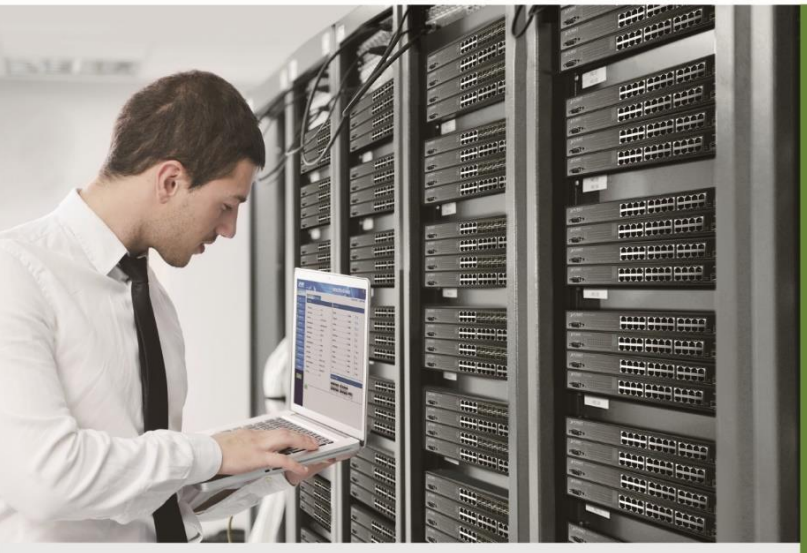
PLANET
Networking & Communication

User's Manual

Multiple Gigabit + 2-Port 1000X SFP Web Smart Ethernet Switch

GS-2210 Web Smart Ethernet Switch Series



www.PLANET.com.tw

Trademarks

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose. PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.

Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements to this User's Manual and/or to the products described in this User's Manual, at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

FCC Warning

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

CE Mark Warning

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

Energy Saving Note of the Device

This power required device does not support Standby mode operation. For energy saving, please remove the power cable to disconnect the device from the power circuit. In view of saving the energy and reducing the unnecessary power consumption, it is strongly suggested to remove the power connection for the device if this device is not intended to be active.

WEEE Warning

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Revision

PLANET GS-2210 Series User's Manual

Models: GS-2210-8T2S, GS-2210-8P2S, GS-2210-16T2S, GS-2210-16P2S, GS-2210-24T2S, GS-2210-24P2S

Revision: 1.0 (Jul, 2024)

Part No: EM-GS-2210 Series_v1.0

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Packet Contents

Thank you for purchasing **Gigabit Web Smart Ethernet Switch**, GS-2210 series. The descriptions of these models are as follows:

Model	Description
GS-2210-8P2S	8-Port 10/100/1000T 802.3at PoE + 2-Port 1000X SFP Web Smart Ethernet Switch (120W)
GS-2210-16P2S	16-Port 10/100/1000T 802.3at PoE + 2-Port 1000X SFP Web Smart Ethernet Switch (240W)
GS-2210-24P2S	24-Port 10/100/1000T 802.3at PoE + 2-Port 1000X SFP Web Smart Ethernet Switch (260W)
GS-2210-8T2S	8-Port 10/100/1000T + 2-Port 1000X SFP Web Smart Ethernet Switch
GS-2210-16T2S	16-Port 10/100/1000T + 2-Port 1000X SFP Web Smart Ethernet Switch
GS-2210-24T2S	24-Port 10/100/1000T + 2-Port 1000X SFP Web Smart Ethernet Switch

Unless specified, "**Web Smart Ethernet Switch**" mentioned in this Quick Installation Guide refers to the GS-2210 series.

Open the box of the **Web Smart Ethernet Switch** and carefully unpack it. The box should contain the following items:

Item / Model	Quick Installation Guide Sheet	Rack-mount Accessory Kit	SFP Dust Cap	AC Power Cord	Rubber Feet
GS-2210-8P2S	■	■	2	1	4
GS-2210-16P2S	■	■	2	1	4
GS-2210-24P2S	■	■	2	1	4
GS-2210-8T2S	■	■	2	1	4
GS-2210-16T2S	■	■	2	1	4
GS-2210-24T2S	■	■	2	1	4

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

1.2 Product Description

NMS is Integrated to Improve Network Management Efficiency

PLANET GS-2210 smart Ethernet switch combined with **NMS** makes network management easier and more efficient. In addition, it is easy to configure whatever application that the industry needs. It features link aggregation, IGMP, QoS, PoE schedule and more to improve the availability of critical business applications.

The GS-2210 PoE+ series provides **8~24 10/100/1000BASE-T** ports featuring **32-watt 802.3at PoE+** and **2 additional Gigabit SFP** slots. With a total power budget of up to **120~260 watts** for different kinds of PoE applications, it provides a quick, safe and cost-effective Power over Ethernet network solution for small businesses and enterprises.

Through the **NMS**, administrators can centrally manage networks of up to **102,400 nodes** from a central office, thereby greatly improving network and power management efficiency. With its user authentication management, combined with the **NMS**, the security of data transmission in modern factory automation systems is enhanced.

The hardware specifications of these models are shown below:

Models	10/100/1000T Copper	100/1000X SFP	PoE Ports	PoE Budget	Power Input
GS-2210-8T2S	8	2	--	--	AC 100~240V, 50/60Hz
GS-2210-16T2S	16	2	--	--	
GS-2210-24T2S	24	2	--	--	
GS-2210-8P2S	8	2	8at	120w	
GS-2210-16P2S	16	2	16at	240w	
GS-2210-24P2S	24	2	24at	260w	

UNI-NMS Remote Management Solution

The GS-2210 series supports PLANET's Universal Network Management System (UNI-NMS) that helps IT staff by remotely managing all network devices and monitoring PDs' operational statuses. Thus, they're designed for both the enterprises and industries where deployments of PDs can be as remote as possible, without having to go to the actual location once a bug or faulty condition is found. With the UNI-NMS, all kinds of businesses can now be speedily and efficiently managed from one platform.

Powerful NMSViewerPro Solution that Meets Evolving Network Management Challenges

The GS-2210 Web Smart Switch series, known for such features as QoS, Link aggregation, PoE, VLANs, IGMP, and so on, provides an eye-catching feature called NMS developed by PLANET to easily and remotely manage and monitor network devices in the local environment from mobile app. This feature not only improves operational convenience, but also ensures users have real-time control over their network infrastructure. It provides users with an unparalleled experience.

The intuitive interface of the local NMSViewerPro allows administrators to easily perform a variety of tasks, including monitoring traffic, setting configuration, troubleshooting, and more. At the same time, PLANET UNI-NMS application provides real-time alerts and notifications, allowing administrators to respond to any emergency situations anytime, anywhere to ensure the stable operation of the network.

The introduction of this feature demonstrates our sensitivity to user needs and our commitment to providing a comprehensive and powerful solution to meet evolving network management challenges. We firmly believe that this feature of supporting local NMSViewerPro will bring users a more efficient and flexible management experience.

PLANET NMS and NMSViewerPro app, which, with PLANET's free cloud service, allows users to quickly and easily detect, configure, deploy and manage devices remotely. You can just scan the NMS agent's (NMS-500/NMS-1000V) QR code using the mobile application to easily monitor and control the remote network devices via the private cloud.

Built-in Unique PoE Functions for Powered Devices Management

As it is the managed PoE switch for surveillance, wireless and VoIP networks, the GS-2210 PoE+ Series features the following special PoE management functions:

- PD alive check
- PoE schedule
- PoE priority
- PoE power limit
- PoE usage monitoring

Intelligent Powered Device Alive Check

The GS-2210 PoE+ Series can monitor connected PD status in real time via PD alive check function. Once the PD stops working and responding, the GS-2210 PoE+ Series will resume the PoE power and bring the PD back to work. It will greatly enhance the network reliability through the PoE port resetting the PD's power source and reducing administrator management burden.

PoE Schedule for Energy Savings

Under the trend of energy savings worldwide and contributing to environmental protection, the GS-2210 PoE+ Series can effectively control the power supply besides its capability of giving high watts power. The "**PoE schedule**" function helps you to enable or disable PoE power feeding for each PoE port during specified time intervals and it is a powerful function to help SMBs or enterprises save power and money. It also increases security by powering off PDs that should not be in use during non-business hours.

PoE Usage Monitor and Power Control

Through the power usage chart in the web management interface, the GS-2210 PoE+ Series empowers administrators to real-time monitor the power usage status of connected PDs. This capability significantly improves facility management efficiency. Additionally, the switch allows for timely activation or deactivation of PoE ports, providing the ability to power off or reboot connected PDs as needed.

Robust Layer 2 Features

The GS-2210 Series can be programmed for basic switch management functions such as port speed configuration, port aggregation, VLAN, **bandwidth control** and **IGMP snooping**. This switch provides **802.1Q tagged VLAN Protocol** functions. By supporting port aggregation, the GS-2210 Series allows the operation of a high-speed trunk combined with multiple ports, and supports fail-over as well. Also, the Layer 2 protocol included to help discover basic information about neighboring devices on the local broadcast domain.

Flexibility and Long-distance Extension Solution

The two mini-GBIC slots built in the GS-2210 Series support SFP auto-detection and dual speed as it features **100BASE-FX** and **1000BASE-SX/LX SFP** (Small Form-factor Pluggable) fiber transceivers to uplink to backbone switch and monitoring center in long distance. The distance can be extended from 550 meters to 2 kilometers (multi-mode fiber) and up to above 10/20/30/40/50/70/120 kilometers (single-mode fiber or WDM fiber). They are well suited for applications within the enterprise data centers and distributions.

Convenient and Smart ONVIF Devices with Detection Feature

PLANET has newly developed an awesome feature -- ONVIF Support -- which is specifically designed for cooperating with video IP surveillances. From the GS-2210 Series GUI, you just need one click to search and show all of the ONVIF devices via network application. In addition, you can open the Camera web page via the IP address link to get real-time monitoring information and online/offline status through IP camera, and perform PoE restart control from the GS-2210 PoE+ series GUI.

ONVIF management functions:

- Supports PLANET ONVIF IP camera discovery
- A maximum of 24 PLANET ONVIF IP cameras can be powered by one GS-2210 PoE+ switch.
- IP camera MAC address, IP address, port and model name
- Open the camera web page via the IP address hyperlink

1.3 Product Features

➢ **Layer 2 Features**

- Complies with the IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z Gigabit Ethernet standard
- Prevents packet loss flow control
  - IEEE 802.3x pause frame flow control in full-duplex mode
  - Back pressure flow control in half-duplex mode
- High performance Store-and-Forward architecture, broadcast storm control, port loopback detection
- 8K MAC address table, automatic source address learning and aging
- Supports VLAN
  - IEEE 802.1Q tag-based VLAN
- Supports Link Aggregation
  - Maximum 8 trunk groups, up to 8 ports per trunk group
  - Cisco ether-channel (static trunk)
- Port mirroring to monitor the incoming or outgoing traffic on a particular port (many-to-1)
- Provides port mirror (many-to-1)

➢ **Quality of Service**

- 8 priority queues on all switch ports
- Support for strict priority and WRR (Weighted Round Robin) CoS policies
- Traffic classification
  - IEEE 802.1p CoS/ToS
  - IPv4 DSCP
  - Port-based WRR
- Strict priority and WRR CoS policies

➢ **Multicast**

- Supports IPv4 IGMP snooping v1, v2
- IGMP snooping port filtering
  - Flood/Drop
  - DIP Mode

➢ **Security**

- Supports DHCP snooping

➢ **Management**

- Management IP for IPv4
- Switch Management Interface
  - Telnet Command Line Interface
  - Web switch management
- BOOTP and DHCP for IP address assignment
- Cable diagnostics to detect the cable connection and the approximate location of the cable fault.
- Firmware upload/download via TFTP or HTTP Protocol for IPv4
- Supports ping test function for IP address or domain name
- NTP (Network Time Protocol)
- PLANET Smart Discovery Utility for deployment management
- PLANET NMS for deployment management
- PLANET NMSViewerPro for deployment management

➢ **Power over Ethernet**

- Complies with IEEE 802.3at/af Power over Ethernet Plus
- Up to 24 ports of IEEE 802.3af/802.3at devices powered
- Supports PoE power up to 32 watts for each PoE port
- Maximum 120~260-watt PoE budget
- Auto detects powered device (PD)
- Circuit protection prevents power interference between ports
- Remote power feeding up to 100 meters in standard mode and 250m in extend mode
- PoE management
  - Total PoE power budget control
  - Per port PoE function enable/disable
  - PoE port power feeding priority
  - Per PoE port power limitation
  - PD classification detection
- Intelligent PoE features
  - PD alive check
  - PoE schedule

