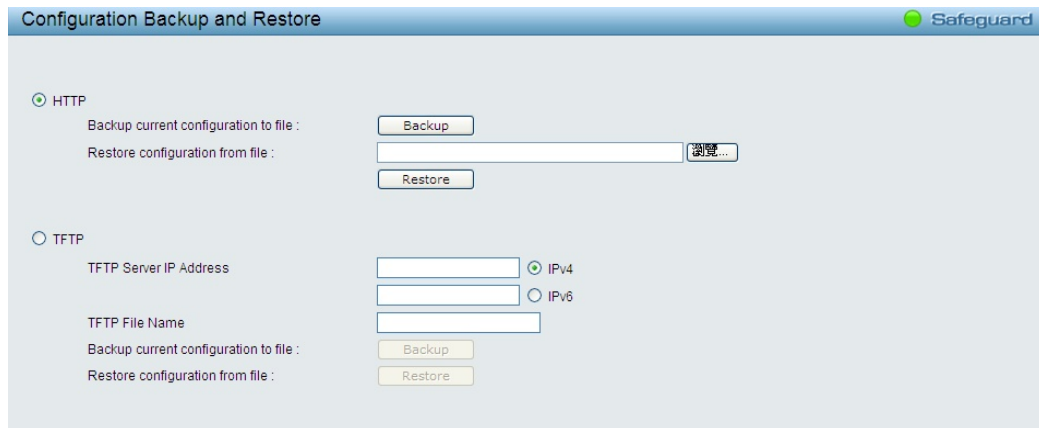


Figure 5.13 – Tool Menu > Configure Backup and Restore

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

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

Click **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. Specify **TFTP Server IP Address** with IPv4 or IPv6 address and **TFTP File Name** for the configuration file you want to save to / restore from.

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

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



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

Firmware Backup and Upgrade

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

Figure 5.14 – Tool Menu > Firmware Backup and Upload

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

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. Specify **TFTP Server IP Address** with IPv4 or IPv6 address and **TFTP File Name** for the configuration file you want to save to / restore from.

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

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



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

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.

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.

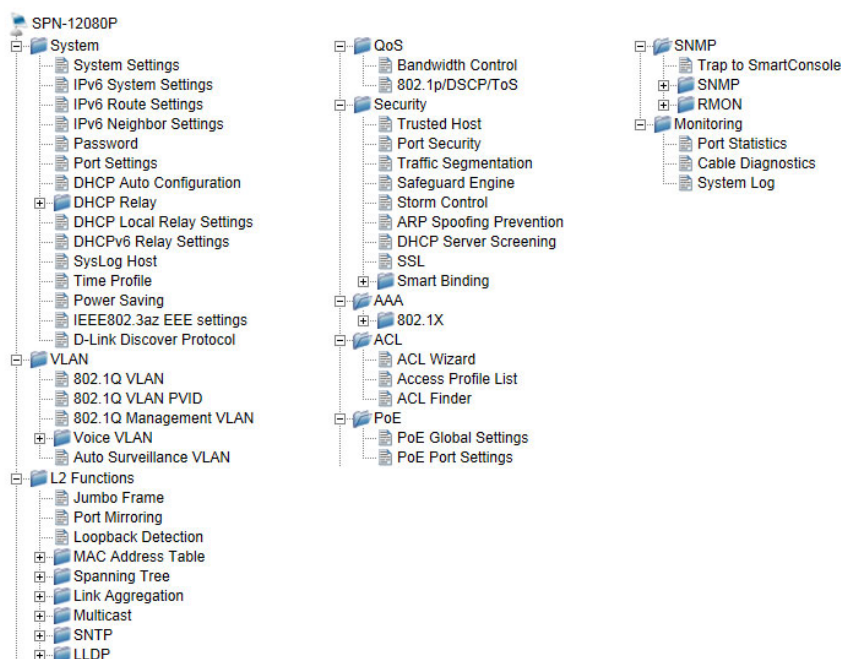


Figure 5.17 –Function Tree

Device Information

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

It also offers an overall status of common software features:

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

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

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

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

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

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

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

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

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

Power Saving: Click **Settings** to link to System > Power Saving. Default is disabled.



Figure 5.18 – 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**, **NetMask** and **Gateway** can be manually configured. When using DHCP mode, the Switch will first look for a DHCP server to provide it with an IP address (including network mask and default gateway) before using the default or previously entered settings. By default the IP setting is static mode with IP address is **10.90.90.90** and subnet mask is **255.0.0.0**.

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

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

Group Interval: The SAMSUNG PoE Switch will routinely send report packets to the SNMP Utility in order to maintain the information integrity. The user can adjust the **Group Interval** to optimal frequency. Selective range is from 120 to 1225 seconds, and 0 means disabling the reporting function, and the default setting is 120 seconds.

Figure 5.19 – System > System Settings

System > IPv6 System Settings

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

Figure 5.20 – 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 5.21 – 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 5.22 – 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

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

Figure 5.23 – System > Password Access Control

System > Port Settings

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

Port	Link Status	Speed	MDI/MDIX	Flow Control
01	1000M Full	Auto	Auto	Disabled
02	Link down	Auto	Auto	Disabled
03	Link down	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

Figure 5.24 – 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 the 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 a configurable **MDI/MDIX** function for users. The switches can be set as an MDI port in order to connect to other hubs or switches without an Ethernet crossover cable.

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

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

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

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.

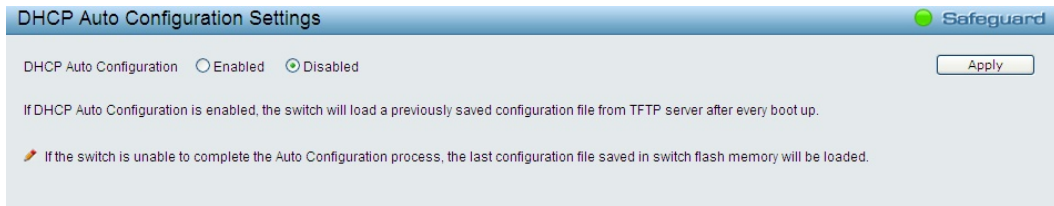


Figure 5.25 – System > DHCP Auto Configuration

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



Figure 5.26 – System > SysLog Host Settings

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

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

Time Stamp: Select Enable to time stamp log messages.

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

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

Informational - Provides device information.

All - Displays all levels of system logs.

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.

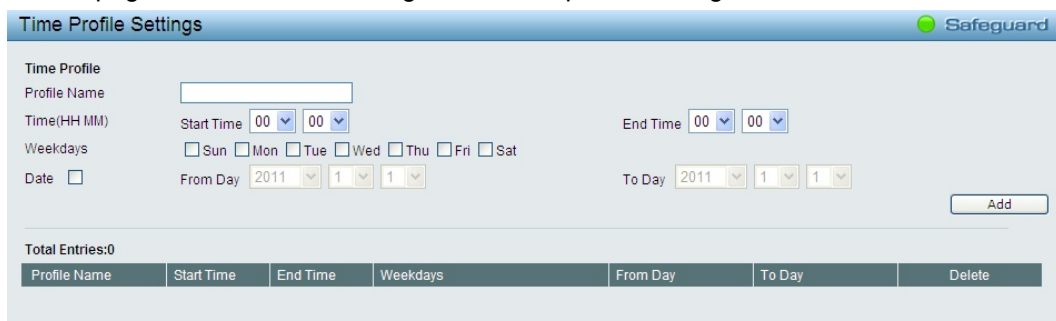


Figure 5.27 – System > Time Profile

Profile Name: Specifies the profile name.

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

Weekdays: Specifies the work day.

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

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

System > Power Saving

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

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

Power Saving Settings Safeguard

Global Settings

Cable Length Detection ☒ Enabled ☐ Disabled

Link Status Detection ☐ Enabled ☒ Disabled Apply

Advanced Power Saving Settings

Type: LED Shut-off State: Disabled

Time Profile 1: None Time Profile 2: None

Select All Clear Apply

Port	01	02	03	04	05
	☐	☐	☐	☐	☐
Port	6	7	8	9	10
	☐	☐	☐	☐	☐

Summary

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

Figure 5.28 – System > Power Saving

Advanced Power Saving Settings:

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

LED Shut-off - The LED Shut-off gets high priority. If the user select LED Shut-off, the profile function will not take effect. It means the LED 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.

Port Standby - The system changes to standby state and wait for a wake up event. Each port on the system enters sleep state by schedule.

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

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

Time Profile 1: Specifies the time profile or None.

Time Profile 2: Specifies the time profile or None.

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

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

Port	State
1	Enabled
2	Enabled
3	Enabled
4	Enabled
5	Enabled
6	Enabled
7	Enabled
8	Enabled
9	Enabled
10	Enabled

Figure 5.29 – 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.

VLAN > 802.1Q VLAN

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

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

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

Rename: Click to rename the VLAN group.

Delete VID: Click to delete the VLAN group.

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

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

VID	VLAN Name	Untagged	Tagged	Delete
1	default	01-10		Delete

Figure 5.30 – Configuration > 802.1Q VLAN

Port	Select All	01	02	03	04	05	06	07	08	09	10
Untagged	All										
Tagged	All										
Not member	All										

Figure 5.31 – Configuration > 802.1Q VLAN > Add VLAN

VLAN > 802.1Q VLAN PVID

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

Port	01	02	03	04	05	06	07	08	09	10
PVID	1	1	1	1	1	1	1	1	1	1

Figure 5.32 – Configuration > 802.1Q VLAN PVID

VLAN > 802.1Q Management VLAN

The 802.1Q Management VLAN setting allows user 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.

Figure 5.33 – Configuration > 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 5.34 – VLAN > Voice VLAN > Voice VLAN Global Settings

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

VLAN ID: The ID of VLAN that you want to assign voice traffic to. You must first create a VLAN from the 802.1Q VLAN page before you can assign a dedicated Voice VLAN. The member port you configured in 802.1Q VLAN setting page will be the static member port of voice VLAN. To dynamically add ports into the voice VLAN, please enable the **Auto Detection** function

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

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

Click **Apply** to implement changes made.

Voice VLAN OUI Settings: This allows the user to configure the user-defined voice traffic's OUI. An 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 a 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: Voice VLAN has higher priority than any other features (including QoS). Therefore the voice traffic will be operated according to the Voice VLAN setting and not impacted by the QoS feature.



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

VLAN > Voice VLAN > Voice VLAN Port Settings

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

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

Figure 5.35 – VLAN > Voice VLAN > Voice VLAN Port Settings

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

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

Tagged / Untagged: tagged or untagged the ports.

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



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



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

VLAN > Voice VLAN > Voice Device List

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

ID	Port	MAC Address	Priority	Type	Delete
----	------	-------------	----------	------	--------

Figure 5.36 – 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 Settings

Similar as Voice VLAN, Auto Surveillance VLAN is a feature that allows you to automatically place the video traffic from specific 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.

Auto Surveillance VLAN Settings Safeguard

Auto Surveillance VLAN Global Settings

Auto Surveillance VLAN ☐ Enabled ☒ Disabled

VLAN ID: 4094 Priority: Medium Tagged Uplink/Downlink Port: Ex: 1,2,4-6

User-defined MAC Settings

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

Component Type: Video Management Server Description: Description (XX-XX-XX-XX-XX-XX) MAC: MAC

Maximum number of user-defined MAC is 5 entries.

ID	Component Type	Description	MAC Address	Delete
01	D-Link Surveillance Device	D-Link IP Surveillance Device	28-10-7B:XXXXXX	Default
02	D-Link Surveillance Device	D-Link IP Surveillance Device	F0-7D-68:0XXXXX	Default

Auto Surveillance VLAN Summary

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

Figure 5.37 – VLAN > Auto Surveillance VLAN

Auto Surveillance VLAN Global Settings:

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

VLAN ID: By default, the VLAN ID 4094 was created as Auto Surveillance VLAN. 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 *Highest, High, Medium and Low*.

Tagged Uplink/Downlink Port: Specifies the 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 specific Surveillance Devices by default. There are another five surveillance components that could be configured to be auto-detected by the Auto Surveillance VLAN. These five components are *Video Management Server (VMS)*, *VMS Client/Remote viewer*, *Video Encoder*, *Network Storage* and *Other IP Surveillance Devices*.

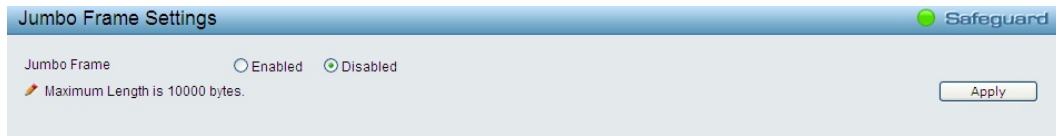
Description: Here to input the description for the component type.

MAC/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

SAMSUNG PoE Switches support jumbo frames (frames larger than the Ethernet frame size of 1536 bytes) of up to 10,000 bytes (tagged). Default is disabled, Select **Enabled** then click **Apply** to turn on the jumbo frame support.