1.4 Product Specifications

Product	GS-2210-8T2S	GS-2210-8P2S	GS-2210-16T2S	GS-2210-16P2S	GS-2210-24T2S	GS-2210-24P2S
Hardware Specifications						
10/100/1000 RJ45 Ports	8	8	16	16	24	24
100/1000BASE-X SFP Ports	2	2	2	2	2	2
Flash Memory	16Mbytes					
Reset Button	< 10 sec: System reboot > 10 sec: Factory default					
ESD Protection	Contact ±6KV , Air ±8KV					
Surge Protection	Differential mode ±2KV , Common mode ±4KV					
Dimensions (W x D x H)	220 x 150 x 44mm		440 x 207 x 44mm		440 x 207 x 44mm	
Weight	1033g	1235g	2368g	2343g	2049g	2500g
Power Consumption	16.4 watts/55.9 BTU	5 watts / 17BTU (System) 130 watts/ 443.3 BTU (System+PoE)	12.7 watts/ 43.3 BTU	7.1 watts / 24.2BTU (System) 283 watts/ 965BTU (System+PoE)	16.4 watts/55.9BTU	9.4watts/ 32BTU (System) 297 watts/ 1012 BTU (System+PoE)
Power Requirements	AC 100~240V, 50/60Hz	AC 100~240V, 50/60Hz	AC 100~240V, 50/60Hz	AC 100~240V, 50/60Hz	AC: 100~240V, 50/60Hz	AC 100~240V, 50/60Hz
Fan	--	1	--	2	--	2
LED	**System:** PWR (Green)	**System:** PWR (Green)	**System:** PWR (Green)	**System:** PWR (Green), **PoE Usage 80%** (Green)	**System:** PWR (Green)	**System:** PWR (Green), **PoE Usage 80%** (Green)
	Ports: LNK/ACT (Green)	**Ports:** LNK/ACT (Green) PoE-in-Use (Amber)	**Ports:** LNK/ACT (Green)	**Ports:** LNK/ACT (Green) PoE-in-Use (Amber)	**Ports:** LNK/ACT (Green)	**Ports:** LNK/ACT (Green) PoE-in-Use (Amber)
Switching Specifications						
Switch Architecture	Store-and-forward					
Switch Fabric	20Gbps/non-blocking		36Gbps/non-blocking		52Gbps/non-blocking	
Switch Throughput	14.88Mpps		26.78Mpps		38.68Mpps	
Address Table	8K MAC address table with auto-learning, auto-aging					
Shared Data Buffer	4.1MB					
Jumbo Frame	10KBytes					
Flow Control	Back pressure for half duplex IEEE 802.3x pause frame for full duplex					
Power over Ethernet Specifications						
PoE Standard	--	IEEE 802.3at PoE+ PSE	--	IEEE 802.3at PoE+ PSE	--	IEEE 802.3at PoE+ PSE
PoE Power Supply Type	--	End-span	--	End-span	--	End-span
PoE Power Output	--	32W (max.)	--	32W (max.)	--	32W (max.)

Power Pin Assignment	--	1/2(+), 3/6(-)	--	1/2(+), 3/6(-)	--	1/2(+), 3/6(-)
PoE Power Budget	--	120 watts (max.)	--	240 watts (max.)	--	260 watts (max.)
Layer 2 Functions						
Port Configuration	EEE Green energy savings disable/enable Port disable/enable/reboot Flow control disable/enable Bandwidth control on each port Port loopback protection					
Port Status	Display each port's speed duplex mode, Display link status Display flow control status Display auto negotiation status Display Green energy saving status					
Port Mirroring	In / Out / All Many-to-1 monitor					
VLAN	802.1Q tagged VLAN, up to 16 VLAN groups					
Bandwidth Control	TX/RX/Both					
Link Aggregation	static trunk Supports 8 groups with 8 ports per trunk group					
QoS	8 priority queues on all switch ports Supports strict priority and Weighted Round Robin (WRR) CoS policies Traffic classification: - IEEE 802.1p CoS/ToS - IPv4 DSCP - Port-based WRR					
Multicast	IPv4 IGMP v1/v2 snooping Up to 256					
Security Functions						
Security	Port isolation DHCP Snooping					
Switch Management Functions						
System Configuration	Telnet, Web browser					
Management	Authentication for IPv4 Telnet user name and password Telnet Cable diagnostics IP address or domain name Ping Test NTP (Network Time Protocol) PLANET Smart Discovery Utility PLANET NMS PLANET NMSViewerPro					
Standard Conformance						
Regulatory Compliance	FCC Part 15 Class A, CE					

Standards Compliance	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3z Gigabit 1000BASE-SX/LX IEEE 802.3ab Gigabit 1000BASE-T IEEE 802.3x flow control and back pressure IEEE 802.1p Class of Service IEEE 802.1Q VLAN tagging IEEE 802.3af Power over Ethernet IEEE 802.3at Power over Ethernet PLUS RFC 783 TFTP RFC 791 IP RFC 792 ICMP RFC 2068 HTTP RFC 1112 IGMP v1 RFC 2236 IGMP v2
Environment	
Operating	Temperature: 0 ~ 50 degrees C Relative Humidity: 5 ~ 90% (non-condensing)
Storage	Temperature: -10 ~ 70 degrees C Relative Humidity: 5 ~ 90% (non-condensing)

2. INSTALLATION

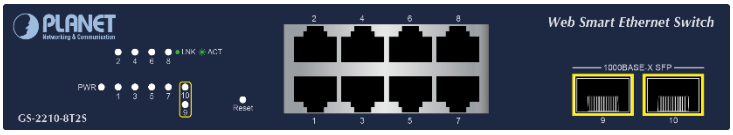
This section describes the hardware features and installation of the Web Smart Ethernet Switch on the desktop or rack mount. For easier management and control of the Web Smart Ethernet Switch, familiarize yourself with its display indicators, and ports. Front panel illustrations in this chapter display the unit LED indicators. Before connecting any network device to the Web Smart Ethernet Switch, please read this chapter completely.

2.1 Hardware Description

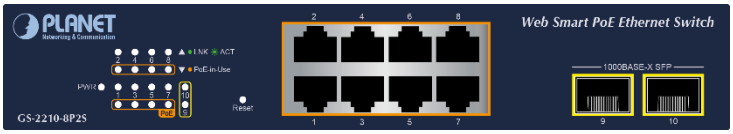
2.1.1 Switch Front Panel

The front panel provides a simple interface monitoring the Web Smart Ethernet Switch. Are show the front panels of the Web Smart Ethernet Switches as belwo.

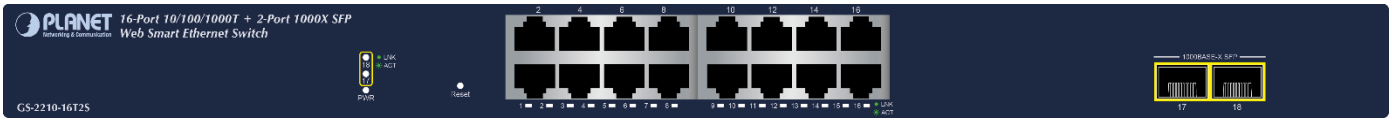
GS-2210-8T2S Front Panel



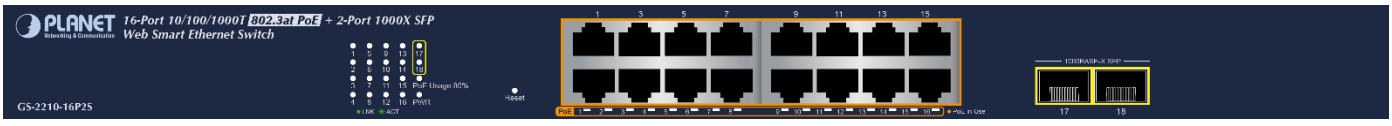
GS-2210-8P2S Front Panel



GS-2210-16T2S Front Panel



GS-2210-16P2S Front Panel



GS-2210-24T2S Front Panel

GS-2210-24P2S Front Panel

■ 10 Gigabit TP interface

8~24 10/100/1000BASE-T Gigabit RJ45 copper ports

■ 10 Gigabit SFP+ slot

2 100/1000BASE-X mini-GBIC/SFP slots

■ Reset button

The front panels of the GS-2210 come with a reset button designed for rebooting the Web Smart Ethernet Switch without turning off and on the power. The following is the summary table of reset button functions:

Reset Button Pressed and Released	Function
< 10 sec: System Reboot	Reboot the Web Smart Ethernet Switch.
> 10 sec: Factory Default	Reset the Web Smart Ethernet Switch to Factory Default configuration. The Web Smart Ethernet Switch will then reboot and load the default settings as shown below: ◦ Default IP Address: **192.168.0.100** ◦ Default Username: **admin** ◦ Default Password: **sw + the last 6 characters of the MAC ID in lowercase**

Find the MAC ID on your device label. The default password is "sw" followed by the last six lowercase characters of the MAC ID.

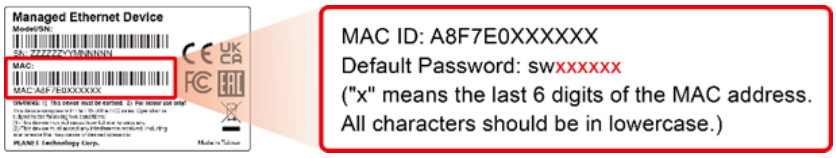


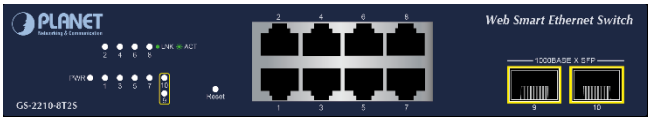
Figure : MAC ID Label

The reset buttons of the GS-2210 are located on the front of their panels.

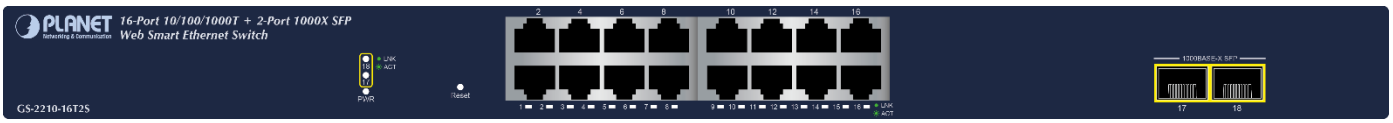
2.1.2 LED Indications

The front panel LEDs indicate instant status of port links, data activity, system operation, system power, and helps monitor and troubleshoot when needed.

GS-2210-8T2S front panel



GS-2210-16T2S Front Panel



GS-2210-24T2S Front Panel

■ **LED Definition**

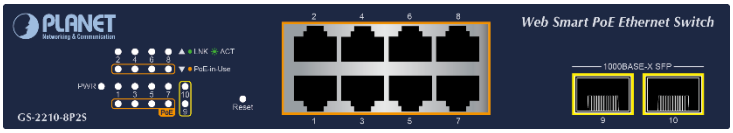
System

LED	Color	Function
PWR	Green	Lights to indicate that the Switch has power.
	Off	Power is off.

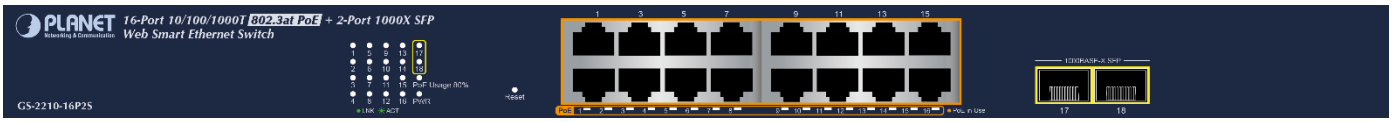
Interfaces

LED	Color	Function	
LNK/ACT	Green	Lights	Indicating the port is running and the connection is successfully established.
		Blinks	Indicating that the switch is actively sending or receiving data over that port.

GS-2210-8P2S Front Panel



GS-2210-16P2S Front Panel



GS-2210-24P2S Front Panel

■ LED Definition

System

LED	Color	Function
PWR	Green	Lights to indicate that the Switch has power.
	Off	Power is off.

Interfaces

LED	Color	Function	
LNK/ACT	Green	Lights	Indicating the port is running and the connection is successfully established.
		Blinks	Indicating that the switch is actively sending or receiving data over that port.
PoE In-Use	Amber	Lights	PD is connected and PoE power supply is normal.
		Off	PD is not connected or PoE power supply is not provided.

2.2 Installing the Switch

This section describes how to install your Web Smart Ethernet Switch and make connections to the Web Smart Ethernet Switch. Please read the following topics and perform the procedures in the order being presented. To install your Web Smart Ethernet Switch on a desktop or shelf, simply complete the following steps.

Note

In the installation steps below, this manual uses the GS-2210-24P2S as an example. However, the steps for GS-2210-8T2S, GS-2210-8P2S, GS-2210-16T2S, GS-2210-16P2S, GS-2210-24T2S is similar.

2.2.1 Desktop Installation

To install the Web Smart Ethernet Switch on desktop or shelf, please follow these steps:

Step 1: Attach the rubber feet to the recessed areas on the bottom of the Web Smart Ethernet Switch.

Step 2: Place the Web Smart Ethernet Switch on the desktop or the shelf near an AC power source, as shown in Figure 2-2-1.

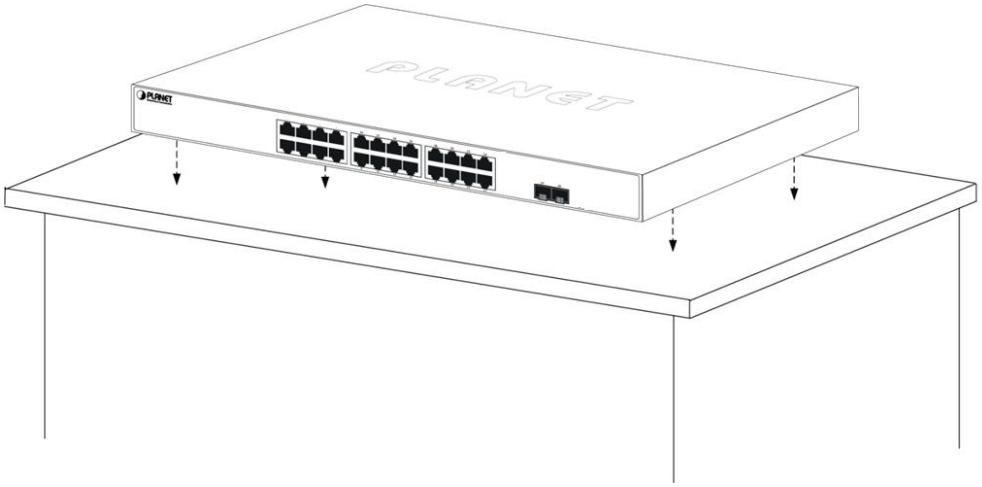


Figure 2-2-1: Place the Web Smart Ethernet Switch on the Desktop

Step 3: Keep enough ventilation space between the Web Smart Ethernet Switch and the surrounding objects.

Note

When choosing a location, please keep in mind the environmental restrictions discussed in Chapter 1, Section 4, and specifications.

Step 4: Connect the Web Smart Ethernet Switch to network devices.

Connect one end of a standard network cable to the 10/100/1G RJ45 ports on the front of the Web Smart Ethernet Switch.

Connect the other end of the cable to the network devices such as printer server, workstation or router.

Note

Connection to the Web Smart Ethernet Switch requires UTP Category 5e network cabling with RJ45 tips. For more information, please see the Cabling Specification in Appendix A.

Step 5: Supply power to the Web Smart Ethernet Switch.

Connect one end of the power cable to the Web Smart Ethernet Switch.

Connect the power plug of the power cable to a standard wall outlet.

When the Web Smart Ethernet Switch receives power, the Power LED should remain solid Green.

2.2.2 Rack Mounting

To install the Web Smart Ethernet Switch in a 19-inch standard rack, please follow the instructions described below.

Step 1: Place the Web Smart Ethernet Switch on a hard flat surface, with the front panel positioned towards the front side.

Step 2: Attach the rack-mount bracket to each side of the Web Smart Ethernet Switch with supplied screws attached to the package.

Figure 2-2-2 shows how to attach brackets to one side of the Web Smart Ethernet Switch.

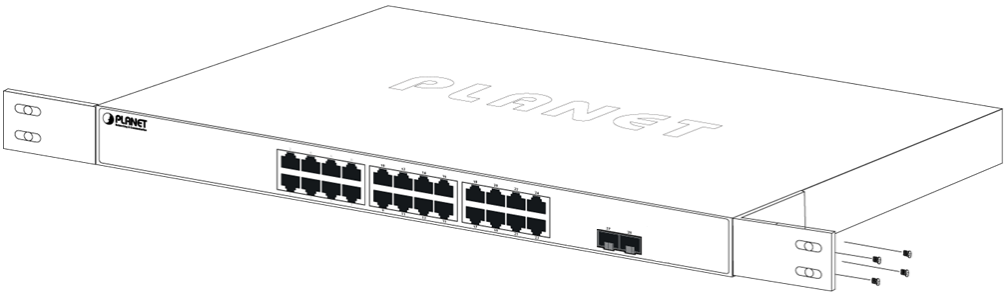


Figure 2-2-2: Attach Brackets to the Web Smart Ethernet Switch.

You must use the screws supplied with the mounting brackets. Damage caused to the parts by using incorrect screws would invalidate the warranty.

Step 3: Secure the brackets tightly.

Step 4: Follow the same steps to attach the second bracket to the opposite side.

Step 5: After the brackets are attached to the Web Smart Ethernet Switch, use suitable screws to securely attach the brackets to the rack, as shown in Figure 2-2-3.

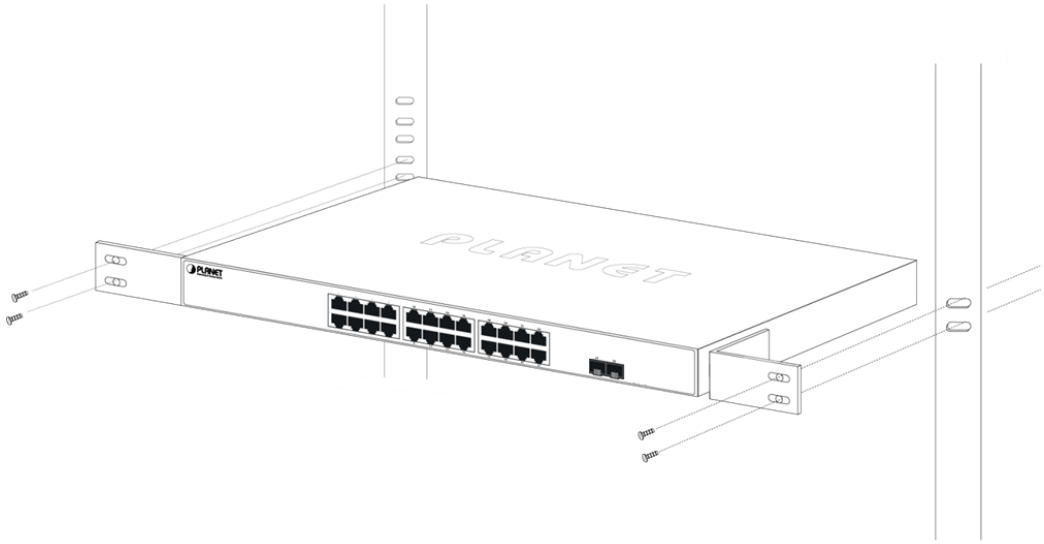


Figure 2-2-3: Mounting Web Smart Ethernet Switch in a Rack

Step 6: Proceed with Steps 4 and 5 of session 2.2.1 Desktop Installation to connect the network cabling and supply power to the Web Smart Ethernet Switch.

2.2.3 Installing the SFP Transceiver

The sections describe how to insert an SFP transceiver into an SFP slot. The SFP transceivers are hot-pluggable and hot-swappable. You can plug in and out the transceiver to/from any SFP port without having to power down the Web Smart Ethernet Switch, as Figure 2-2-4 shows.

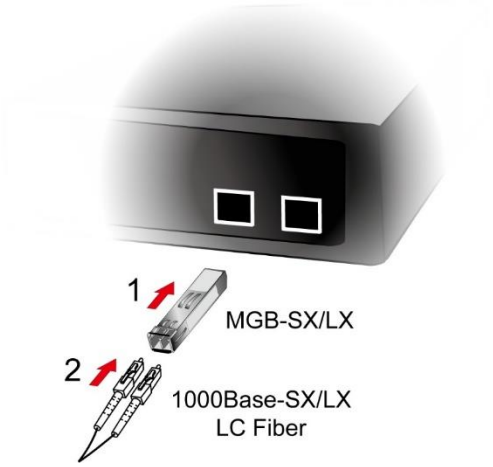


Figure 2-2-4: Plugging in the SFP Transceiver

■ Approved PLANET SFP Transceivers

PLANET Web Smart Ethernet Switch supports both single mode and multi-mode SFP transceivers. The following list of approved PLANET SFP transceivers is correct at the time of publication:

Gigabit Ethernet Transceiver (1000BASE-X SFP)

Ordering Information	
MGB-GT	SFP-Port 1000BASE-T Module
MGB-LX	SFP-Port 1000BASE-LX mini-GBIC module - 20km
MGB-SX	SFP-Port 1000BASE-SX mini-GBIC module - 550m
MGB-SX2	SFP-Port 1000BASE-SX mini-GBIC module - 2km
MGB-L40	SFP-Port 1000BASE-LX mini-GBIC module - 40km
MGB-L80	SFP-Port 1000BASE-LX mini-GBIC module - 80km
MGB-L120	SFP-Port 1000BASE-LX mini-GBIC module - 120km
MGB-LA10	SFP-Port 1000BASE-BX (WDM, TX:1310nm) mini-GBIC module - 10km
MGB-LB10	SFP-Port 1000BASE-BX (WDM, TX:1550nm) mini-GBIC module - 10km
MGB-LA20	SFP-Port 1000BASE-BX (WDM, TX:1310nm) mini-GBIC module - 20km
MGB-LB20	SFP-Port 1000BASE-BX (WDM, TX:1550nm) mini-GBIC module - 20km
MGB-LA40	SFP-Port 1000BASE-BX (WDM, TX:1310nm) mini-GBIC module - 40km
MGB-LB40	SFP-Port 1000BASE-BX (WDM, TX:1550nm) mini-GBIC module - 40km
MGB-LA80	SFP-Port 1000BASE-BX (WDM, TX:1490nm) mini-GBIC module - 80km
MGB-LB80	SFP-Port 1000BASE-BX (WDM, TX:1550nm) mini-GBIC module - 80km

MFB-Series Transceiver (100BASE-FX SFP)

Ordering Information	
MFB-FX	SFP-Port 100BASE-FX Transceiver (1310nm) -2km
MFB-F20	SFP-Port 100BASE-FX Transceiver (1310nm) - 20km
MFB-FA20	SFP-Port 100BASE-BX Transceiver (WDM,TX:1310nm) -20km
MFB-FB20	SFP-Port 100BASE-BX Transceiver (WDM,TX:1550nm) -20km
MFB-F40	SFP-Port 100BASE-FX Transceiver (1310nm) - 40KM
MFB-F60	SFP-Port 100BASE-FX Transceiver (1310nm) - 60KM

It is recommended to use PLANET SFP on the Web Smart Ethernet Switch. If you insert an SFP transceiver that is not supported, the Web Smart Ethernet Switch will not recognize it.

1. Before we connect the GS-2210 to the other network device, we have to make sure both sides of the SFP transceivers are with the same media type, for example, 1000BASE-SX to 1000BASE-SX, 1000BASE-LX to 1000BASE-LX.
2. Check whether the fiber-optic cable type matches with the SFP transceiver requirement.
   - To connect to 1000BASE-SX SFP transceiver, please use the multi-mode fiber cable with one side being the male duplex LC connector type.
   - To connect to 1000BASE-LX SFP transceiver, please use the single-mode fiber cable with one side being the male duplex LC connector type.

■ Connecting the Fiber Cable

1. Insert the duplex LC connector into the SFP transceiver.
2. Connect the other end of the cable to a device with SFP transceiver installed.
3. Check the LNK/ACT LED of the SFP slot on the front of the Web Smart Ethernet Switch. Ensure that the SFP transceiver is operating correctly.
4. Check the Link mode of the SFP port if the link fails. To function with some fiber-NICs or Media Converters, user has to set the port Link mode to "**1000M Force**".