Jumbo Frame Settings Safeguard

Jumbo Frame ☐ Enabled ☒ Disabled

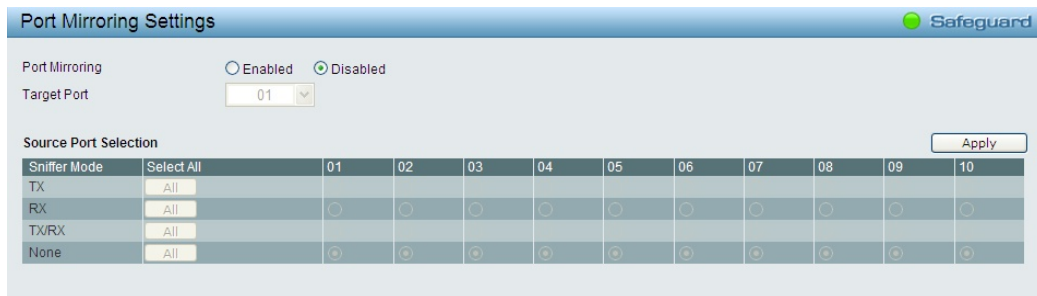
Maximum Length is 10000 bytes.

Apply

Figure 5.38 – 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.



Port Mirroring Settings Safeguard

Port Mirroring ☐ Enabled ☒ Disabled

Target Port

Source Port Selection Apply

Sniffer Mode	Select All	01	02	03	04	05	06	07	08	09	10
TX	All										
RX	All	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
TX/RX	All	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
None	All	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Figure 5.39 – L2 Functions > Port Mirroring

Selection options for the Source Ports are as follows:

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

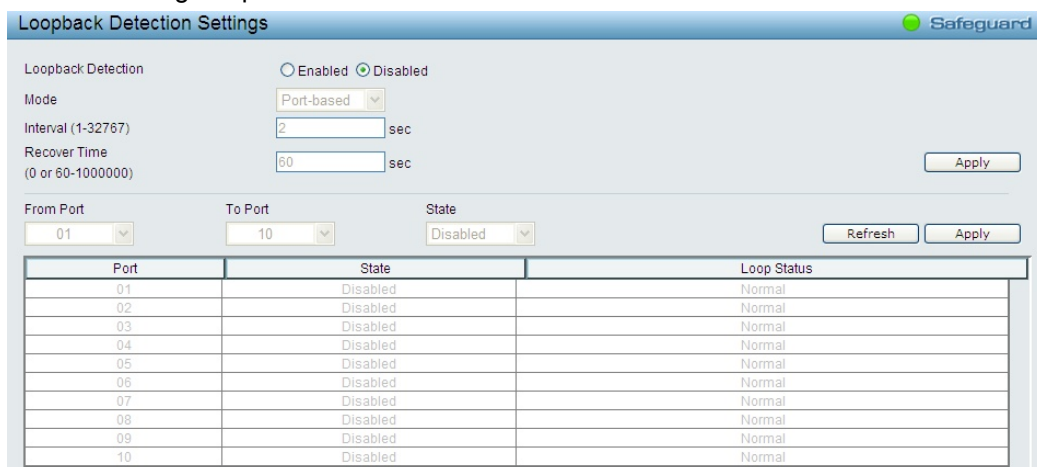
RX (receive) mode: Duplicates the data that is received from the source port and forwards it to the Target Port. Click “all” to include all ports into port mirroring.

TX/RX (transmit and receive) mode: Duplicate both the data transmitted from and data sent to the source port, and forwards all the data to the assigned Target Port. Click “all” to include all ports into port mirroring.

None: Turns off the mirroring of the port. Click “all” to remove all ports from mirroring.

L2 Functions > Loopback Detection

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



Loopback Detection Settings Safeguard

Loopback Detection ☐ Enabled ☒ Disabled

Mode

Interval (1-32767) sec

Recover Time (0 or 60-1000000) sec Apply

From Port To Port State Refresh Apply

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

Figure 5.40 – L2 Functions > Loopback Detection

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

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

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

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

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

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

State: Use the drop-down menu to toggle between *Enabled* and *Disabled*. Default is *Disabled*.

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

L2 Functions > MAC Address Table > Static MAC

This feature provides two distinct functions. The **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 5.41 – L2 Functions > MAC Address Table > Static Mac Address

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 Lists** 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 then Click **Add**. Click **Delete** to remove one entry or click **Delete all** to clear the list.

By disabling Auto Learning capability and specifying the static MAC addresses, the network is protected from potential threats like hackers, because traffic from illegal MAC addresses will not be forwarded by the Switch.

L2 Functions > MAC Address Table > Dynamic Forwarding Table

For each port, this table displays the MAC address learned by the Switch. To add a MAC address to the Static Mac Address List, click the **Add** checkbox, and then click **Apply** associated with the identified address.

Figure 5.42 – L2 Functions > MAC Address Table > Dynamic Forwarding Table

L2 Functions > Spanning Tree > STP Global Settings

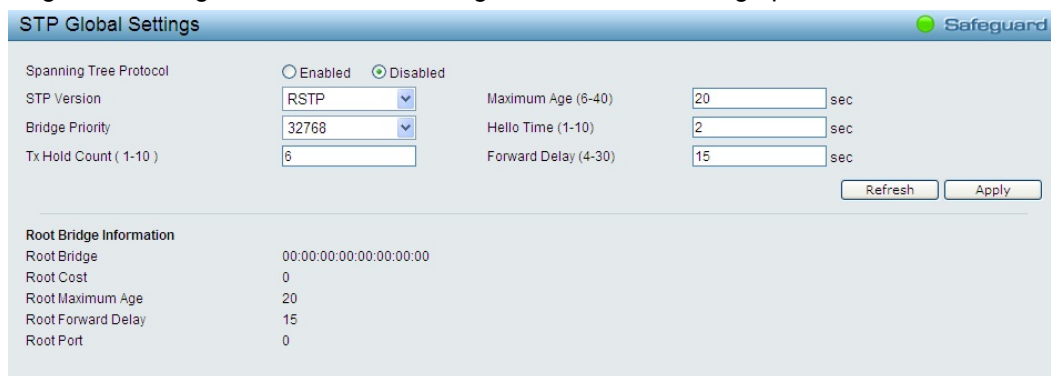
The Switch implements two versions of the Spanning Tree Protocol, the Rapid Spanning Tree Protocol (RSTP) as defined by the IEEE 802.1w specification and a version compatible with the IEEE 802.1D

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:



STP Global Settings	
Spanning Tree Protocol	☐ Enabled ☒ Disabled
STP Version	RSTP
Bridge Priority	32768
Tx Hold Count (1-10)	6
Maximum Age (6-40)	20 sec
Hello Time (1-10)	2 sec
Forward Delay (4-30)	15 sec
Refresh Apply	
Root Bridge Information	
Root Bridge	00:00:00:00:00:00:00:00
Root Cost	0
Root Maximum Age	20
Root Forward Delay	15
Root Port	0

Figure 5.43 – 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 Cost: Display the cost of the Root Bridge.

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

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

Root port: Displays the root port.

Click **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 the groups of ports, each port-group of which will have its own spanning tree, and will require some of its own configuration settings.

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

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

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

Port	State	Priority	External Cost	Edge	P2P	Restricted Role	Restricted TCN	Port Status
01	Enable	128	AUTO/20000	Auto	Auto	False	False	Disabled
02	Enable	128	AUTO/20000	Auto	Auto	False	False	Disabled
03	Enable	128	AUTO/20000	Auto	Auto	False	False	Disabled
04	Enable	128	AUTO/20000	Auto	Auto	False	False	Disabled
05	Enable	128	AUTO/20000	Auto	Auto	False	False	Disabled
06	Enable	128	AUTO/20000	Auto	Auto	False	False	Disabled
07	Enable	128	AUTO/20000	Auto	Auto	False	False	Disabled
08	Enable	128	AUTO/20000	Auto	Auto	False	False	Disabled
09	Enable	128	AUTO/20000	Auto	Auto	False	False	Disabled
10	Enable	128	AUTO/20000	Auto	Auto	False	False	Disabled

Figure 5.44 – 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 consists up to eight ports. Select the ports to be grouped together, and then click **Apply** to activate the selected Trunking groups. Two types of link aggregation can be selected:

Static - Static link aggregation.

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

Disable - Remove all members in this trunk group.

Port Trunking

Link Aggregation ☐ Enabled ☒ Disabled Apply

Link Aggregation Settings

Group Type Apply

Port	01	02	03	04	05
	☐	☐	☐	☐	☐
Port	6	7	8	9	10
	☐	☐	☐	☐	☐

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

Trunking list			
Group	Type	Ports	Delete

Figure 5.45 – 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.

LACP Port Settings

From Port To Port Activity Timeout Apply

Port	Activity	Timeout
01	Active	Long (90 sec)
02	Active	Long (90 sec)
03	Active	Long (90 sec)
04	Active	Long (90 sec)
05	Active	Long (90 sec)
06	Active	Long (90 sec)
07	Active	Long (90 sec)
08	Active	Long (90 sec)
09	Active	Long (90 sec)
10	Active	Long (90 sec)

Figure 5.46 – 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 Web Smart 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 Web Smart 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) 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	default	Enabled	Disabled	Disabled		View

Figure 5.47 – L2 Functions > Multicast > IGMP Snooping

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

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

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

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

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

Static Router Ports

01	02	03	04	05	06	07	08	09	10
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Dynamic Router Ports

01	02	03	04	05	06	07	08	09	10
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Apply

Figure 5.48 – L2 Functions > Multicast > IGMP Snooping VLAN Settings

State : Specify the State to be enabled or disabled.

Querier State: SAMSUNG PoE 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

Group ID	VLAN ID	VLAN Name	Multicast Group	Multicast MAC address	Member Port	Delete
001	1	default	239.255.255.250	01-00-5E-7F-FF-FA	01	Delete

Back Delete All

Figure 5.45 – 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 > Multicast Forwarding

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

Multicast Forwarding Settings Safeguard

VID:

Multicast MAC Address: Add

Port	Select All	01	02	03	04	05	06	07	08	09	10
Member	All	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
None	All	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒

Total Static Entries: 0

VID	MAC Address	Member Ports	Delete
-----	-------------	--------------	--------

Figure 5.49 – 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 Safeguard

VLAN ID:

Filtering Mode: Forward Unregistered Groups ▼ Apply

Multicast Filtering Mode Table

Multicast Filtering Mode	VLAN ID
Forward Unregistered Groups	1
Filter Unregistered Groups	

Figure 5.50 – 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 unregistered 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 5.51 – 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 and specify the IP address of the primary SNTP server from which the system time is retrieved.

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

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

Click **Apply** to implement changes made.

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

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

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

L2 Functions > SNTP > TimeZone Settings

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

Figure 5.52 – L2 Functions > SNTP > TimeZone Settings

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

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

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

Daylight Saving Time Settings:

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

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

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

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

Click **Apply** to implement changes made.

L2 Functions > LLDP > LLDP Global Settings

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

LLDP Global Settings	
LLDP	☒ Enabled ☐ Disabled
Message TX Hold Multiplier (2 - 10)	4
Message TX Interval (5 - 32768)	30 sec
LLDP Reinit Delay (1 - 10)	2 sec
LLDP TX Delay (1 - 8192)	2 sec
Apply	
LLDP System Information	
Chassis ID Subtype	macAddress
Chassis ID	00-01-02-03-04-05
System Name	
System Description	DGS-1210-10P 3.10.006

Figure 5.53 – L2 Functions > LLDP > LLDP Global Settings

LLDP: When this function is *Enabled*, the switch can start to transmit, receive and process the LLDP packets. For the advertisement of LLDP packets, the switch announces the information to its neighbor through ports. For the receiving of LLDP packets, the switch will learn the information from the LLDP packets advertised from the neighbor in the neighbor table. Click **Apply** to make the change effective.

Message TX Hold Multiplier (2-10): This parameter is a multiplier that determines the actual TTL value used in an LLDPDU. The default value is 4.

Message TX Interval (5-32768): This parameter indicates the interval at which LLDP frames are transmitted on behalf of this LLDP agent. The default value is 30 seconds.

LLDP Reinit Delay (1-10): This parameter indicates the amount of delay from the time adminStatus becomes "disabled" until re-initialization is attempted. The default value is 2 seconds.

LLDP TX Delay (1-8192): This parameter indicates the delay between successive LLDP frame transmissions initiated by value or status changes in the LLDP local systems MIB. The value for txDelay is set by the following range formula: $1 < \text{txDelay} < (0.25 \times \text{msgTxInterval})$. The default value is 2 seconds.

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.

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

Figure 5.54 – 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.

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

Figure 5.55 – 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)

Figure 5.56 – L2 Functions > LLDP > 802.1 Extension TLV Port Settings

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

Port VLAN ID : Specifies the Port VLAN ID to be enabled or disabled.

VLAN Name : Specifies the VLAN name to be enabled or disabled in the LLDP port. If select Enabled, users can specifies the content of VLAN ID or VLAN Name or all.

Protocol Identity : Specifies the Protocol Identity to be enabled or disabled in the LLDP port. If select Enabled, users can specifies the EAPOL, LACP, GVRP, STP or ALL.

Click **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 5.57 – L2 Functions > LLDP > 802.3 Extension TLV Port Settings

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

MAC/PHY Configuration/Status: Specifies whether the MAC/PHY Configuration Status is enabled on the port. The possible field values are:

Enabled – Enables the MAC/PHY Configuration Status on the port.

Disabled – Disables the MAC/PHY Configuration Status on the port.

Power via MDI: Advertises the Power via MDI implementations supported by the port. The possible field values are:

Enabled – Enables the Power via MDI configured on the port.

Disabled – Disables the Power via MDI configured on the port.

Link Aggregation: Specifies whether the link aggregation is enabled on the port. The possible field values are:

Enabled – Enables the link aggregation configured on the port.

Disabled – Disables the link aggregation configured on the port.

Maximum Frame Size: Specifies whether the Maximum Frame Size is enabled on the port. The possible field values are:

Enabled – Enables the Maximum Frame Size configured on the port.

Disabled – Disables the Maximum Frame Size configured on the port.

Define these parameter fields. Click **Apply** to implement changes made and click **Refresh** to refresh the table information.

L2 Functions > LLDP > LLDP Management Address Settings

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

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

Figure 5.58 – 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 on 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	rfindex	1.3.6.1.2.1.2.2.1.1	(NONE)

Figure 5.59 – L2 Functions > LLDP > LLDP Management Address Table

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

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

Management Address: Displays the IP address.

IF Type: Displays the IF Type.

OID: Displays the SNMP OID.

Advertising Ports: Displays the advertising ports.

L2 Functions > LLDP > LLDP Local Port Table

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

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

Figure 5.60 – L2 Functions > LLDP > LLDP Local Port Table

Port : Displays the port number.

Port ID Subtype: Displays the port ID subtype.

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

Port Description: Displays the port description.

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

LLDP Local Port Normal Table Safeguard	
No.	1
Port Id Subtype	Interface Alias
Port Id	Slot0/1
Port Description	Ethernet Interface
Port VID	1
Management Address Count	1
PPVID Entries Count	0
VLAN Name Entries Count	1
Protocol Identity Entries Count	0
MAC/PHY Configuration/Status	See detail
Power Via MDI	See detail
Link Aggregation	See detail
Maximum Frame Size	1522
Show LLDP Local Port Brief Table Show LLDP Local Port Detailed Table	

Figure 5.61 – L2 Functions > LLDP > LLDP Local Port Normal Table

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

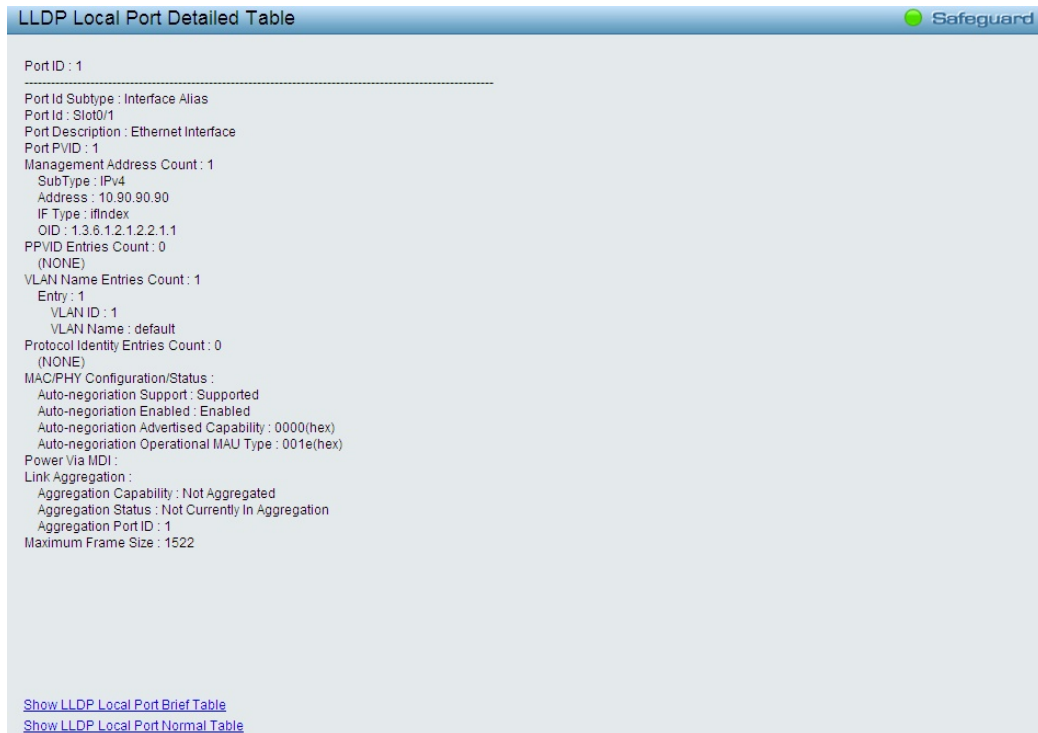


Figure 5.62 – L2 Functions > LLDP > LLDP Local Port Detailed Table

L2 Functions > LLDP > LLDP Remote Port Table

This LLDP Remote Port Table page is used to display the LLDP Remote Port Brief Table. Select port number and click **Search** to display additional information.

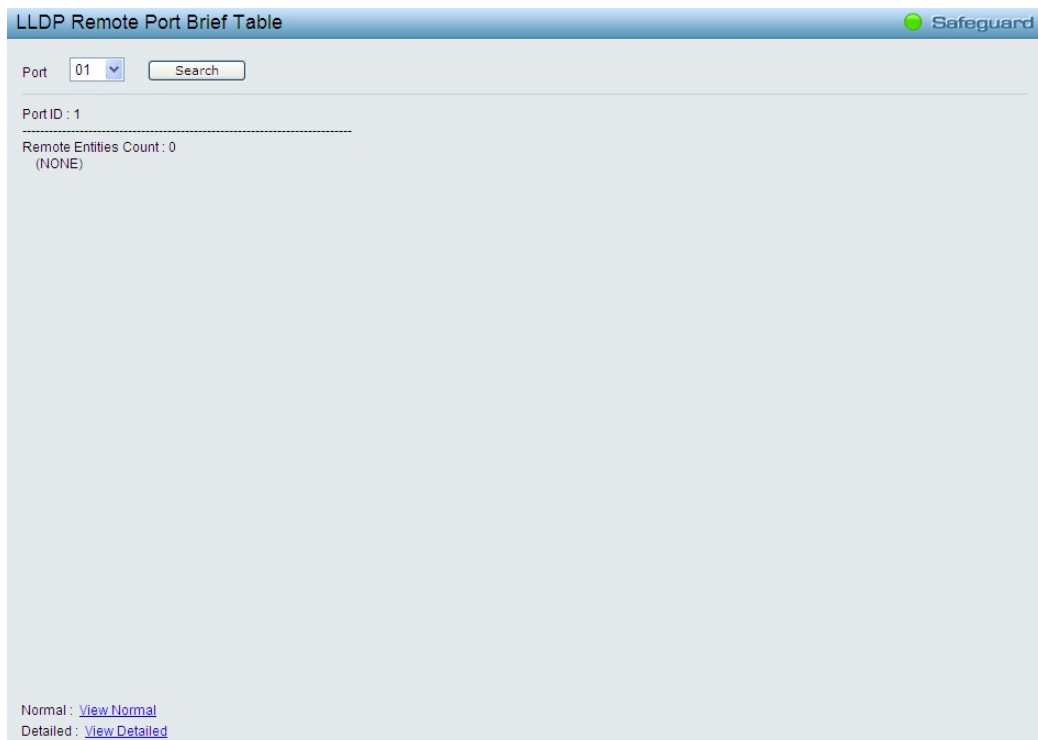
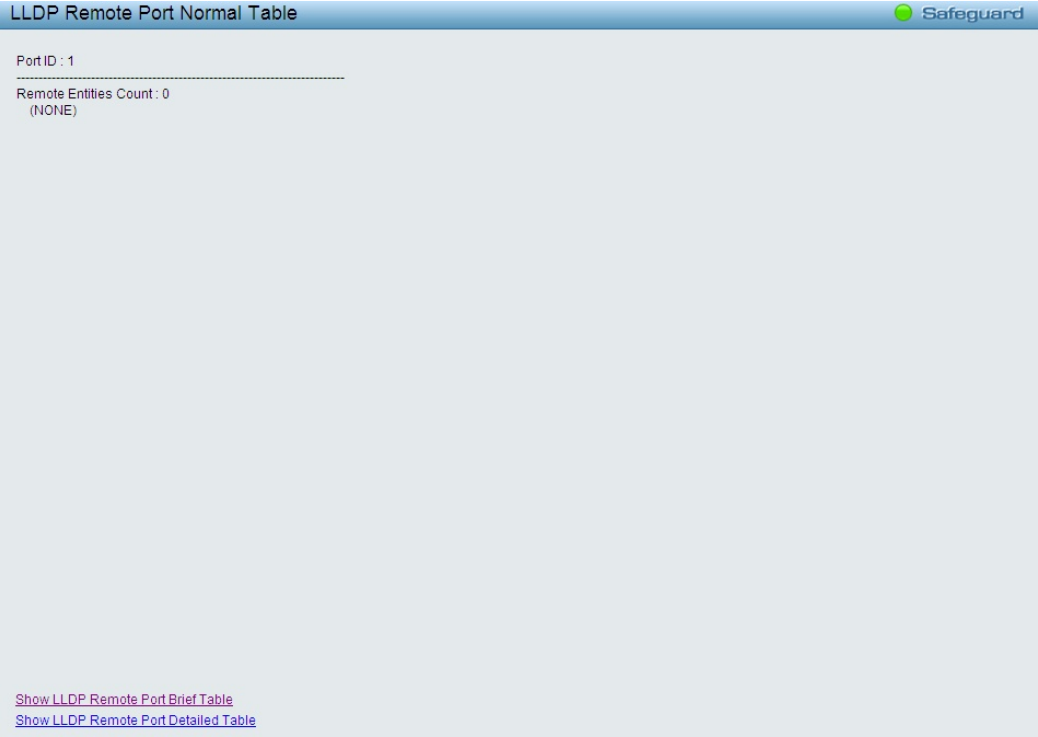


Figure 5.63 – L2 Functions > LLDP > LLDP Remote Port Table

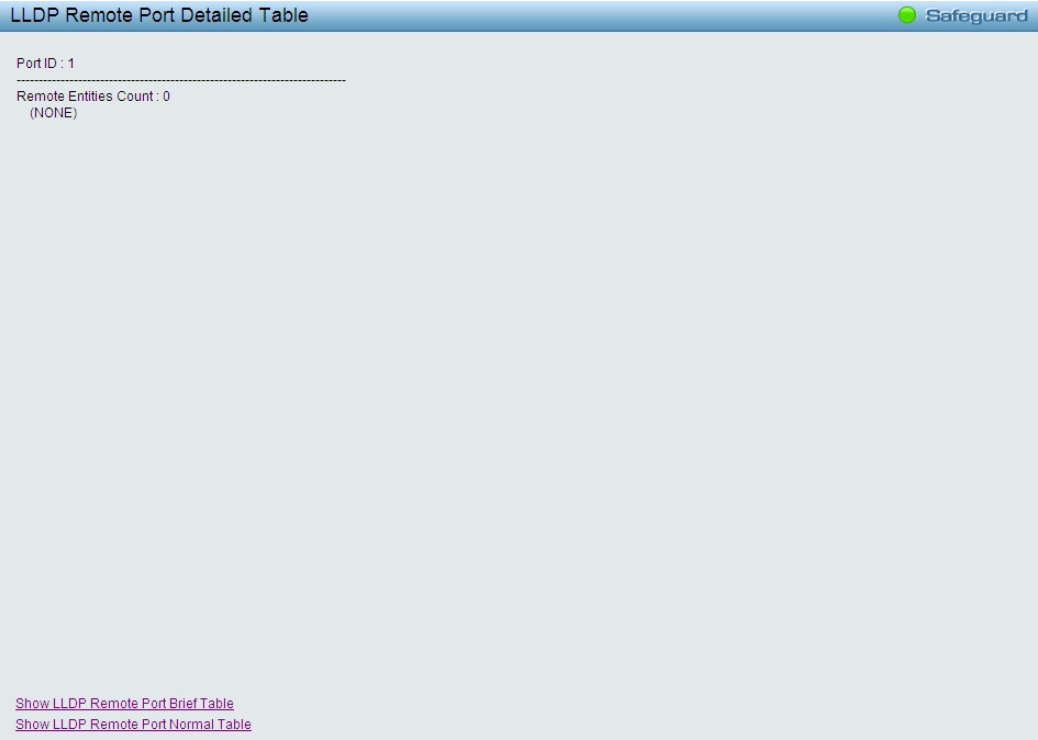
To view the settings for a remote port, click **View Normal** and the following page displays.



LLDP Remote Port Normal Table	
Port ID : 1	
Remote Entities Count : 0 (NONE)	
Show LLDP Remote Port Brief Table Show LLDP Remote Port Detailed Table	

Figure 5.64 – L2 Functions > LLDP > LLDP Remote Port Normal Table

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



LLDP Remote Port Detailed Table	
Port ID : 1	
Remote Entities Count : 0 (NONE)	
Show LLDP Remote Port Brief Table Show LLDP Remote Port Normal Table	

Figure 5.65 – L2 Functions > LLDP > LLDP Remote Port Detailed Table

L2 Functions > LLDP > LLDP Statistics

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

LLDP Statistics Table



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

Figure 5.66 – L2 Functions > LLDP > LLDP Statistics

The following information can be viewed:

LLDP Statistics System: Displays the counters that refer to the whole switch.

Last Change Time – Displays the time for when the last change entry was last deleted or added. It also displays the time elapsed since last change was detected.