■ Removing the Transceiver Module

1. Make sure there is no network activity anymore.
2. Remove the Fiber-Optic Cable gently.
3. Lift up the lever of the MGB module and turn it to a horizontal position.
4. Pull out the module gently through the lever.

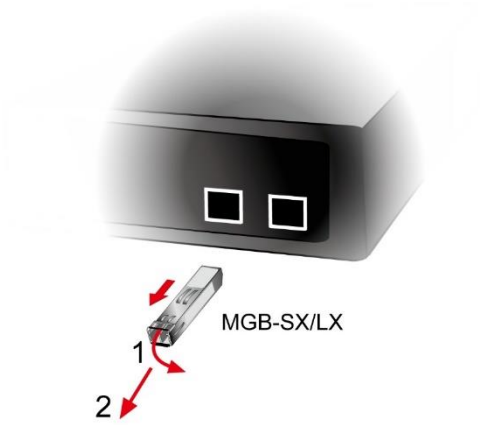


Figure 2-2-5: How to Pull Out the SFP Transceiver

Note

Never pull out the module without lifting up the lever of the module and turning it to a horizontal position. Directly pulling out the module could damage the module and the SFP module slot of the Web Smart Ethernet Switch.

3. SWITCH MANAGEMENT

This chapter explains the methods that you can use to configure management access to the Web Smart Ethernet Switch. It describes the types of management applications and the communication and management protocols that deliver data between your management device (workstation or personal computer) and the system. It also contains information about port connection options.

3.1 Web Management

The Web Smart Ethernet Switch provides a built-in browser interface. You can manage it remotely by having a remote host with Web browser, such as Google Chrome, Mozilla Firefox or Apple Safari.

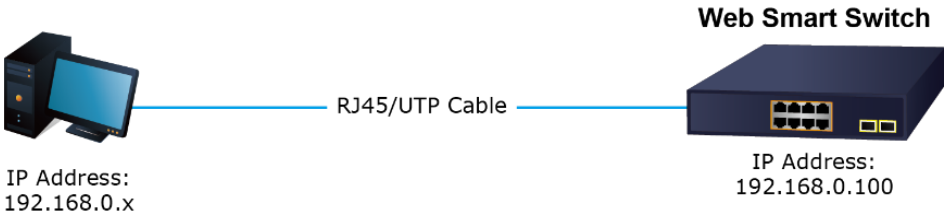


Figure: IP Management Diagram

Note

It is recommended to use Chrome 98.0.xxx or above to access the Web Smart Ethernet Switch. If the Web interface of the Web Smart Ethernet Switch is not accessible, please turn off the anti-virus software or firewall and then try it again.

The following shows how to start up the **Web Management** of the Web Smart Ethernet Switch. Please note the Web Smart Ethernet Switch is configured through an Ethernet connection. Please make sure the manager PC must be set to the same **IP subnet address**.

For example, the IP address of the Web Smart Ethernet Switch is configured with ***192.168.0.100*** on **Interface VLAN 1**, then the manager PC should be set to **192.168.0.x** (where x is a number between 1 and 254, except 100), and the default subnet mask is 255.255.255.0.

Logging in to the Web Smart Ethernet Switch

1. Use Google Chrome or above Web browser and enter IP address ***http://192.168.0. 100*** (that you have just set in console) to access the Web interface.
2. When the following dialog box appears, please enter the configured username and password.

   The factory default user name and password are as follows:

   Default IP of Interface VLAN 1: **192.168.0.100**
   Username: **admin**
   Password: **sw + the last 6 characters of the MAC ID in lowercase**

   Find the MAC ID on your device label. The default password is "sw" followed by the last six lowercase characters of the MAC ID.

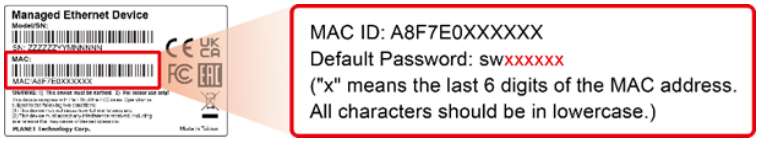


Figure: MAC ID Label

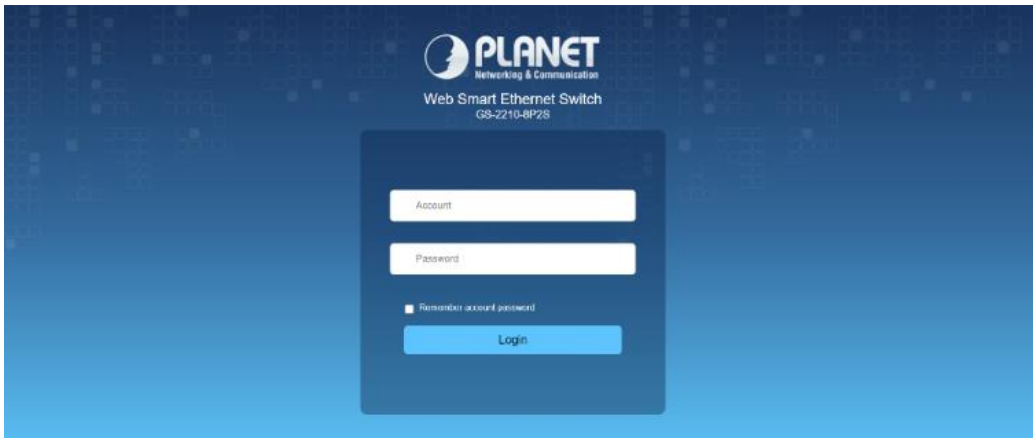


Figure : Login Screen

3. After entering the password, the main screen appears as shown in below.

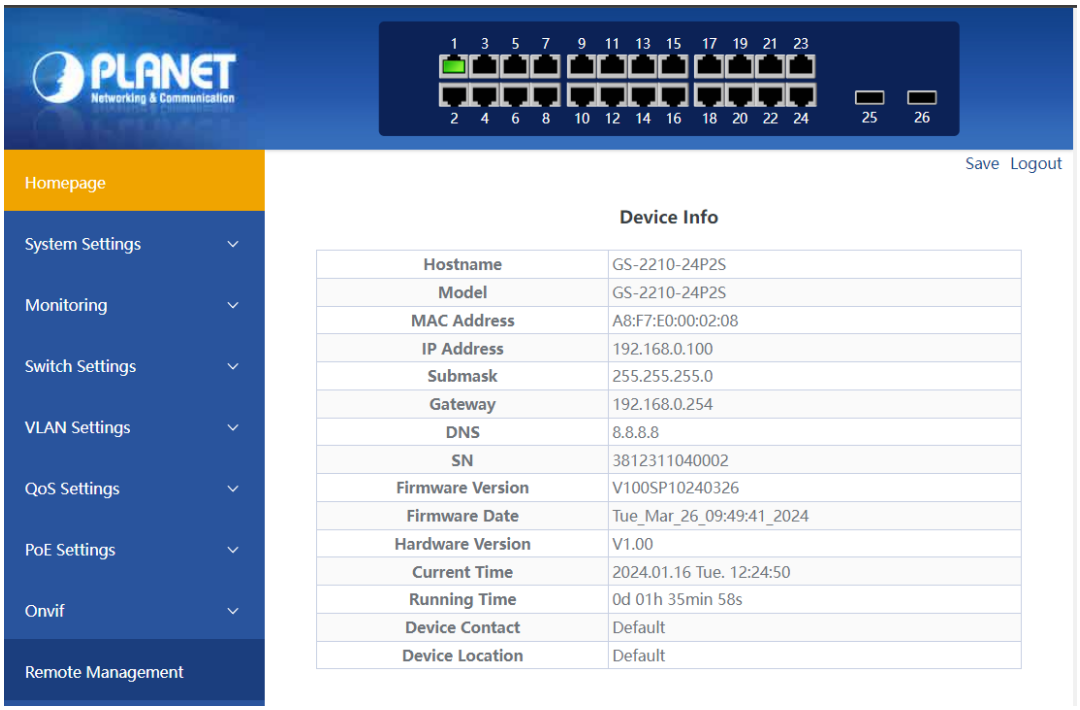


Figure : Web Main Screen of Web Smart Ethernet Switch

4. The Switch Menu on the left of the Web page lets you access all the commands and statistics the Switch provides.

Now, you can use the Web management interface to continue the switch management, please refer to the user manual for more.

3.2 Discovery through PLANET NMS Controller (NMS-500/NMS-1000V)

The GS-2210 Series is the Web Smart Ethernet Switch, which can be centrally monitored by PLANET NMS Controller.

Follow the steps below to discover the Web Smart Ethernet Switch through PLANET NMS controller (NMS-500/NMS-1000V). Please ensure each Web Smart Ethernet Switch uses a different static IP in the same subnet before physically connecting to the managed network.

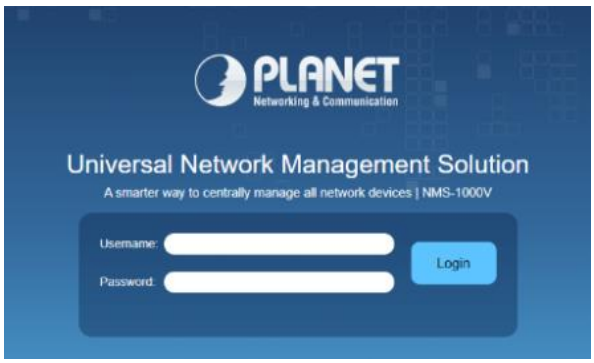
It supports PLANET NMS system and NMSViewerPro app networking feature, which, with PLANET's free cloud service, allows users to quickly and easily detect, configure, deploy and manage devices remotely. Users can just scan the NMS agent's (NMS-500/NMS-1000V) QR code with their mobile devices in order to easily monitor and control the remote network via the private cloud.

Note

1. Please regularly check PLANET website for the latest compatible list of the Web Smart Ethernet Switch in each firmware version.
2. Supports GS-2210 Series Web Smart Ethernet Switch. Please use the versions listed below:
   GS-2210 series: V100SP10240326
   NMS-500: v1.0b240506 (Newer than the last version)
   NMS-1000V-10/12: v1.0b240506 (Newer than the last version)

Step 1. Launch the Web browser (Google Chrome is recommended.) and enter the default IP address https://192.168.1.100:8888 of the NMS controller. Then, enter the default username and password "admin" to log on to the system.

*The secure login with SSL (HTTPS) prefix is required.



Step 2. Go to the "**Domain**" page to discover and add the Web Smart Ethernet Switch to the device list. Then, you can search and add them and go to the **"Device List"** and **"Topology View"** page to monitor the Web Smart Ethernet Switch.

3.3 PLANET NMSViewerPro App (Expected to be launched in April, 2024)

To get PLANET NMSViewerPro app, you can follow the steps below. After it is done, you can now monitor and control your network devices, such as switches, routers, etc., from your iOS or Android based smartphone or tablet.

How to begin

Step 1. Setting the smart phone's Wi-Fi to connect with NMS and internet

Turn on your smart phone's Wi-Fi setting to enable to be connected to the Wi-Fi within the NMS domain and to confirm that the Internet can be accessed normally.

Step 2. Download PLANET NMSViewerPro App

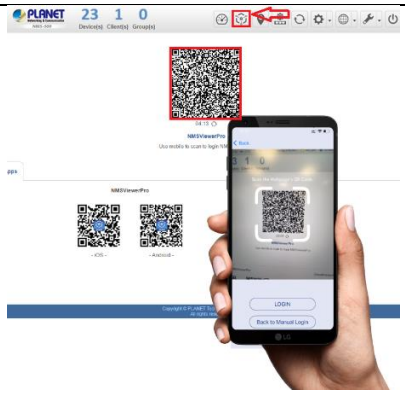
Get the **PLANET NMSViewerPro** App from the Apple App Store or Google play, or simply scan the QR code.

Step 3. First use PLANET NMSViewerPro

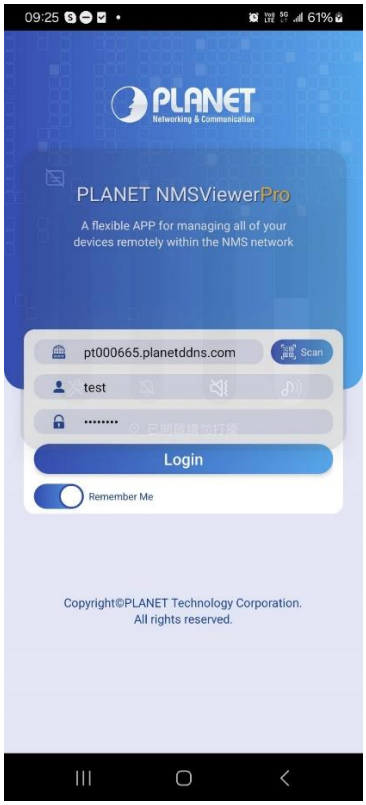
Open the PLANET NMSViewerPro app. You can log in by scanning the NMS-500/1000V QR code or entering the Domain Name/IP address of the NMS equipment provided in the NMS equipment.