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

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

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

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

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

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

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

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

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

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

RxPortTLVsUnrecognized – Displays the number of well-formed TLVs, but with an 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
08	No Limit	No Limit
09	No Limit	No Limit
10	No Limit	No Limit

Figure 5.67 – QoS > Bandwidth Control

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

Type: This drop-down menu allows you to select between *RX* (receive), *TX* (transmit), and *Both*. This setting will determine whether the bandwidth ceiling is applied to receiving, transmitting, or both receiving and transmitting packets.

No Limit: This drop-down menu allows you to specify that the selected port will have no bandwidth limit. *Enabled* disables the limit.

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

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

QoS > 802.1p/DSCP/ToS

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

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

Port	Priority
01	Medium
02	Medium
03	Medium
04	Medium
05	Medium
06	Medium
07	Medium
08	Medium
09	Medium
10	Medium

For ingress untagged packets, the per port "Default Priority" settings will be applied to packets of each port to provide port-based traffic prioritization.
For ingress tagged packets, D-Link Smart Switches will refer to their 802.1p information and prioritize them with 4 different priority queues.

802.1p mapping table

Low	=1,2
Medium	=0,3
High	=4,5
Highest	=6,7

Figure 5.68 – QoS > 802.1p/DSCP/ToS

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

Queuing Mechanism:

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

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

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

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

Priority: Defines the priority assigned to the port. The priorities are Highest, High, Medium and Low.

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

QoS > IPv6 Traffic Class Priority Settings

The IPv6 Traffic Class Priority Settings page allows user to configure the priority of traffic class.

Figure 5.69 – QoS > IPv6 Traffic Class Priority Settings

IPv6 Traffic Class (0-255): Specify the value of IPv6 class.

Priority: Defines the priority assigned to the port. The priorities are Highest, High, Medium and Low.

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

QoS > TCP/UDP Port Priority Settings

The TCP/UDP Port Priority Settings page allows user to configure the port priority.

Figure 5.70 – QoS > TCP/UDP Port Priority Settings

TCP/UDP: Specify port priority of TCP or UDP to be configured.

TCP/UDP Port (0-65535): Specify the TCP or UDP port.

Priority: Defines the priority assigned to the port. The priorities are Highest, High, Medium and Low.

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

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.

Figure 5.71 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 can not be changed once the port lock is enabled. Using the drop-down menu, change **Admin State** to *Enabled*, input Max Learning Address, and then click **Apply**.

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 5.72 – 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.

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

Figure 5.73 – 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 **Traffic Segmentation** table.

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

Security > Safeguard Engine

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

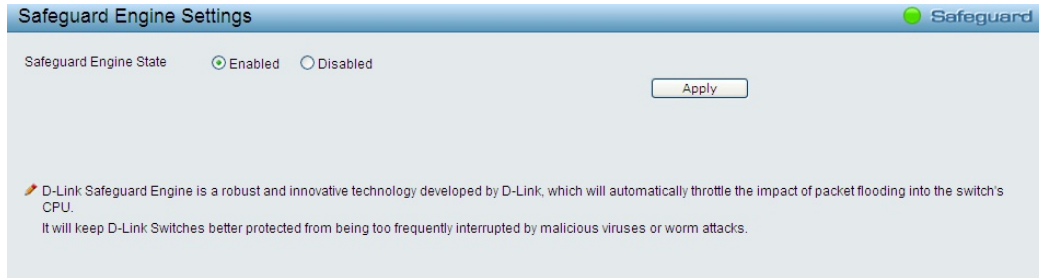


Figure 5.74 – Security > Safeguard Engine

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.

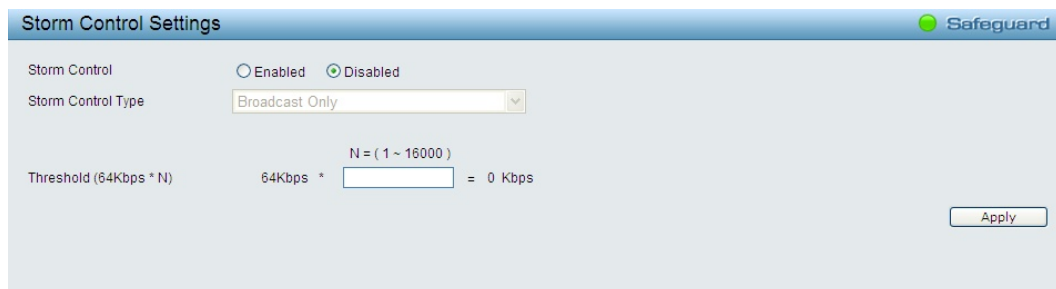


Figure 5.75 – Security > Storm Control

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.

ARP Spoofing Prevention Settings Safeguard

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

Total Entries: 0 Delete All

Maximum 64 entries.

IP Address	MAC Address	Ports	Delete
------------	-------------	-------	--------

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

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

Figure 5.76 – Security > ARP Spoofing Prevention

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

Security > DHCP Server Screening

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

DHCP Server Screening Settings Safeguard

DHCP Server Trusted Port Settings Apply

Port	01	02	03	04	05
	☒	☒	☒	☒	☒
Port	6	7	8	9	10
	☒	☒	☒	☒	☒

Trusted DHCP Server IP Settings

☒ IPv4 Add

☐ IPv6 Ex:(1234::1234) Add

Trusted DHCP Server IP Lists

Maximum 5 entries.

Index	IP Address	Delete
-------	------------	--------

Figure 5.77 – 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.

Click **Add** to add a DHCP 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 5.78 – 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 > Smart Binding > Smart Binding Settings

The primary purpose of Smart Binding is to restrict client access to a switch by enabling administrators to configure pairs of client MAC and IP addresses that are allowed to access networks through a switch.

The Smart Binding function is port-based, meaning that a user can enable or disable the function on any individual port. Once Smart Binding is enabled on a switch port, the switch will restrict or allow client access by checking the pair of IP-MAC addresses with the pre-configured database, also known as the “IMPB white list”.

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

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

Figure 5.79 – Security > Smart Binding > Smart Binding Settings

The Smart Binding Settings page contains the following fields:

From Port/ To Port: Select a range of ports to set for IP-MAC-port binding.

State: Use the drop-down menu to enable or disable these ports for Smart Binding.

Enabled –Enable Smart Binding with related configurations to the ports

Disabled –Disable Smart Binding.

Packet Inspection: Specifies *ARP Inspection* or *IP+ARP Inspection* for the IP packets. If ARP inspection is selected, the Switch will inspect incoming ARP packets and compare them with the Switch’s Smart Binding white list entries. If the IP-MAC pair of an ARP packet is not found in the white list, the Switch will block the MAC address. A major benefit of Loose state is that it uses less CPU resources. However, it cannot block malicious users who send only unicast IP packets. An example of this is that a malicious user can perform DoS attacks by statically configuring the ARP table on their PC. In this case, the Switch cannot block such attacks because the PC will not send out ARP packets. If **ARP+ IP Inspection** mode is selected, the Switch

will inspect all incoming ARP and IP packets and compare them to the IMPB white list. If the IP-MAC pair find a match in the white list, the packets from that MAC address are unblocked. If not, the MAC address will stay blocked. While the mode examines every ingress ARP and IP packet, it enforces better security.

DHCP Snooping: By enable DHCP Snooping, the switch will snoop the packets sent from DHCP Server and clients, and update information to the White List.

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

Security > Smart Binding > Smart Binding

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

Figure 5.80 – 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: The Auto Scan Setting can list connected devices and easily select to bind. It contains the following fields:

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

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

Binding: check the box to select desired binding devices.

Apply: click **Apply** to set IP-MAC-Port Binding entries.”

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

Clear All: to cancel the box of Binding

Security > Smart Binding > White List

When IP +ARP Inspection Mode is selected, the White List page displays finished IP-MAC-Port Binding entries from page Smart Binding. Only IP packets or ARP packets carrying matched IP-MAC-Port information can access to the switch. You can cancel a device’s authorization by deleting it from the table.

Figure 5.81 – Security > Smart Binding > White List

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

Click **Select All** to select all entries of the table or click **Clean** to select none entries. Please keep at least one management host in the White List.

Security > Smart Binding > Black List

The Black List page shows unauthorized accesses. When ARP Inspection is selected and a device sends out an ARP packet containing unmatched IP-MAC-Port information, the device will be forbidden and listed here.

Figure 5.82 – Security > Smart Binding > Black List

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

VID: Enter the VLAN ID number of the device.

IP Address: Enter the IP Address of the device.

MAC Address: Enter the MAC Address of the device.

Port: Enter the port number which the device connects to.

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

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

AAA > 802.1X > 802.1X Settings

Network switches provide easy and open access to resources, by simply attaching a client PC. Unfortunately this automatic configuration also allows unauthorized personnel to easily intrude and possibly gain access to sensitive data.

IEEE-802.1X provides a security standard for network access control, especially in Wi-Fi wireless networks. 802.1X holds a network port disconnected until authentication is completed. The switch uses Extensible Authentication Protocol over LANs (EAPOL) to exchange authentication protocol client identity (such as a user name) with the client, and forward it to another remote RADIUS authentication server to verify access rights. The EAP packet from the RADIUS server also contains the authentication method to be used. The client can reject the authentication method and request another, depending on the configuration of the client software and the RADIUS server. Depending on the authenticated results, the port is either made available to the user, or the user is denied access to the network.

The RADIUS servers make the network a lot easier to manage for the administrator by gathering and storing the user lists.

802.1X Settings

802.1X ☐ Enabled ☒ Disabled

802.1X Global Settings

Radius Server IP: ☒ IPv4 ☐ IPv6

Key:

Confirm Key:

TxPeriod (1 - 65535 sec):

ReAuthEnabled:

QuietPeriod (0 - 65535 sec):

ServerTimeout (1 - 65535 sec):

SuppTimeout (1 - 65535 sec):

MaxReq (1 - 10):

ReAuthPeriod (1 - 4294967295 sec):

802.1X Port Access Control

From Port: To Port: Control:

Port	Control	Port Status	Session Time	User ID
01	Force Authorized	*	0	*****
02	Force Authorized	*	0	*****
03	Force Authorized	*	0	*****
04	Force Authorized	*	0	*****
05	Force Authorized	*	0	*****
06	Force Authorized	*	0	*****
07	Force Authorized	*	0	*****
08	Force Authorized	*	0	*****
09	Force Authorized	*	0	*****
10	Force Authorized	*	0	*****

Figure 5.83 – Security > 802.1X > 802.1X Settings

By default, 802.1X is disabled. To use EAP for security, select enabled and set the 802.1X **Global Settings** for the Radius Server and applicable authentication information.

RADIUS Server IP: The IP address of the external Radius Server. You need to specify an RADIUS server to enable 802.1X authentication. Select IPv4 or IPv6 and specify the IP address.

Key: Masked password matching the Radius Server Key. The max. length is 32 characters.

Confirm Key: Enter the Key a second time for confirmation.

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 24 seconds.

ReAuthEnabled: This function is to determine whether regular re-authentication will take place on this port(s). When the 802.1X function is enabled, the switch sends an EAP-request/identity packet to client. The ReAuthEnabled function is by default disabled.

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.

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

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 – 4294967295 sec): This command affects the behavior of the switch only if periodic re-authentication is enabled. Default is 3600.

To establish 802.1X port-specific assignments, select the **From Ports / To Ports** and select **Enable**.

802.1X Port Access Control: Three type of Port Access Control State can be "Force Authorized", "Force Unauthorized" and "Auto".

Select **Force Authorized** 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 **Force Unauthorized** 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**.

ACL > ACL Wizard

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

The ACL Configuration Wizard will aid with the creation of access profiles and ACL Rules. The ACL Wizard will create the access rule and profile automatically. The maximum usable profiles are 50 and with 200 Rules in total for the switch. For DES-1210-52, the maximum usable profiles are 50 and with 450 Rules in total for the switch.

Figure 5.84 – ACL > ACL Wizard

From: Specify the origin of accessible packets. The possible values are:

- Any** - Indicates ACL action will take effect on packets from any source.
- MAC Address** - Indicates ACL action will be on packets from this MAC address.
- IPv4 Addresses** - Indicates ACL action will be on packets from this IPv4 source address.
- IPv6 Address** - Indicates ACL action will be on packets from this IPv6 source address.

To: Specify the destination of accessible packets. The possible values are:

- Any** - Indicates ACL action will be on packets to any destination.
- MAC Address** - Indicates ACL action will be on packets from this MAC address. The field of format is xx-xx-xx-xx-xx-xx.
- IPv4 Addresses** - Indicates ACL action will be on packets from this IPv4 source address.
- IPv6 Address** - Indicates ACL action will be on packets from this IPv6 source address.

Service Type: Specify the Type of Service to match. The possible values are:

- Any** - Indicates any service type of packets are examined.
- Ether type** - Select Ethernet type and IP, ARP or User Define address for filtering packets.
- ICMP All** - Indicates all ICMP packets are examined.
- IGMP** - IGMP packets can be filtered by IGMP message type.
- TCP All** - Indicates all TCP packets are examined.
- TCP Source Port** - Specify packets from the TCP source port.
- TCP Destination Port** - Matches the packet to the TCP Destination Port.
- UDP All** - Indicates all UDP packets are examined.
- UDP Source Port** - Specify packets from the UDP source port.
- UDP Destination Port** - Matches the packet to the UDP Destination Port.