2-1. Scan the NMS-500/1000V QR code only (No need to enter any Domain Name/IP address, and account and password), shown in the screen below:

Log in to the NMS and follow the steps below:

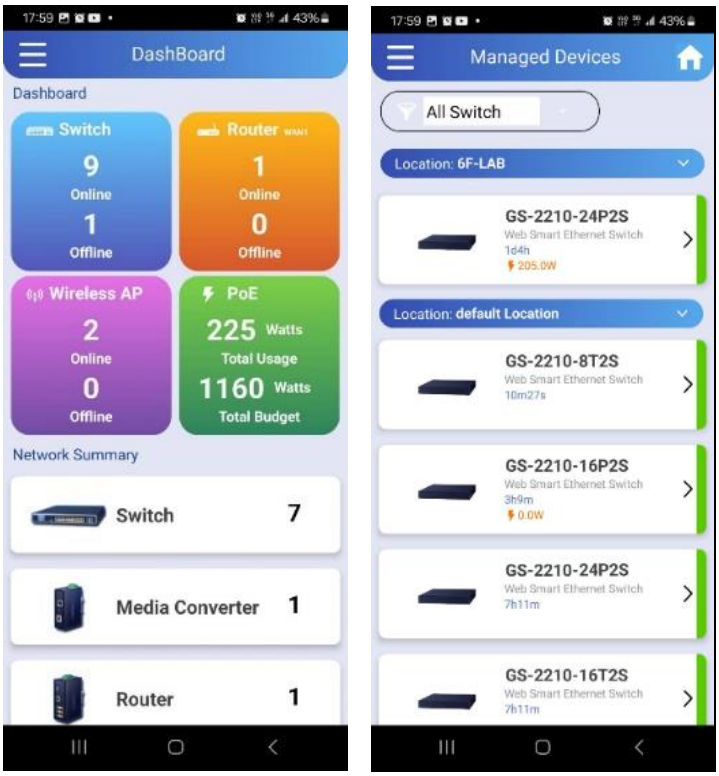
NMS login QR code page	NMSViewerPro scan button
	

2-2. Enter the NMS-500/1000V Domain Name/IP address, and account and password, shown in the screen below:



Step 3. Find your device in Managed Devices list

After logging in the app, you can see the Dashboard and Managed Devices found in the NMS-500/1000V.



3.4 PLANET Smart Discovery Utility

For easily listing the Web Smart Ethernet Switch in your Ethernet environment, the Planet Smart Discovery Utility from user's manual CD-ROM is an ideal solution. The following installation instructions are to guide you to running the Planet Smart Discovery Utility.

1. Deposit the Planet Smart Discovery Utility in administrator PC.
2. Run this utility as the following screen appears.

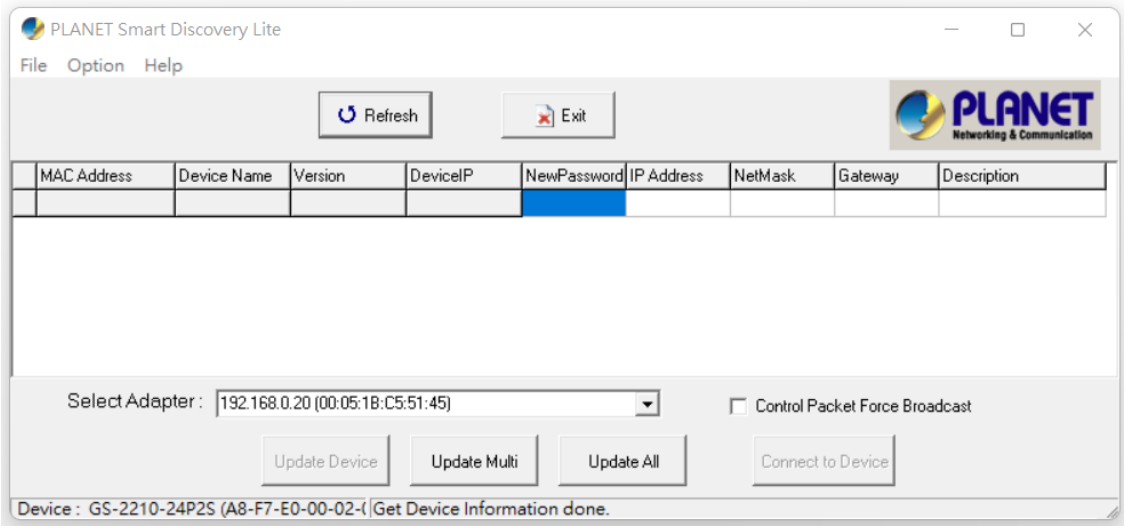


Figure 3-1-6: Planet Smart Discovery Utility Screen

Note

If there are two LAN cards or above in the same administrator PC, choose a different LAN card by using the **"Select Adapter"** tool.

3. Press the **"Refresh"** button for the currently connected devices in the discovery list as the screen shows below:

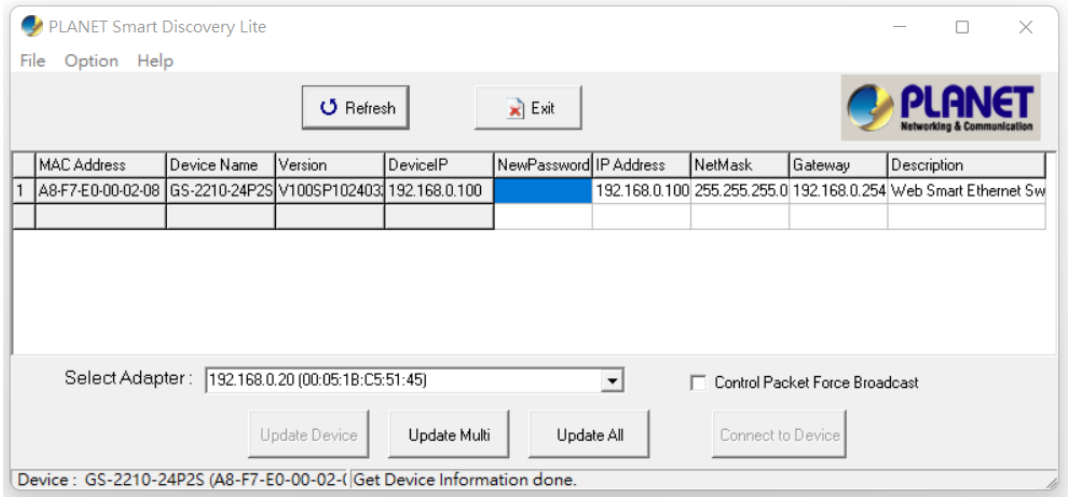


Figure : Planet Smart Discovery Utility Screen

1. This utility shows all necessary information from the devices, such as MAC address, device name, firmware version, and device IP subnet address. It can also assign new password, IP subnet address and description to the devices.

2. After setup is completed, press the "**Update Device**", "**Update Multi**" or "**Update All**" button to take effect. The functions of the 3 buttons above are shown below:
   - **Update Device**: use current setting on one single device.
   - **Update Multi:** use current setting on choose multi-devices.
   - **Update All:** use current setting on whole devices in the list.

   The same functions mentioned above also can be found in "**Option**" tools bar.

3. To click the "**Control Packet Force Broadcast**" function, it allows you to assign a new setting value to the Web Smart Switch under a different IP subnet address.

4. Press the "**Connect to Device**" button and the Web login screen appears.

5. Press the "**Exit**" button to shut down the Planet Smart Discovery Utility.

4. Web-based Management

This section introduces the configuration and functions of the Web-based management from Web Smart Ethernet Switch.

Logging in to the Web Smart Ethernet Switch Please refer to Chapter 3.1

After entering the username and password, the main screen appears as shown in below.

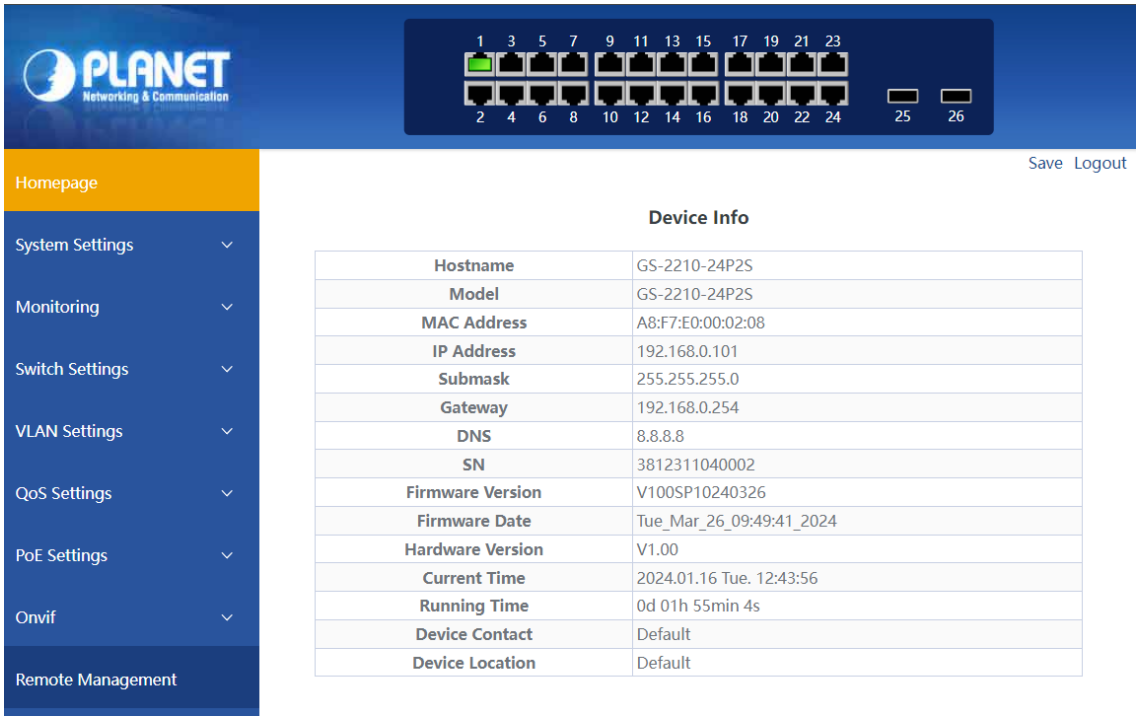


Figure : Web Main Page

Now, you can use the Web management interface to continue the switch management or manage the Web Smart Ethernet Switch by Web interface. The Switch Menu on the left of the web page lets you access all the commands and statistics the Web Smart Ethernet Switch provides.

Note

1. It is recommended to use Google Chrome, Mozilla Firefox or above to access Web Smart Ethernet Switch.
2. The changed IP address takes effect immediately after clicking on the **Save** button. You need to use the new IP address to access the Web interface.
3. For security reason, please change and memorize the new password after this first setup.
4. Only accept command in lowercase letter under web interface.

The Web Smart Ethernet Switch provides a Web-based browser interface for configuring and managing it. This interface allows you to access the Web Smart Ethernet Switch using the Web browser of your choice. This chapter describes how to use the Web Smart Ethernet Switch's Web browser interface to configure and manage it.

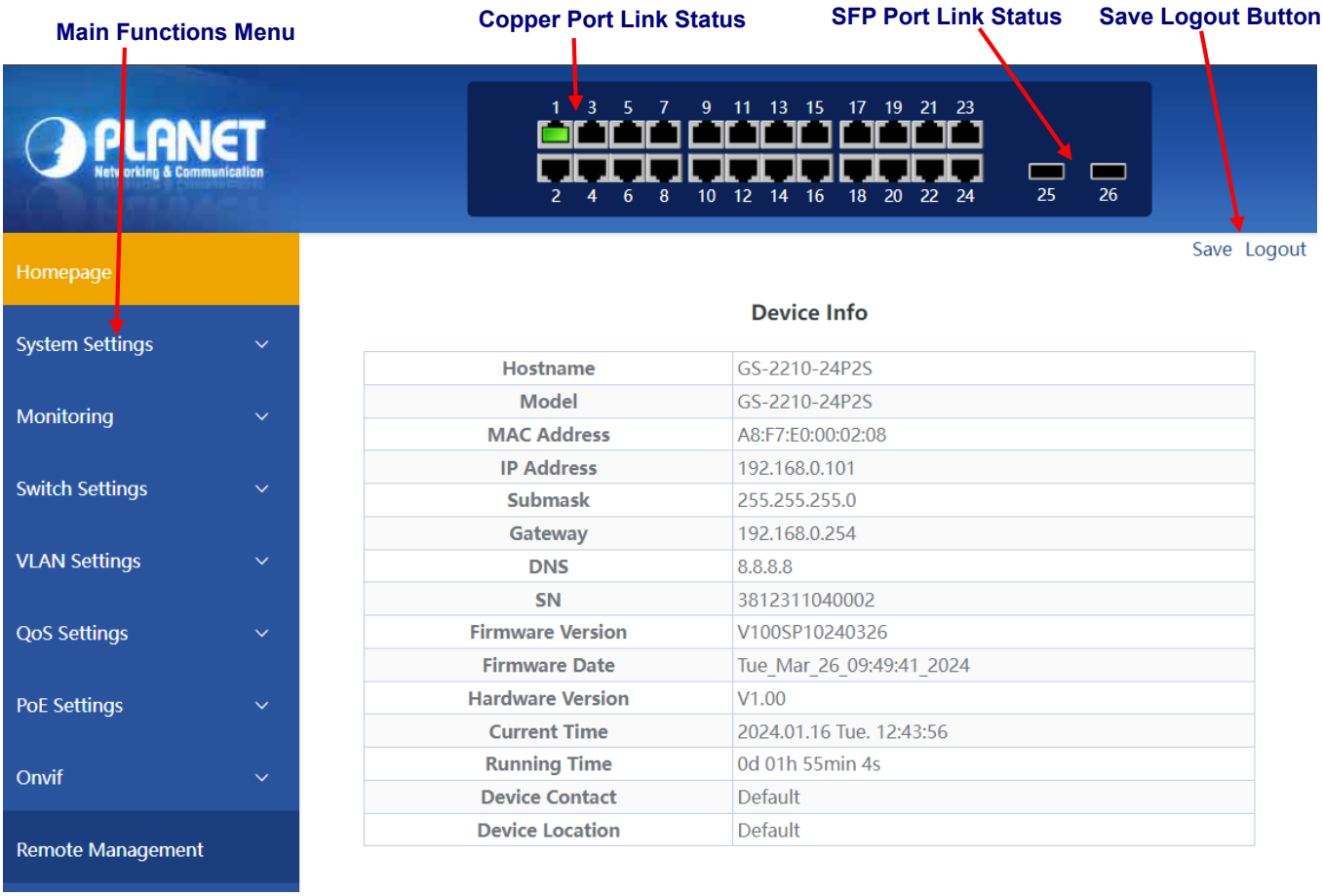


Figure : Web Main Page

Panel Display

The web agent displays an image of the Web Smart Ethernet Switch's ports. The Mode can be set to display different information for the ports, including Link up or Link down. Clicking on the image of a port opens the **Port Statistics** page. The port status is illustrated as follows:

State	Disabled	Down	Link	PoE in Use
RJ45 Ports				
SFP Ports				--

Main Menu

Using the onboard web agent, you can define system parameters, manage and control the Web Smart Ethernet Switch, and all its ports, or monitor network conditions. Via the Web-Management, the administrator can set up the Web Smart Ethernet Switch by selecting the functions those listed in the Main Function. The screen in below appears.

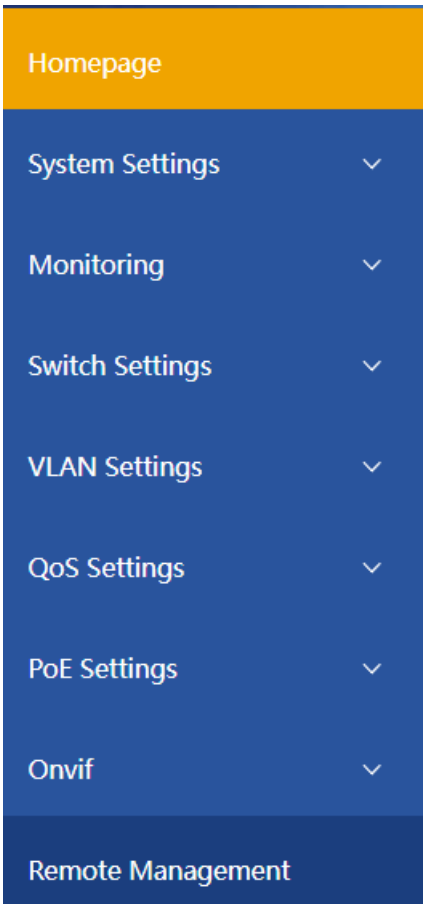


Figure : Web Smart Ethernet Switch Main Functions Menu

4.1. Homepage

The homepage interface displays the basic information of the device.

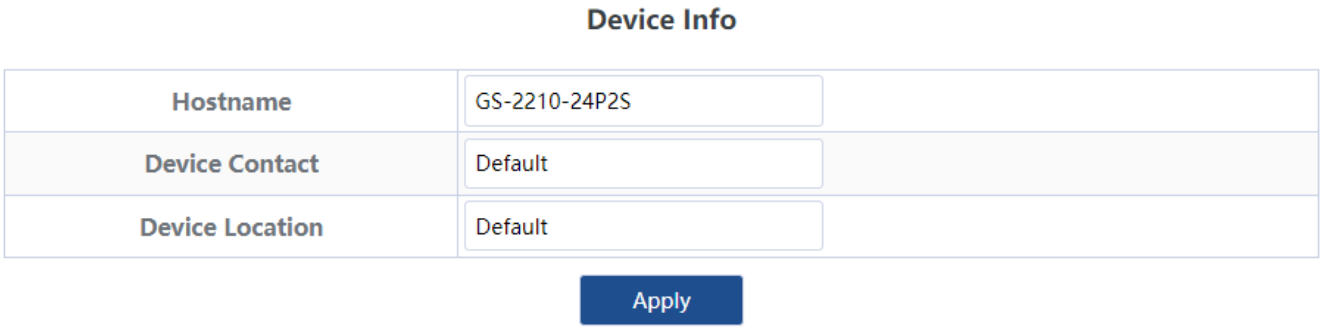
Device Info

Hostname	GS-2210-24P2S
Model	GS-2210-24P2S
MAC Address	A8:F7:E0:00:02:08
IP Address	192.168.0.101
Submask	255.255.255.0
Gateway	192.168.0.254
DNS	8.8.8.8
SN	3812311040002
Firmware Version	V100SP10240326
Firmware Date	Tue_Mar_26_09:49:41_2024
Hardware Version	V1.00
Current Time	2024.01.16 Tue. 12:56:33
Running Time	0d 02h 07min 42s
Device Contact	Default
Device Location	Default

4.2. System Settings

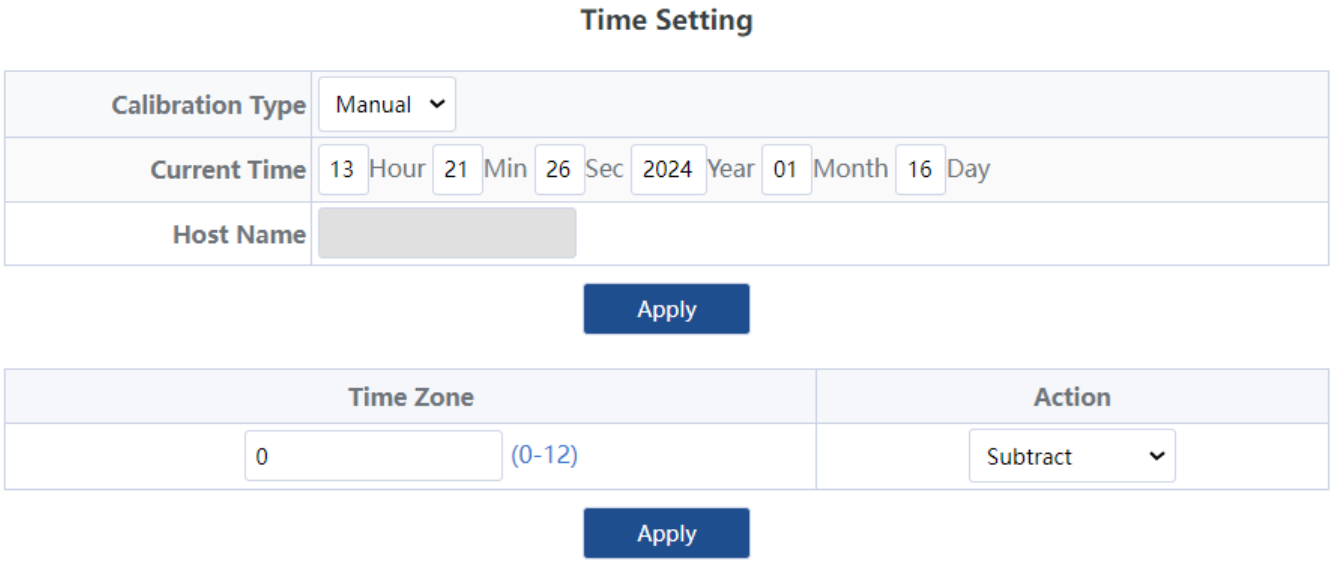
4.2.1. Device Info

Configure the information of the device, including Device Name, Device Contact and Device Location.



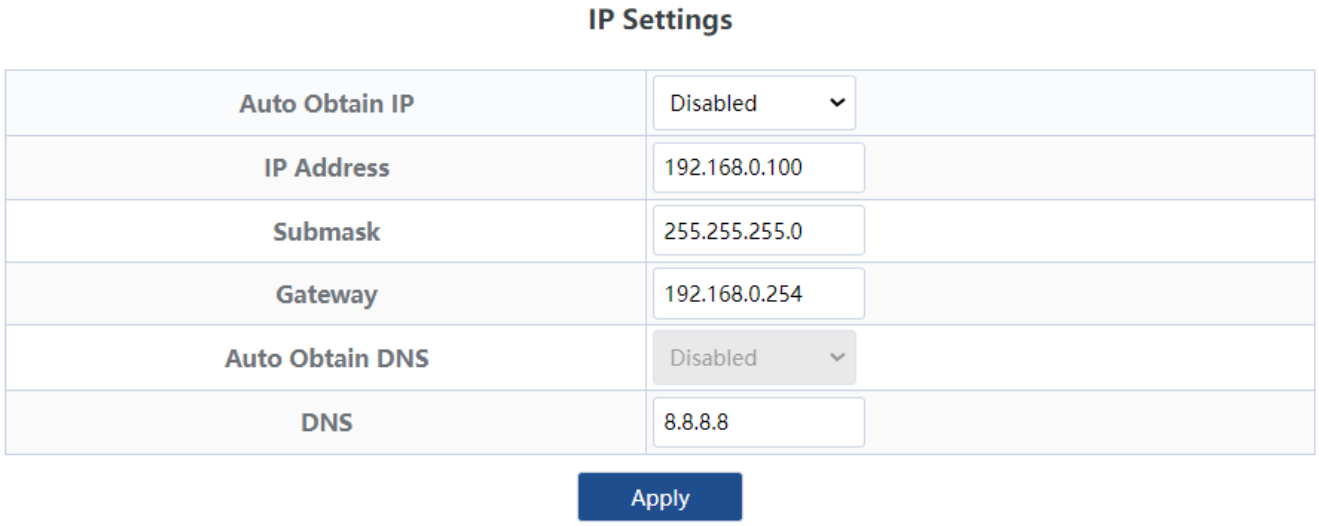
4.2.2. Time Setting

Configure the information of the device, including Calibration Type, Current Time and Host Name and Time Zone setting.