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

Ports: Enter a range of ports to be configured.

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



NOTE: Once the ACL rules conflict, rules with the smaller rule ID will take higher priority.



NOTE: Be careful on ACL configuration. Inappropriate design may lead to management access failure.

ACL > ACL Profile List

The ACL Profile List provides information for configuring ACL Profiles manually. ACL profiles are attached to interfaces, and define how packets are forwarded if they match the ACL criteria.

Access Profile List Safeguard					
Add Delete All					
Profile ID	Type	Profile Summary			
51	Voice VLAN	Source MAC	Show Details	Show Rules	Delete
52	ARP-SP	Source MAC, Ether Type, ARP Sender MAC, ARP Sender IP	Show Details	Show Rules	Delete
53	ARP-SP	Ether Type, ARP Sender IP	Show Details	Show Rules	Delete
54	IMPB	Source MAC, Source IP	Show Details	Show Rules	Delete
55	ACL QOS	Destination Port, IPv6 Class	Show Details	Show Rules	Delete
56	Surveillance VLAN	Source MAC	Show Details	Show Rules	Delete
57	Dhcp Server Screening	Source IP, Source Port, Destination Port	Show Details	Show Rules	Delete
58	Zone Defense	Source IP	Show Details	Show Rules	Delete

Current/Max. Profile: 0/50, Current/Max. Rule: 1/200

Figure 5.85 – ACL > ACL Profile List

The contents of Access Profile List table include:

Profile ID: Indicates the profile Identification number. The possible configured profile IDs are 1~50, and profile ID 51 is reserved for Voice VLAN.

Type: The owner type of ACL profile; it can be normal ACL or Voice VLAN.

Profile Summary: Displays the profile summary.

Show Details: To display an ACL's profile details. The ACL profile details are displayed below the ACL table.

Show Rules: To show the access rule in this profile.

Edit / New Rules: To edit or create an access rule in this profile. To add a new rule, please see **Access Rule List** in the next section.

Delete: To delete an access profile.

To manually add a profile, click **Add**:

Figure 5.86 – Add Access Profile

The steps of adding an access profile are described below:

- 1) After selecting the **Profile ID** and **Frame Type** (MAC, IPv4 or IPv6), specify attributes like Untagged/Tagged (for MAC), ICMP/IGMP/TCP/UDP (for IPv4), or ICMP/TCP/UDP (for IPv6). Click **Select** and a simplified frame diagram will be displayed.

Figure 5.87 – Add Access Profile

The 오류! 참조 원본을 찾을 수 없습니다. contains the following fields:

Parameter	Description
Profile ID	Select an unique identifier number for this profile set. This value is from 2 to 50.

Frame Type	Select frame 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. Select MAC ACL to instruct the Switch to examine the layer 2 part of each packet header. Select IPv4 ACL to instruct the Switch to examine the IPv4 address in each frame's header. Select IPv6 ACL to instruct the Switch to examine the IPv6 address in each frame's header. Select Packet Content to instruct the Switch to examine the packet content in each frame's header.
MAC ACL	Defines the ACL profile Layer 2 protocols. The possible values are: Tagged - Defines the profile Layer 2 to match 802.1Q fields in the Layer 2 header. Untagged - Defines the profile Layer 2 to check the Layer 2 header without the 802.1Q fields.
IPv4 ACL	Defines the IPv4 ACL profile protocols. The possible fields are: ICMP - Specifies ICMP as the Layer 4 protocol that the access profile checks. IGMP - Specifies IGMP as the Layer 4 protocol that the access profile checks. TCP - Specifies TCP as the Layer 4 protocol that the access profile checks. UDP - Specifies UDP as the Layer 4 protocol that the access profile checks.
IPv6 ACL	Defines the IPv6 ACL profile protocols. The possible fields are: ICMP — Specifies ICMP as the Layer 3 IPv6 protocol that the access profile checks. TCP — Specifies TCP as the Layer 3 IPv6 protocol that the access profile checks. UDP — Specifies UDP as the Layer 3 IPv6 protocol that the access profile checks.

To define the MAC ACL profile: Select **MAC ACL** with Tagged and click **Select** button. The updates to show the follows:

Add ACL Profile Safeguard

Select Profile ID:

Select Frame Type: ☒ MAC ACL ☐ IPv4 ACL ☐ IPv6 ACL Select

You can select the field in the packet to create filtering mask

MAC Address	802.1Q VLAN	Ether Type	PayLoad
MAC Address ☐ Source MAC Mask Mask Generate ☐ Destination MAC Mask Mask Generate			
802.1Q VLAN ☐ 802.1p ☐ VLAN VID			
Ether Type ☐ Ether Type			

Back Add

Figure 5.88 – Add Access Profile (MAC ACL)

The Add ACL Profile MAC ACL contains the following fields:

Field	Description
Source MAC Mask	Enter a MAC address mask for the source MAC address, e.g. FF-FF-FF-FF-FF-FF.
Destination MAC Mask	Enter a MAC address mask for the destination MAC address, e.g. FF-FF-FF-FF-FF-FF.
802.1p	Selecting this option instructs the Switch to examine the 802.1Q VLAN identifier of each packet header and use this as the full or partial criterion for forwarding.
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.
Ether Type	Selecting this option instructs the Switch to examine the Ethernet type value in each frame's header.

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

To define the IPv4 ACL ICMP profile: Select **IPv4 ACL** with **ICMP** and click **Select** button. The updates to show the follows:

Figure 5.89 – Add Access Profile (IPv4 ACL ICMP)

The Add ACL Profile IPv4 ACL ICMP address page contains the following fields:

Field	Description
Source IP Mask	Defines the range of source IP addresses, relevant to the ACL rules. (0=ignore, 1=check). For example, to set 176.212.XX.XX, use mask 255.255.0.0
Destination IP Mask	Defines the range of destination IP addresses, relevant to the ACL rules. (0=ignore, 1=check). For example, to set 176.212.XX.XX, use mask 255.255.0.0
ICMP Type	Sets the ICMP Type field as an essential field to match.
ICMP Code	Sets the ICMP code field as an essential field to match.

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

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

Add ACL Profile Safeguard

Select Profile ID:

Select Frame Type: ☐ MAC ACL ☒ IPv4 ACL ☐ IPv6 ACL

IGMP

You can select the field in the packet to create filtering mask

L2 Header	IPv4 DSCP	IPv4 Address	IGMP
IGMP ☐ Type			

Figure 5.90 – Add Access Profile (IPv4 ACL IGMP)

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

To define the IPv4 ACL TCP profile: Select **IPv4 ACL** with **TCP** and click **Select** button. The updates to show the follows:

Add ACL Profile Safeguard

Select Profile ID:

Select Frame Type: ☐ MAC ACL ☒ IPv4 ACL ☐ IPv6 ACL

TCP

You can select the field in the packet to create filtering mask

L2 Header	IPv4 DSCP	IPv4 Address	TCP Port	TCP Flag
TCP Port ☐ Source Port Mask Mask Generate ☐ Destination Port Mask Mask Generate TCP Flag ☐ TCP Flag				

Figure 5.91 – Add Access Profile (IPv4 ACL TCP)

The Add ACL Profile IPv4 ACL TCP port page contains the following fields:

Field	Description
Source Port Mask	Defines the range of source Ports relevant to the ACL rules. (0=ignore, 1=check). For example, to set 0 – 15, set mask of FFF0.
Destination Port Mask	Defines the range of destination IP addresses, relevant to the ACL rules. (0=ignore, 1=check). For example, to set 0 – 15, set mask of FFF0.
TCP Flag	Sets the TCP Flag Type field as an essential field to match.

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

To define the IPv4 ACL UDP profile: Select **IPv4 ACL** with **UDP** and click **Select** button. The updates to show the follows:

Figure 5.92 – Add Access Profile (IPv4 ACL UDP)

The Add ACL Profile IPv4 ACL UDP port page contains the following fields:

Field	Description
Source Port Mask	Defines the range of source Ports relevant to the ACL rules. (0=ignore, 1=check). For example, to set 0 – 15, set mask of F.
Destination Port Mask	Defines the range of destination IP addresses, relevant to the ACL rules. (0=ignore, 1=check). For example, to set 0 – 15, set mask of F.

Click **Add** 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 profile: Select **IPv6 ACL** with **ICMP** and click **Select** button. The updates to show the follows:

The screenshot shows the 'Add ACL Profile' window with the following configuration:

- Select Profile ID:** 1
- Select Frame Type:**
 - ☐ MAC ACL
 - ☐ IPv4 ACL
 - ☒ IPv6 ACL
- Protocol:** ICMP
- Select button:** [Select]
- Filtering Mask Selection:**
 - ☐ L2 Header
 - ☒ IPv6 Class
 - ☒ IPv6 Address
 - ☒ ICMP
- IPv6 Class:**
 - ☐ IPv6 Class
- IPv6 Address:**
 - ☐ Source IP Mask: [] [Mask Generate]
 - ☐ Destination IP Mask: [] [Mask Generate]
- ICMP:**
 - ☐ ICMP Type
 - ☐ ICMP Code
- Buttons:** [Back] [Add]

Figure 5.93 – Add Access Profile (IPv6 ACL ICMP)

The Add ACL Profile IPv6 ACL ICMP address page contains the following fields:

Field	Description
Source IP Prefix	Defines the range of source IP addresses, relevant to the ACL rules. (0=ignore, 1=check). For example, to set 2002:0:0:0:0:b0d4:0, use mask 128
Destination IP Prefix	Defines the range of destination IP addresses, relevant to the ACL rules. (0=ignore, 1=check). For example, to set 2002:0:0:0:0:bfd4:0, use mask 128
ICMP Type	Sets the ICMP Type field as an essential field to match.
ICMP Code	Sets the ICMP code field as an essential field to match.

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

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

Figure 5.94 – Add Access Profile (IPv6 ACL TCP)

The Add ACL Profile IPv6 ACL TCP port page contains the following fields:

Field	Description
Source Port Mask	Defines the range of source Ports relevant to the ACL rules. (0=ignore, 1=check). For example, to set 0 – 15, set mask of FFF0.
Destination Port Mask	Defines the range of destination IP addresses, relevant to the ACL rules. (0=ignore, 1=check). For example, to set 0 – 15, set mask of FFF0.

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

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

Figure 5.95 – Add Access Profile (IPv6 ACL UDP)

The Add ACL Profile IPv6 ACL UDP port page contains the following fields:

Field	Description
Source Port Mask	Defines the range of source Ports relevant to the ACL rules. (0=ignore, 1=check). For example, to set 0 – 15, set mask of F.
Destination Port Mask	Defines the range of destination IP addresses, relevant to the ACL rules. (0=ignore, 1=check). For example, to set 0 – 15, set mask of F.

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



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

2) Selecting the field of interest will display the related columns in the lower part of the page. Enter the filtering mask and click **Apply** when done. A filtering mask is to specify the digit that you want to check. For example, if you want to check a network of 192.168.1.0/24, then you should enter the IP mask as 255.255.255.0.



Figure 5.96 – Access Rule List



NOTE: You cannot select Payload in a MAC ACL, or L2 Header in IP ACL.

3) After the **Profile ID** has been created, click **Continue** to go back to the main Access Profile List page, clicking the **Edit / New Rules** button to enter the **Access Rule List** page.

Figure 5.97 – Access Rule List

Profile ID: Indicates the corresponding access profile Identification number.

Access ID: Indicates the access rule Identification number.

Profile Type: Displays the profile type.

Summary: Displays the access rule summary.

Action: Displays the access rule action.

To add a new rule, click **Add**:

Figure 5.98 – Add Access Rule

Profile Information displays the information to which the rule is being added to, including **Profile ID** and **Ether Type**.

In **Rule Detail**, you can specify the details of an access rule. Below are all the possible parameters that can be set.

Access ID: Specify the Access ID (1-65535).

Type: Display the type of rule. MAC, IPv4 or IPv6.

IPv6 Class: Specify the class of IPv6. The range is 0 to 255.

VLAN ID: Specify the VLAN ID.

Destination IPv6 Address: Specify the destination IPv6 address.

Source IPv6 Address: Specify the source IPv6 address.

IP Protocol: Specify the IP protocol of access rule.

Type: Specify the type. The possible value is from 0 to 255.

Code: Specify the code of access rule. The field range is from 0 to 255.

Ports: Specify the switch ports that you want to implement the access rule to.

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 **Apply** to make it effective.



NOTE: The switch begins the access rule with the smallest access ID, so be careful in assigning the ID for the expected results.

To modify an existing rule, please click on the Access ID hyperlink.

Access Rule List					
Safeguard					
Back Add					
Profile ID	Access ID	Type	Summary	Action	Delete
2	2	IPv6	ICMPv6, ICMPv6 Type, ICMPv6 Code, Destination IPv6, Source IPv6, IPv6 class	Permit	Delete

Figure 5.99 – ACL > Access Profile List > Access Rule List

ACL > ACL Finder

This page is used to help find a previously configured ACL entry. To search for an entry, enter the profile ID from the drop-down menu, select a port that you wish to view, define the state and click **Search**. The table on the lower half of the screen will display the entries. To delete an entry click the corresponding **Delete** button.