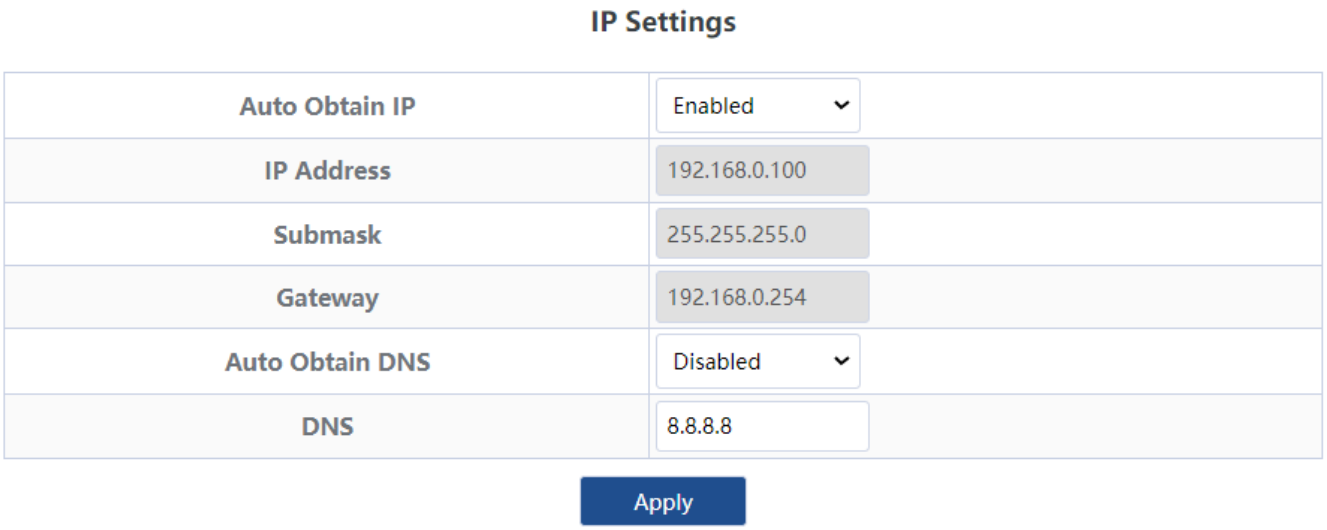


4.2.3. IP Settings

Configure device management IP (default static IP: 192.168.0.100)



When "Auto Obtain IP" is displayed as follows:

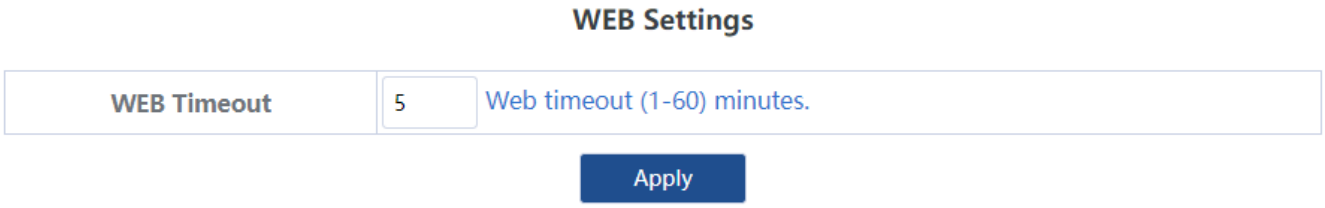


Tips:

1. When configuring IP, the device will be disconnected briefly. If automatic IP acquisition is enabled, you need to obtain the configuration IP from the uplink device or web management through device management IP: 10.XX.XX.XX(XX.XX.XX is the last two digits of the MAC address of the current device).

4.2.4. WEB Settings

Configure web page timeout, default is 5 minutes.

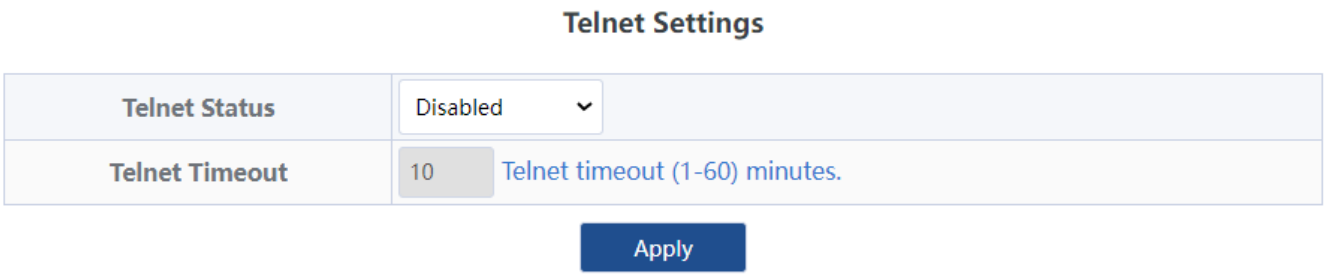


Tips:

1. The timeout can be configured for 1-60 minutes

4.2.5. Telnet Settings

Configure Telnet timeout, default Status is Disable, Telnet Timeout is 10 minutes.

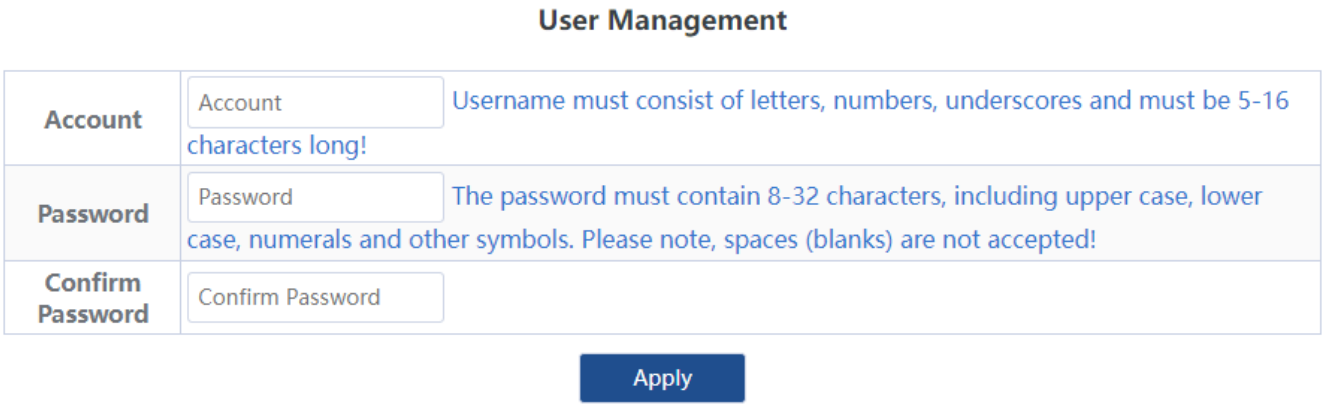


Tips:

1. The timeout can be configured for 1-60 minutes

4.2.6. User Management

Configure the account and password for web page login (The password must contain 6-16 characters and contain only letters, numbers and the following special characters: <=>[]!@#$*().)

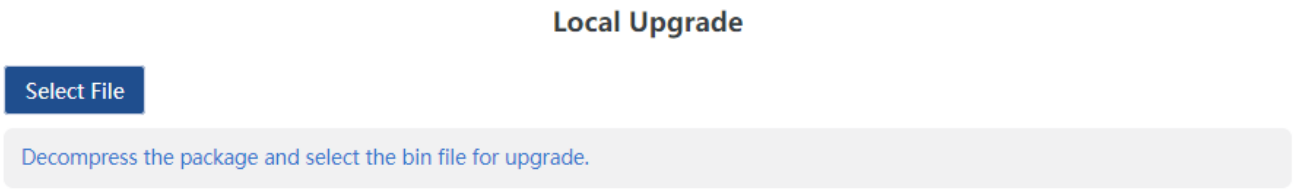


4.2.7. Upgrade

System upgrade can be divided into **Local upgrade**:

1. Local upgrade

Click《**Select File**》and select the software package you want to upgrade in the pop-up file selection box (the software upgrade package is a file in xxx.bin format).

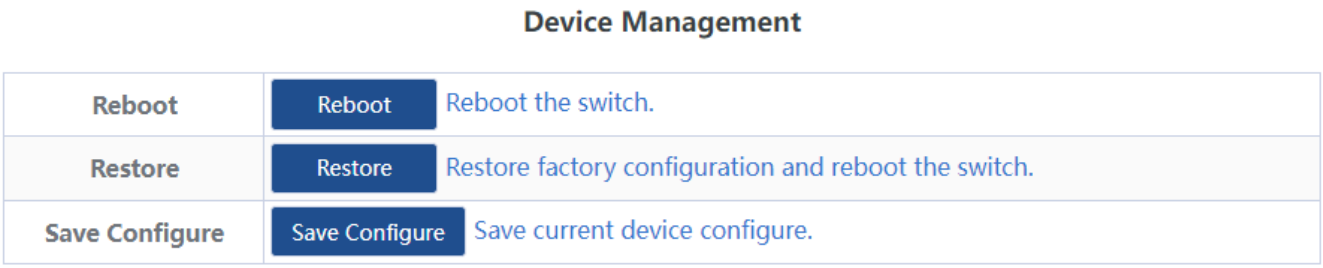


4.2.8. Device Management

Click《**Reboot**》to restart the equipment.

Click《**Restore**》to restore the factory configuration and restart the equipment.

Click《**Save Configure**》to save current device configure.



4.3. Monitoring

4.3.1. Port Statistics

The Port Statistics page displays the data statistics and status of the device port, such as the port sending and receiving rate, sending and receiving packets, etc.

Port Statistics

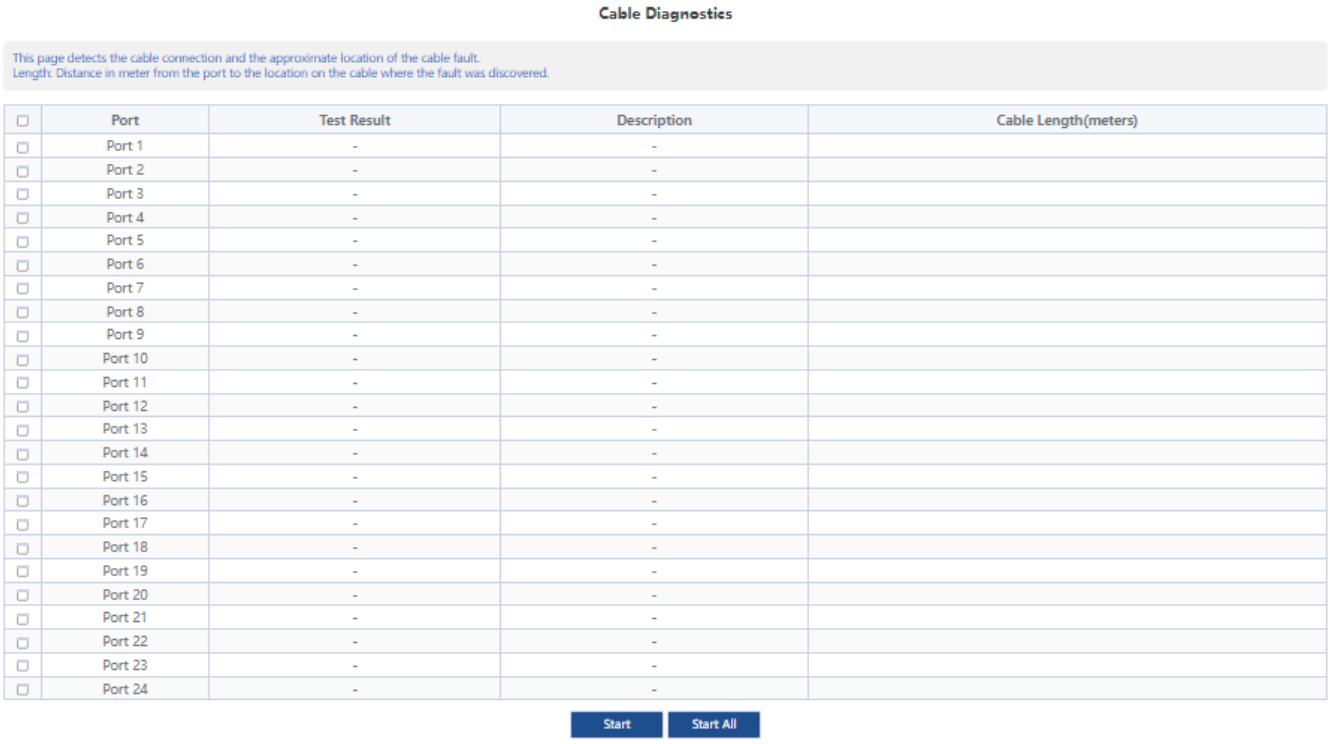
No.	Port	Link Status	Rx/Tx Rate(Bps)	Rx/Tx Rate(pps)	Rx/Tx Success	Rx/Tx Failure
1	Port 1	Connected	0/0	0/0	1147397/4635408	0/0
2	Port 2	Disconnect	0/0	0/0	0/0	0/0
3	Port 3	Disconnect	0/0	0/0	0/0	0/0
4	Port 4	Disconnect	0/0	0/0	0/0	0/0
5	Port 5	Disconnect	0/0	0/0	0/0	0/0
6	Port 6	Disconnect	0/0	0/0	0/0	0/0
7	Port 7	Disconnect	0/0	0/0	0/0	0/0
8	Port 8	Disconnect	0/0	0/0	0/0	0/0
9	Port 9	Connected	0/0	0/0	114362/211053	0/0
10	Port 10	Disconnect	0/0	0/0	0/0	0/0
11	Port 11	Disconnect	0/0	0/0	0/0	0/0
12	Port 12	Disconnect	0/0	0/0	0/0	0/0
13	Port 13	Disconnect	0/0	0/0	0/0	0/0
14	Port 14	Disconnect	0/0	0/0	0/0	0/0
15	Port 15	Disconnect	0/0	0/0	0/0	0/0
16	Port 16	Disconnect	0/0	0/0	0/0	0/0
17	Port 17	Disconnect	0/0	0/0	0/0	0/0
18	Port 18	Disconnect	0/0	0/0	0/0	0/0
19	Port 19	Disconnect	0/0	0/0	0/0	0/0
20	Port 20	Disconnect	0/0	0/0	0/0	0/0
21	Port 21	Disconnect	0/0	0/0	0/0	0/0
22	Port 22	Disconnect	0/0	0/0	0/0	0/0
23	Port 23	Disconnect	0/0	0/0	0/0	0/0
24	Port 24	Disconnect	0/0	0/0	0/0	0/0
25	Port 25	Disconnect	0/0	0/0	0/0	0/0
26	Port 26	Disconnect	0/0	0/0	0/0	0/0