ACL Finder					
Safeguard					
ACL rule finder helps you identify any rule has been assigned to a specific port					
Profile ID	Any	Ports		Search	
Profile ID	Access ID	Type	Summary	Action	Delete
54	255	IMPB	IP	Deny	Delete

Figure 5.100 – ACL > ACL Finder

PoE > PoE Global Settings (SPN-12080P/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.

PoE Global Settings

PoE Power Threshold (7.1-78.0)

78.0

Watts

Power Shut Off Sequence

Deny next port

Apply

System Power Status

Total PoE Power Budget

78

Power Used

0

Power Left

78

The percentage of system power supplied

0%

1. 7 watts guard band is reserved for system to prevent a PD from being powered off when encountering a sudden increment of PD power supply. When Used Power reaches guard band, a new PD will trigger the action defined in Power Shut Off Sequence.

2. If a sudden increment of a PD power causes PSE power overload, switch will firstly stop power supply to the port with a low priority PD. As a result, high priority PD can work without being affected.

Figure 5.101 – PoE > PoE Global Setting

System Power Threshold: Manually configure the system power budget 7.1 ~ 78.0 watts for SPN-12080P and 7.1 ~ 185.0 watts for SPN-14240P.

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 (SPN-12080P/28P only)

SPN-12080P/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 for port 1~4, meeting IEEE802.3af standards and pre-802.3at standards.

SPN-12080P/28P works with all 802.3af or 802.3at capable devices. The Switch also works in PoE mode with all non-802.3af capable AP, IP Cam and IP phone equipment via the PoE splitter.

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. SPN-12080P/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.

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

Figure 5.102 – 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 SPN-12080P/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 > Trap to SmartConsole Utility

By configuring the Trap Setting, it allows SmartConsole Utility to monitor specified events on this PoE Switch. By default, Trap Setting is disabled. When the Trap Setting is enabled, enter the **Destination IP** address of the managing station that will receive trap information when event happens.

Figure 5.103 – SNMP > Trap to SmartConsole Utility

You can select which event message(s) to be sent to the managing station.

Destination IP: Specifies the destination IP.

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

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.

PoE Power On / Off: Status of power per port (Only for SPN-12080P/28P)

PoE Power Error: The four trap events are: power over loading, short circuit, thermal shutdown and power deny (Only for SPN-12080P/28P).



NOTE: The total PoE power budget is 78 watts for SPN-12080P and 185 watts for SPN-14240P. The remaining 7watts is reserved for the last PoE device to be connected to the switch. The Power Deny trap message is sent out when the switch hits the total power budget and when a new Power Device (PD) requests to connect to the switch at the same time.

PoE Over Max Power Budget: When the system supplies power to PDs and hits the max PoE power budget of 78watts and 185watts, the system will send out this trap message. (Only for SPN-12080P/28P)

SNMP > SNMP > SNMP Global Settings

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

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

The default SNMP global state is disabled. Select Enable and click **Apply** to enable the SNMP function.

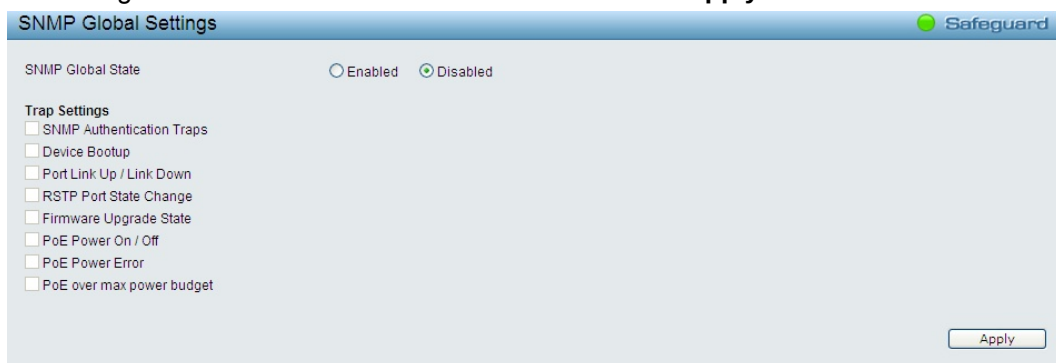


Figure 5.104 – SNMP > SNMP > SNMP Global Settings

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

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

Device Bootup: System boot-up information.

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

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

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

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

PoE Power On / Off: Status of power per port (Only for SPN-12080P/28P)

PoE Power Error: The four trap events are: power over loading, short circuit, thermal shutdown and power deny (Only for SPN-12080P/28P).



NOTE: The total PoE power budget is 78 watts for SPN-12080P and 185 watts for SPN-14240P. The remaining 7watts is reserved for the last PoE device to be connected to the switch. The Power Deny trap message is sent out when the switch hits the total power budget and when a new Power Device (PD) requests to connect to the switch at the same time.

PoE Over Max Power Budget: When the system supplies power to PDs and hits the max PoE power budget of 78 watts and 185 watts, the system will send out this trap message. (Only for SPN-12080P/28P)

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.

SNMP User Table Safeguard

User Name *

Group Name *

SNMP Version

Encrypt

Auth-Protocol Password

Privacy Protocol Password

* indicates mandatory data.

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 5.105 – SNMP > SNMP > SNMP User Table

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

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

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

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

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

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

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

SNMP > SNMP > SNMP Group Table

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

Group Name: 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.

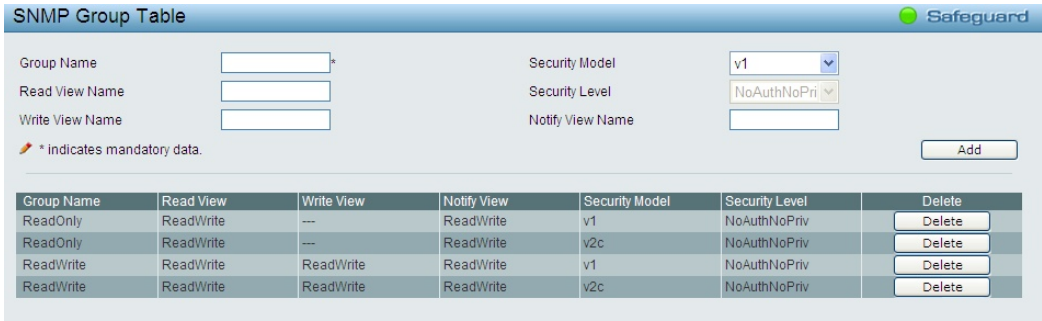
Security Level: This function is only available when you select SNMPv3 security level.

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.



SNMP Group Table Safeguard

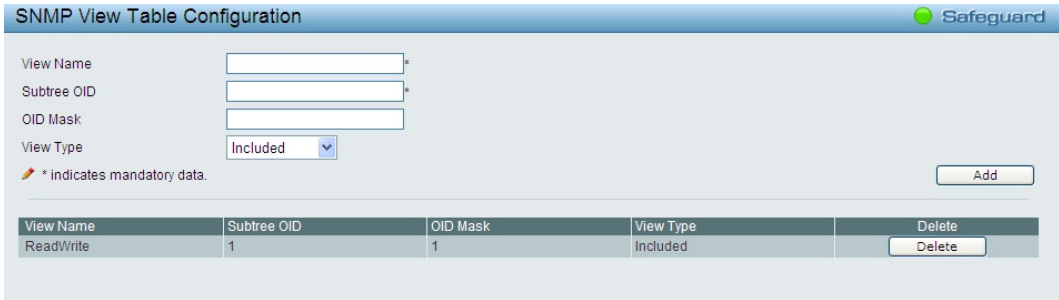
Group Name * Security Model v1
 Read View Name Security Level NoAuthNoPriv
 Write View Name Notify View Name
 * indicates mandatory data. Add

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

Figure 5.106 – SNMP > SNMP > SNMP Group Table

SNMP > SNMP > SNMP View

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



SNMP View Table Configuration Safeguard

View Name *
 Subtree OID *
 OID Mask
 View Type Included
 * indicates mandatory data. Add

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

Figure 5.107 – 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: Name of the community string

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



SNMP Community Table Safeguard

Community Name *
 User Name (View Policy) ReadOnly
 * indicates mandatory data. Add

Community Name	User Name	Delete
public	ReadOnly	Delete
private	ReadWrite	Delete

Figure 5.108 –SNMP > SNMP > SNMP Community

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

SNMP > SNMP > SNMP Host

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



The interface shows the 'SNMP Host Table' configuration page. It includes a 'Safeguard' status indicator. The configuration fields are: 'Host IP Address' (text input), 'SNMP Version' (dropdown menu set to 'V1'), and 'Community String/SNMPv3 User Name' (text input). There are radio buttons for 'IPv4' (selected) and 'IPv6'. An 'Apply' button is located at the bottom right. Below the form is a table with the following columns: 'Host IP Address', 'SNMP Version', 'Community Name/SNMPv3 User Name', and 'Delete'.

Figure 5.109 – 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.

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

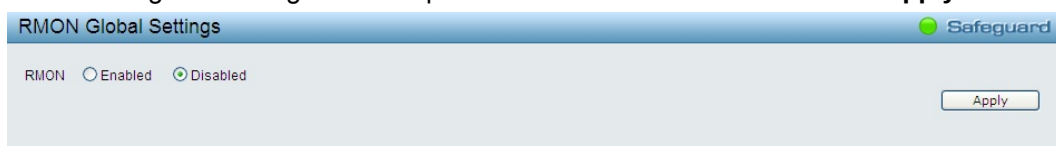


The interface shows the 'SNMP Engine ID' configuration page. It includes a 'Safeguard' status indicator. The 'Engine ID' field contains the value '4447532d313231302d31305000010203040'. There are 'Default' and 'Apply' buttons. A note at the bottom states: 'Engine ID length is 10-64, the accepted character is from 0 to F.'

Figure 5.110 – SNMP > SNMP > SNMP Engine ID

SNMP > RMON > RMON Global Settings

Users can enable and disable remote monitoring (RMON) status for the SNMP function on the Switch. In addition, RMON Rising and Falling Alarm Traps can be enabled and disabled. Click **Apply** to make effects.



The interface shows the 'RMON Global Settings' configuration page. It includes a 'Safeguard' status indicator. The 'RMON' status is set to 'Disabled' (radio button). There is an 'Apply' button at the bottom right.

Figure 5.111 - 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 interface shows the 'RMON Ethernet Statistics Settings' configuration page. It includes a 'Safeguard' status indicator. The configuration fields are: 'Index (1~65535)' (text input), 'Port' (text input), and 'Owner' (text input). There is a note: '* Indicates mandatory data.' and buttons for 'Refresh' and 'Add'. Below the form is a table with the following columns: 'Index', 'Port', 'Drop Events', 'Octets', 'Packets', 'Broadcast Packets', 'Multicast Packets', 'Owner', and 'Delete'.

Figure 5.112 - SNMP > RMON > RMON Ethernet Statistics Configuration

The RMON Ethernet Statistics Configuration contains the following fields:

Index (1 - 65535): Indicates the RMON Ethernet Statistics entry number.

Port: Specifies the port from which the RMON information was taken.

Owner: Displays the RMON station or user that requested the RMON information.

Click **Add** to make the configurations take effects and click **Refresh** to redisplay the table information.

SNMP > RMON > RMON History

The RMON History Control Configuration page contains information about samples of data taken from ports. For example, the samples may include interface definitions or polling periods.

Figure 5.113 - SNMP > RMON > RMON History Control Settings

The History Control Configuration contains the following fields:

Index (1 - 65535): Indicates the history control entry number.

Port: Specifies the port from which the RMON information was taken.

Buckets Requested (1 ~ 50): Specifies the number of buckets that the device saves.

Interval (1 ~ 3600): Indicates in seconds the time period that samplings are taken from the ports. The field range is 1-3600. The default is 1800 seconds (equal to 30 minutes).

Owner: Displays the RMON station or user that requested the RMON information.

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

SNMP > RMON > RMON Alarm Settings

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 5.114 -. SNMP > RMON > RMON Alarm Settings

The configuration contains the following fields:

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

Variable: Specify the selected MIB variable value.

Rising Threshold (0 ~ 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 ~ 2³¹-1): 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 ~ 2³¹-1): 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 5.115 - SNMP > RMON > RMON Event Settings

The RMON Events Page contains the following fields:

Index (1~ 65535): Displays the event.

Description: Specifies the user-defined event description.

Type: Specifies the event type. The possible values are:

None – Indicates that no event occurred.

Log – Indicates that the event is a log entry.

SNMP Trap – Indicates that the event is a trap.

Log and Trap – Indicates that the event is both a log entry and a trap.

Community: Specifies the community to which the event belongs.

Owner: Specifies the time that the event occurred.

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

Monitoring > Port Statistics

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

Port	TxOK	RxOK	TxError	RxError
01	30786	134754	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

Figure 5.116 – Monitoring > Port Statistics

Refresh: Renews the details collected and displayed.

Clear: To reset the details displayed.

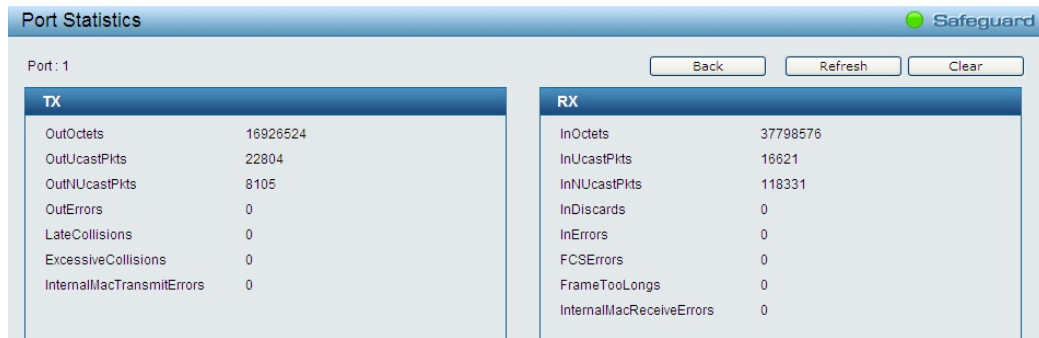
TxOK: Number of packets transmitted successfully.

RxOK: Number of packets received successfully.

TxError: Number of transmitted packets resulting in error.

RxError: Number of received packets resulting in error.

To view the statistics of individual ports, click one of the linked port numbers for details.



Port Statistics		Safeguard	
Port: 1			
TX		RX	
OutOctets	16926524	InOctets	37798576
OutUcastPkts	22804	InUcastPkts	16621
OutNUcastPkts	8105	InNUcastPkts	118331
OutErrors	0	InDiscards	0
LateCollisions	0	InErrors	0
ExcessiveCollisions	0	FCSErrors	0
InternalMacTransmitErrors	0	FrameTooLongs	0
		InternalMacReceiveErrors	0

Figure 5.117 – Monitoring > Port Statistics

Back: Go back to the Statistics main page.

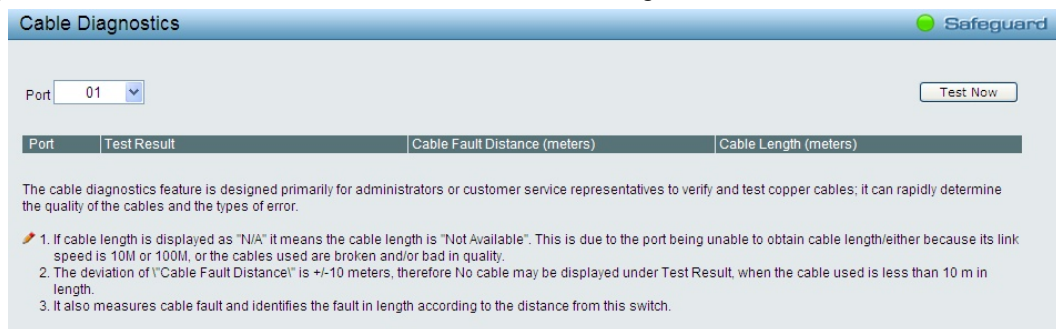
Refresh: To renew the details collected and displayed.

Clear: To reset the details displayed.

Monitoring > Cable Diagnostics

The Cable Diagnostics is designed primarily for administrators and customer service representatives to examine the copper cable quality. It rapidly determines the type of cable errors occurred in the cable.

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



Cable Diagnostics Safeguard

Port: 01 [v] [Test Now]

Port	Test Result	Cable Fault Distance (meters)	Cable Length (meters)
The cable diagnostics feature is designed primarily for administrators or customer service representatives to verify and test copper cables; it can rapidly determine the quality of the cables and the types of error. 1. If cable length is displayed as "N/A" it means the cable length is "Not Available". This is due to the port being unable to obtain cable length/either because its link speed is 10M or 100M, or the cables used are broken and/or bad in quality. 2. The deviation of "Cable Fault Distance" is +/-10 meters, therefore No cable may be displayed under Test Result, when the cable used is less than 10 m in length. 3. It also measures cable fault and identifies the fault in length according to the distance from this switch.			

Figure 5.118 – Monitoring > Cable Diagnostic

Test Result: The description of the cable diagnostic results.

- **OK** means the cable is good for the connection.
- **Short in Cable** means the wires of the RJ45 cable may be in contact somewhere.
- **Open in Cable** means the wires of RJ45 cable may be broken, or the other end of the cable is simply disconnected.
- **Test Failed** means some other errors occurred during cable diagnostics. Please select the same port and test again.

Cable Fault Distance (meters): Indicates the distance of the cable fault from the Switch port, if the cable is less than 2 meters, it will show "No Cable".

Cable Length (meter): If the test result shows OK, then cable length will be indicated for the total length of the cable. The cable lengths are categorized into four types: <50 meters, 50~80 meters, 80~100 meters and >100 meters.



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

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

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.

ID	Time	Log Description	Severity
1	Jan 2 05:18:41 2012	Successful login through Web (IP: 10.0.0.106)	info
2	Jan 2 05:05:29 2012	Logout through Web(IP: 10.0.0.106)	info
3	Jan 2 05:05:29 2012	Web session timed out (IP: 10.0.0.106)	info
4	Jan 2 04:13:23 2012	Successful login through Web (IP: 10.0.0.106)	info
5	Jan 2 02:05:11 2012	Logout through Web(IP: 10.0.0.106)	info
6	Jan 2 02:05:11 2012	Web session timed out (IP: 10.0.0.106)	info
7	Jan 2 00:52:42 2012	Successful login through Web (IP: 10.0.0.106)	info
8	Jan 1 07:04:33 2012	Logout through Web(IP: 10.0.0.106)	info
9	Jan 1 07:04:33 2012	Web session timed out (IP: 10.0.0.106)	info
10	Jan 1 05:50:46 2012	Successful login through Web (IP: 10.0.0.106)	info
11	Jan 1 05:37:56 2012	Logout through Web(IP: 10.0.0.106)	info
12	Jan 1 05:37:56 2012	Web session timed out (IP: 10.0.0.106)	info
13	Jan 1 04:35:21 2012	Successful login through Web (IP: 10.0.0.106)	info
14	Jan 1 04:33:24 2012	Login failed through Web (IP: 10.0.0.106)	warning
15	Jan 1 04:33:22 2012	Successful login through Web (IP: 10.0.0.106)	info
16	Jan 1 01:55:58 2012	Logout through Web(IP: 10.0.0.106)	info
17	Jan 1 01:55:58 2012	Web session timed out (IP: 10.0.0.106)	info
18	Jan 1 00:18:13 2012	Successful login through Web (IP: 10.0.0.106)	info
19	Jan 1 00:00:07 2012	System started up	critical
20	Jan 1 00:00:02 2012	Port 1 link up, 1Gbps FULL duplex	info

Figure 5.119 – 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.

6 Command Line Interface

The SAMSUNG PoE 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 login 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 (**SPN-14240P>**):

```
SPN-14240P login: admin
Password:
SPN-14240P>
```

Figure 6.1 – Command Prompt

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

CLI Commands:

The Basic Switch commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
?	
download	{ firmware_fromTFTP cfg_fromTFTP } {<ipaddr> <ipv6addr>} <path_filename>
Upload	{ firmware_fromTFTP cfg_fromTFTP } {<ipaddr> <ipv6addr>} <path_filename>
config ipif system	{ ipaddress <ip-address> <subnet-mask> gateway <gw-address> dhcp bootp }
config ipif system	{ ipv6 ipv6address <ipv6networkaddr> dhcpv6_client [enable disable] }
logout	
ping	<ip_addr>
ping6	<ipv6addr>
reboot	
reset config	
show ipif	
show switch	
config account admin password	<passwd>

Command	Parameter
save	
debug info	

Each command is listed in detail, as follows:

?	
Purpose	To display a list of commands.
Syntax	?
Description	The ? command displays a list of commands of the switch.
Parameters	None.
Restrictions	None.

Example usage:

To display a list of commands of the switch:

```
SPN-14240P> ?
USEREXEC commands :
  config account admin password <passwd>
  config ipif System { ipaddress <ip-address> <subnet-mask> gateway <gw-
address> | dhcp }
  debug info
  download { firmware_fromTFTP tftp://ip-address/filename | cfg_fromTFTP
tftp://ip-address/filename }
  logout
  ping <ip_addr>
  reboot
  reset config
  save
  show ipif
  show switch
  upload { firmware_toTFTP tftp://ip-address/filename | cfg_toTFTP tftp://ip-
address/filename }
SPN-14240P>
```

download	
Purpose	To download and install a firmware, boot, or switch configuration file from a TFTP server.
Syntax	download { <i>firmware_fromTFTP</i> <i>cfg_fromTFTP</i> } {<ipaddr> <ipv6addr>} <path_filename>
Description	The download command downloads a firmware, boot, or switch configuration file from a TFTP server.
Parameters	<i>firmware_fromTFTP</i> – Download and install new firmware on the Switch from a TFTP server.

cfg_fromTFTP - Download a switch configuration file from a TFTP server.

<ipaddr> - The IPv4 address of the TFTP server.

<ipv6addr> - The 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.

Restrictions None.

Example usage:

To download a firmware file:

```
SPN-14240P> download firmware_fromTFTP 1.1.1.23 1\dgs_1210-10032.ros
01-Jan-2000 01:19:48 %COPY-I-FILECPY: Files Copy - source URL tftp://1.1.1.23
/1\dgs_1210-10032.ros destination URL Unit all flash://image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
01-Jan-2000 01:22:49 %COPY-W-TRAP:
The copy operation was completed successfully
!
3920460 bytes copied in 00:03:01 [hh:mm:ss]

SPN-14240P>
```



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

upload

Purpose	To upload the firmware file or a Switch configuration file to a TFTP server.
Syntax	upload { firmware_fromTFTP cfg_fromTFTP } {<ipaddr> <ipv6addr>} <path_filename>
Description	The upload command uploads the Switch's current settings to a TFTP server.

Parameters	<i>firmware_toTFTP</i> – Upload the firmware on the Switch from a TFTP server. <i>cfg_toTFTP</i> – Specifies that the Switch's current settings will be uploaded to the TFTP server. <i><ipaddr></i> – The IPv4 address of the TFTP server. <i><ipv6addr></i> – The IPv6 address of the TFTP server. <i><path_filename></i> – The filename of the firmware or switch configuration file on the TFTP server. You need to specify the DOS path if the file is not at the root directory of the TFTP server.
Restrictions	None.

Example usage:

To upload a firmware file:

```
SPN-14240P>upload firmware_toTFTP 1.1.1.23 1\running—config
01-Jan-2000 01:26:11 %COPY-I-FILECPY: Files Copy - source URL
running-config destination URL tftp://1.1.1.23/1\running-config
.....01-Jan-2000 01:26:16 %COPY-W-TRAP: The copy operation was
completed success fully
!
158 bytes copied in 00:00:05 [hh:mm:ss]
SPN-14240P>
```

config ipif system

Purpose	To configure the System IP interface.
Syntax	config ipif system { ipaddress <ip-address> <subnet-mask> gateway <gw-address> dhcp bootp }
Description	The config ipif system command configures the System IP interface on the Switch.
Parameters	<i>ipaddress <ip-address> <subnet-mask></i> – The IP address and subnet mask to be created. Users need to specify the address and mask information using the traditional format (for example, 10.1.2.3/255.0.0.0) <i>gateway <gw-address></i> – The IP address of the router or gateway. <i>dhcp</i> – Allows the selection of the DHCP protocol for the assignment of an IP address to the Switch's System IP interface. <i>bootp</i> – Allows the selection of the BOOTP to the switch.
Restrictions	None.

Example usage:

To configure the IP interface System:

```
SPN-14240P> config ipif System ipaddress 10.48.74.122/8
Success.
SPN-14240P>
```

config ipif system

Purpose	To configure the System IPv6 interface.
Syntax	config ipif system { ipv6 ipv6address <ipv6networkaddr> dhcpv6_client [enable disable] }
Description	The config ipif system command configures the System IPv6 interface on the Switch.
Parameters	<i>ipv6 ipv6address <ipv6networkaddr></i> – Use this parameter to statically assign an IPv6address to this interface. This address should define a host address and a network prefix length. Multiple IPv6 addresses can be configured for a single IP interface. Ex: 3ffe:501:ffff:100::1/64. The /64 represents the prefix length of the IPv6 addresses. <i>dhcpv6_client [enable disable]</i> – Specify the DHCPv6 client to be disabled or enabled.
Restrictions	None.

Example usage:

To configure the IPv6 interface System:

```
SPN-24240P> config ipif System ipv6 ipv6address 3ffe:501:ffff:100::1/64
```

Success.

```
SPN-14240P>
```

logout

Purpose	To log out a user from the Switch's console.
Syntax	logout
Description	The logout command terminates the current user's session on the Switch's console.
Parameters	None.
Restrictions	None.

Example usage:

To terminate the current user's console session:

```
SPN-14240P> logout
```



NOTE: Save your configuration changes before logging out.

ping

Purpose	To test the connectivity between network devices.
Syntax	<ipaddr>
Description	The ping command checks if another IP address is reachable on the network. You can ping the IP address connected to through the managed VLAN (VLAN 1 by default), as long as there is a

	physical path between the switch and the target IP equipment. By default, Switch sends five pings to the target IP.
Parameters	<ipaddr> - The IP address of the host.
Restrictions	None.

Example usage:

To ping the IP address 10.90.90.91:

```
SPN-14240P> ping 10.90.90.91

Reply Received From :10.90.90.91, TimeTaken : 20 msecs
Reply Received From :10.90.90.91, TimeTaken : 20 msecs
Reply Received From :10.90.90.91, TimeTaken : 20 msecs

--- 10.90.90.91 Ping Statistics ---
3 Packets Transmitted, 3 Packets Received, 0% Packets Loss
SPN-14240P>
```

ping6

Purpose	To test the connectivity between network devices.
Syntax	ping6 <ipv6addr>
Description	The pingv6 command checks if another IP address is reachable on the network. You can ping the IP address connected to through the managed VLAN (VLAN 1 by default), as long as there is a physical path between the switch and the target IP equipment. By default, Switch sends five pings to the target IP.
Parameters	<ipv6addr> - The IPv6 address of the host.
Restrictions	None.

Example usage:

To ping the IP address 3000::1:

```
SPN-14240P> ping6 3000 ::1

Reply Received From : 3000 ::1, TimeTaken : 20 msecs
Reply Received From : 3000 ::1, TimeTaken : 20 msecs
Reply Received From : 3000 ::1, TimeTaken : 20 msecs

--- 3000 ::1 Ping Statistics ---
3 Packets Transmitted, 3 Packets Received, 0% Packets Loss
SPN-14240P>
```

reboot

Purpose	To reboot the Switch. If the Switch is a member of a stack, it may be rebooted individually, without affecting the other members of the stack.
---------	--

Syntax	reboot
Description	The reboot command reboots the system. All network connections are terminated and the boot code executes.
Parameters	None.
Restrictions	None.

Example usage:

To restart the Switch:

```
SPN-14240P> reboot
% Device will reboot, please wait a few minutes to re-login.
SPN-14240P>
```

reset config

Purpose	To reset the Switch to the factory default settings.
Syntax	reset config
Description	All configurations will be reset to the default settings.
Parameters	None.
Restrictions	None.

Example usage:

To restore all of the Switch's parameters to their default values:

```
SPN-14240P> reset config
% Device will reboot after reset configuration successfully.

SPN-14240P>
```

show ipif

Purpose	To display the configuration of an IP interface on the Switch.
Syntax	show ipif
Description	The show ipif command displays the current IP address of the switch.
Parameters	None.
Restrictions	None.

Example usage:

To display IP interface settings:

```
SPN-14240P> show ipif

IP Setting Mode      : Static
IP Address           : 10.90.90.90
Subnet Mask          : 255.0.0.0
Default Gateway      : 0.0.0.0
```

```

DHCPv6 Client State      : Disabled
IPv6 Global Unicast Address: 3ffe:501:ffff:100:100::1/64

SPN-14240P>

```

show switch

Purpose	To display information about the Switch.
Syntax	show switch
Description	The show switch command displays the status of the switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the switch information:

```

SPN-14240P> show switch

System Name      :
System Contact   :
System Location  :
System up time    : 0 days, 6 hrs, 32 min, 17 secs
System Time      : 02/01/2012 06:32:19
System hardware version : B1
System firmware version : 3.10.006
System boot version  : 1.00.005
System Protocol version : 2.001.004
System serial number : 1MB1733K0000A
MAC Address      : 00-01-02-03-04-05

SPN-14240P>

```

config account admin password

Purpose	To display the configuration of an IP interface on the Switch.
Syntax	config account admin password <passwd>
Description	The config account admin password command sets the administrator password.
Parameters	<passwd> – The new password of the administrator.
Restrictions	None.

Example usage:

To configure the account admin password:

```

SPN-14240P> config account admin password 1234

SPN-14240P>

```

save

Purpose	To save changes in the Switch's configuration to non-volatile RAM.
Syntax	save
Description	The save command saves the configuration changes to the memory.
Parameters	None.
Restrictions	None.

Example usage:

To save the Switch's current configuration to non-volatile RAM:

```
SPN-14240P> save
Building configuration ...
[OK]

SPN-14240P>
```

debug info

Purpose	To display the ARP table and MAC FDB information of the Switch.
Syntax	debug info
Description	The debug info command displays the ARP table and MAC FDB of the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the ARP table and MAC FDB information of the Switch:

```
SPN-14240P> debug info
% segmentation fault log file:

File doesn't exist !!!
% ARP table :
```

Address	Hardware Address	Type	Interface	Mapping
-----	-----	----	-----	-----
10.90.90.90	00:18:8b:bf:75:30	ARPA	vlan1	Static
10.90.90.98	00:19:5b:14:3d:c4	ARPA	vlan1	Dynamic
10.255.255.255	ff:ff:ff:ff:ff:ff	ARPA	vlan1	Static

```

% MAC table :
```

Vlan	Mac Address	Type	Ports
-----	-----	-----	-----
1	00:00:00:00:00:26	Learnt	Gi0/7
Total Mac Addresses displayed: 1			
SPN-14240P>			

Appendix A - Ethernet Technology

This chapter will describe the features of the SAMSUNG PoE Switch and provide some background information about Ethernet/Fast Ethernet/Gigabit Ethernet switching technology.

Gigabit Ethernet Technology

Gigabit Ethernet is an extension of IEEE 802.3 Ethernet utilizing the same packet structure, format, and support for CSMA/CD protocol, full duplex, and management objects, but with a tenfold increase in theoretical throughput of over 100-Mbps Fast Ethernet and a hundredfold increase over 10-Mbps Ethernet. Since it is compatible with all 10-Mbps and 100-Mbps Ethernet environments, Gigabit Ethernet provides a straightforward upgrade without wasting existing investments in hardware, software, or trained personnel.

The increased speed and extra bandwidth offered by Gigabit Ethernet is essential in solving network bottlenecks, which frequently develops as more advanced computer users and newer applications continue to demand greater network resources. Upgrading key components, such as backbone connections and servers to Gigabit Ethernet technology, can greatly improve network response times as well as significantly speed up the traffic between subnets.

Gigabit Ethernet enables fast optical fiber connections to support video conferencing, complex imaging, and similar data-intensive applications. Likewise, since data transfers occur 10 times faster than Fast Ethernet, servers outfitted with Gigabit Ethernet NIC's are able to perform 10 times the number of operations in the same amount of time.

In addition, the phenomenal bandwidth delivered by Gigabit Ethernet is the most cost-effective method to take advantage of today and tomorrow's rapidly improving switching and routing internetworking technologies. With expected advances in the coming years in silicon technology and digital signal processing, which will enable Gigabit Ethernet to eventually operate over unshielded twisted-pair (UTP) cabling, a flexible foundation for the next generation of network technology products will be created. This will outfit your network with a powerful 1000-Mbps-capable backbone/server connection.

Fast Ethernet Technology

The growing importance of LANs, and the increasing complexity of desktop computing applications are fueling the need for high performance networks. A number of high-speed LAN technologies have been proposed to provide greater bandwidth and improve client/server response times. Among them, 100BASE-T (Fast Ethernet) provides a non-disruptive, smooth evolution from the current 10BASE-T technology. The non-disruptive and smooth evolution nature, and the dominating potential market base, virtually guarantees cost-effective and high performance Fast Ethernet solutions.

100Mbps Fast Ethernet is a standard specified by the IEEE 802.3 LAN committee. It is an extension of the 10Mbps Ethernet standard with the ability to transmit and receive data at 100Mbps, while maintaining the CSMA/CD Ethernet protocol. Since the 100Mbps Fast Ethernet is compatible with all other 10Mbps Ethernet environments, it provides a straightforward upgrade and utilizes existing investments in hardware, software, and personnel training.

Switching Technology

Another approach to push beyond the limits of Ethernet technology is the development of switching technology. A switch bridges Ethernet packets at the MAC address level of the Ethernet protocol transmitting among connected Ethernet or Fast Ethernet LAN segments.

Switching is a cost-effective way of increasing the total network capacity available to users on a local area network. A switch increases capacity and decreases network loading by dividing a local area network into different segments, which won't compete with each other for network transmission capacity.

The switch acts as a high-speed selective bridge between the individual segments. The switch, without interfering with any other segments, automatically forwards traffic that needs to go from one segment to another. By doing this the total network capacity is multiplied, while still maintaining the same network cabling and adapter cards.

Appendix B - Technical Specifications

Hardware Specifications

Key Components / Performance

- Switching Capacity:
 - SPN-12080P: 20Gbps
 - SPN-14240P: 56Gbps
- Max. Forwarding Rate
 - SPN-12080P: 14.88Mpps
 - SPN-14240P: 41.7Mpps
- Forwarding Mode: Store and Forward
- Packet Buffer memory:
 - SPN-12080P: 1MBytes
 - SPN-14240P: 1MBytes
- DDRII for CPU: 128M Bytes
- Flash Memory: 16M Bytes

Port Functions

- 10/100/1000Base-T ports compliant with the following standards:
 - IEEE 802.3
 - IEEE 802.3u
 - IEEE 802.3ab
 - IEEE 802.3az Energy Efficient Ethernet
 - IEEE 802.3af (SPN-12080P/28P only)
 - IEEE 802.3at (SPN-12080P/28P only)
 - Supports Half/Full-Duplex operations
 - IEEE 802.3x Flow Control support for Full-Duplex mode
 - Auto MDI/MDIX
 - IEEE802.3af Power over Ethernet on Port 1 ~ Port 8 GE ports (SPN-12080P only)
 - IEEE802.3af Power over Ethernet on Port 1~ Port 24 GE ports (SPN-14240P)
 - IEEE802.3at Power over Ethernet on Port 1~Port 8 GE ports (SPN-12080P)
 - IEEE802.3at Power over Ethernet on Port 1~ Port 4 GE ports (SPN-14240P only)
- SFP ports compliant with the following standards:
 - IEEE 802.3z
 - Supports Full-Duplex operations
- SFP transceivers supported
- WDM Transceivers Supported:

Physical & Environment

- AC input, 100~240 VAC, 50/60Hz, internal universal power supply
- Acoustic Value:
 - SPN-12080P/20/28: 0dB (Fan-less)
 - SPN-14240P: 52.2dB (3 Smart Fans)
- Operation Temperature:

- SPN-14240P: 5~50°C
- SPN-12080P: 5~40°C
- Storage Temperature -20~70°C
- Operation Humidity: 0%~95% RH
- Storage Humidity: 0%~95% RH

Emission (EMI) Certifications

- FCC class A
- CE Class A
- VCCI Class A
- IC Class A

Safety Certifications

- cUL, LVD, CE

Features

L2 Features

- Supports up to 16K MAC address
- Supports 256 static MAC
- Jumbo frame: Supports up to 10,000 bytes
- IGMP snooping v1/v2:
 - Supports 256 multicast groups
 - Supports at least 64 static multicast groups
- 802.1D Spanning Tree
- 802.1w Rapid Spanning Tree
- Loopback Detection
- 802.3ad Link Aggregation:
 - SPN-12080P: Supports max 5 groups per device and 8 ports per group
 - SPN-14240P: Supports max 14 groups per device and 8 ports per group
- Port mirroring
- STNP
- LLDP/LLDP-MED
- IPv6 neighbor Discovery (ND)
- L2 Multicast Filtering

VLAN

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

QoS (Quality of Service)

- Priority queue mapping by :
 - 802.1p
 - DSCP
 - ToS
 - TCP/UDP port number
 - IPv6 traffic class
- Up to 4 queues per port

- Supports Strict / WRR mode in queue handling
- Bandwidth Control

AAA

- 802.1X port-based access control
- Support RADIUS server

ACL

- Max 50 ingress ACL profiles
- Ingress ACL rules:
 - SPN-14240P: 200 rules (each rule can be associated to a single port or multiple ports)
- Support different ACL policy packet contents:
 - MAC address
 - Ethernet Type
 - IPv4 address
 - IPv6 address
 - ICMP
 - IGMP
 - TCP/UDP port number

Security

- Trusted Host
- Port Security: Support 64 MAC addresses per port
- Traffic Segmentation
- Safeguard Engine
- Broadcast Storm Control
- ARP Spoofing Prevention: Supports max 64 entries
- DHCP Server Screening: Able to configure 5 IP addresses for DHCP server.
- SSL: Support v1/v2/v3
- Smart Binding
 - Support manual configuration and scanning for binding.
 - Supports ARP packet inspection as default, ARP and IP packet inspection as an option.
 - Supports DHCP Snooping

OAM

- Cable Diagnostics
- Reset button (reset to factory default)

Management

- Web-based GUI
- proprietary CLI
- SNMP support
- DHCP client
- Trap setting for destination IP, system events, fiber port events, twisted-pair port events
- Password access control

- Web-based configuration backup / restoration
- Web-based firmware backup/restore
- Firmware upgrade using Web-based management
- Reset, Reboot

Green Technology

- Power Saving: Enabled by default to save power:
 - By Link Status: Drastically save power when the switch port link is down. For example, no PC connection or the connected PC is powered off.
 - By Cable Length: Detects the length of connected RJ-45 cables and adjusts power usage accordingly without affecting performance. Once the RJ-45 connection is less than 20 meters, the switch will reduce the power instead of full power, which is only needed for 100 meters cables.
 - By LED Shut-Off: LEDs can be turned on/off by port or system through schedule.
 - By Port Shut-Off: Each port on the system can be turned on/off by schedule.
 - By Port Standby: Each port on the system enters sleep state by schedule.
 - By System Hibernation: System enters hibernation by schedule. In this mode, switches save most power since main chipsets (both MAC and PHY) are disabled for all ports, and energy required to power the CPU is minimal.

Appendix C – Rack mount Instructions

Safety Instructions - Rack Mount Instructions - The following or similar rack-mount instructions are included with the installation instructions:

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

B) Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

C) Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

D) Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

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