Clear

4.3.2. Cable Diagnostics

You can roughly understand the cable condition of the corresponding port through cable detection (such as whether the cable is short circuited, disconnected, etc.).

Click 《**Start All**》 and wait for the test results to return.



Cable Diagnostics

This page detects the cable connection and the approximate location of the cable fault.
Length: Distance in meter from the port to the location on the cable where the fault was discovered.

Port	Test Result	Description	Cable Length(meters)
Port 1	-	-	
Port 2	-	-	
Port 3	-	-	
Port 4	-	-	
Port 5	-	-	
Port 6	-	-	
Port 7	-	-	
Port 8	-	-	
Port 9	-	-	
Port 10	-	-	
Port 11	-	-	
Port 12	-	-	
Port 13	-	-	
Port 14	-	-	
Port 15	-	-	
Port 16	-	-	
Port 17	-	-	
Port 18	-	-	
Port 19	-	-	
Port 20	-	-	
Port 21	-	-	
Port 22	-	-	
Port 23	-	-	
Port 24	-	-	

Start | Start All

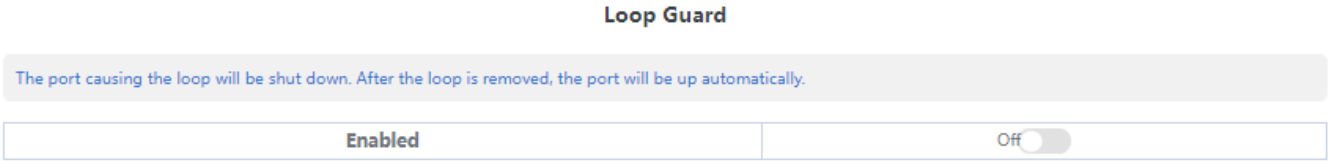
Cable Diagnostics

This page detects the cable connection and the approximate location of the cable fault.
Length: Distance in meter from the port to the location on the cable where the fault was discovered.

Port	Test Result	Description	Cable Length(meters)
Port 1	Nomal	Nomal(Correctly terminated pair)	(1, 2) 17 (3, 6) 17 (4, 5) 17 (7, 8) 17
Port 2	Disconnected	Please check whether the network cable is connected(Open pair,no link partner)	(1, 2) 2 (3, 6) 2 (4, 5) 1 (7, 8) 2
Port 3	Disconnected	Please check whether the network cable is connected(Open pair,no link partner)	(1, 2) 2 (3, 6) 1 (4, 5) 1 (7, 8) 1
Port 4	Disconnected	Please check whether the network cable is connected(Open pair,no link partner)	(1, 2) 2 (3, 6) 2 (4, 5) 2 (7, 8) 1
Port 5	Not Enabled	The port is shut down. Please enable the port first.	(1, 2) 0 (3, 6) 0 (4, 5) 0 (7, 8) 0
Port 6	Disconnected	Please check whether the network cable is connected(Open pair,no link partner)	(1, 2) 1 (3, 6) 1 (4, 5) 1 (7, 8) 1

4.3.3. Loop Guard

Configure enable loop guard



Tips:

The port causing the loop will be shut down. After the loop is removed, the port will be up automatically.（Default is disable）.

4.3.4. Ping Test

Configure enable loop guard

Configure the information of the device, including Host Name IP address or domain name.

4.3.5. IGMP Snooping

Configure IGMP Snooping

Unknown multicast Handel Action can configure **FLOOD** or **DROP**, Select the VLAN you want to enable and click 《**Apply**》 to save.

Tips:

IGMP Snooping only supports DIP mode, the maximum multicast entry is 10, Unknown multicast Handel Action default is flood.

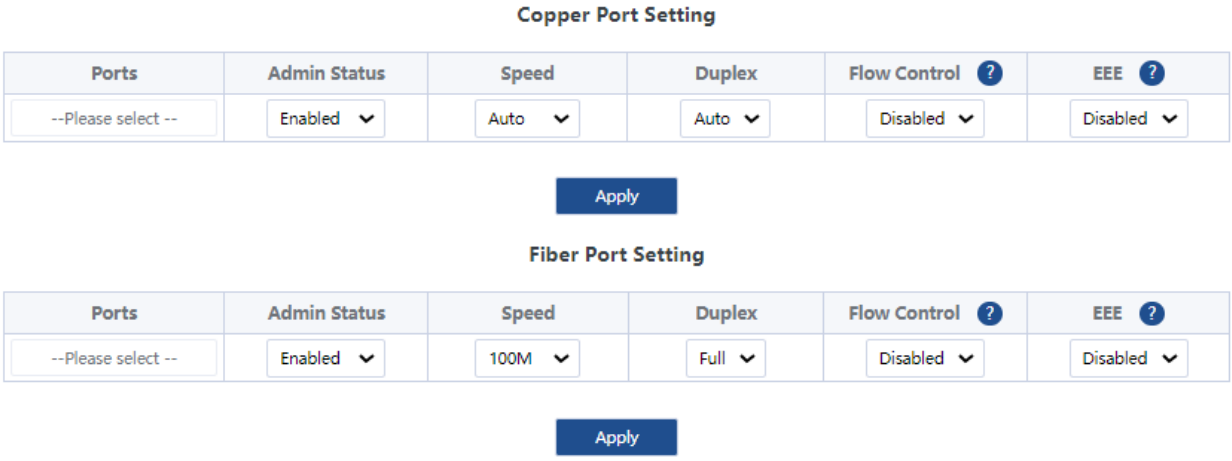
4.4. Switch Settings

4.4.1. Port Settings

Copper Port and Fiber Port configuration can batch configure the status, speed, duplex, flow control and EEE properties of ports. The page is divided into two parts:

Configuration part:

Select the port to be configured, then select each attribute to be configured, and click **《Apply》** to distribute the configuration.



Display part:

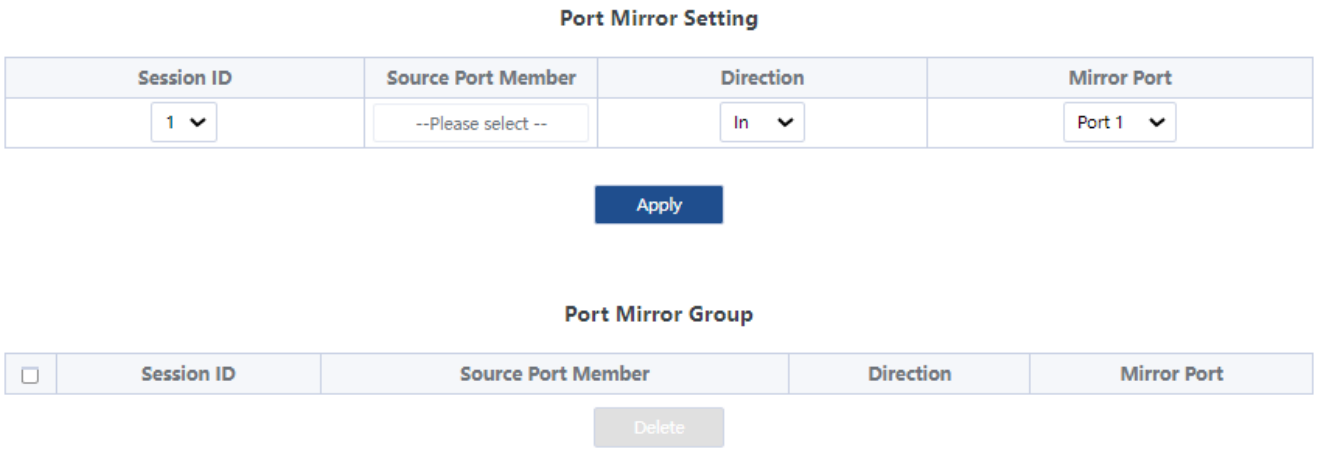
Displays the configuration attributes and actual effective attributes of each port of the device.

Port List

No.	Port	Admin Status	Speed Duplex		Flow Control		EEE
			Config	Actual	Config	Actual	
1	Port 1	Enabled	Auto/Auto	1000M/Full	Disabled	Disabled	Disabled
2	Port 2	Enabled	Auto/Auto	Link Down	Disabled	Disabled	Disabled
3	Port 3	Enabled	Auto/Auto	Link Down	Disabled	Disabled	Disabled
4	Port 4	Enabled	Auto/Auto	Link Down	Disabled	Disabled	Disabled
5	Port 5	Disabled	Auto/Auto	Link Down	Disabled	Disabled	Disabled
6	Port 6	Enabled	Auto/Auto	Link Down	Disabled	Disabled	Disabled
7	Port 7	Enabled	Auto/Auto	Link Down	Disabled	Disabled	Disabled
8	Port 8	Enabled	Auto/Auto	Link Down	Disabled	Disabled	Disabled
9	Port 9	Enabled	Auto/Auto	100M/Full	Disabled	Disabled	Disabled
10	Port 10	Enabled	Auto/Auto	Link Down	Disabled	Disabled	Disabled
11	Port 11	Enabled	Auto/Auto	Link Down	Disabled	Disabled	Disabled
12	Port 12	Enabled	Auto/Auto	Link Down	Disabled	Disabled	Disabled
13	Port 13	Enabled	Auto/Auto	Link Down	Disabled	Disabled	Disabled
14	Port 14	Enabled	Auto/Auto	Link Down	Disabled	Disabled	Disabled
15	Port 15	Enabled	Auto/Auto	Link Down	Disabled	Disabled	Disabled
16	Port 16	Enabled	Auto/Auto	Link Down	Disabled	Disabled	Disabled
17	Port 17	Enabled	Auto/Auto	Link Down	Disabled	Disabled	Disabled
18	Port 18	Enabled	Auto/Auto	Link Down	Disabled	Disabled	Disabled
19	Port 19	Enabled	Auto/Auto	Link Down	Disabled	Disabled	Disabled
20	Port 20	Enabled	Auto/Auto	Link Down	Disabled	Disabled	Disabled
21	Port 21	Enabled	Auto/Auto	Link Down	Disabled	Disabled	Disabled
22	Port 22	Enabled	Auto/Auto	Link Down	Disabled	Disabled	Disabled
23	Port 23	Enabled	Auto/Auto	Link Down	Disabled	Disabled	Disabled
24	Port 24	Enabled	Auto/Auto	Link Down	Disabled	Disabled	Disabled
25	Port 25	Enabled	Auto/Auto	Link Down	Disabled	Disabled	Disabled
26	Port 26	Enabled	Auto/Auto	Link Down	Disabled	Disabled	Disabled

4.4.2. Port Mirroring

The input / output messages of one or more source image ports are forwarded to the destination image port to monitor the network.

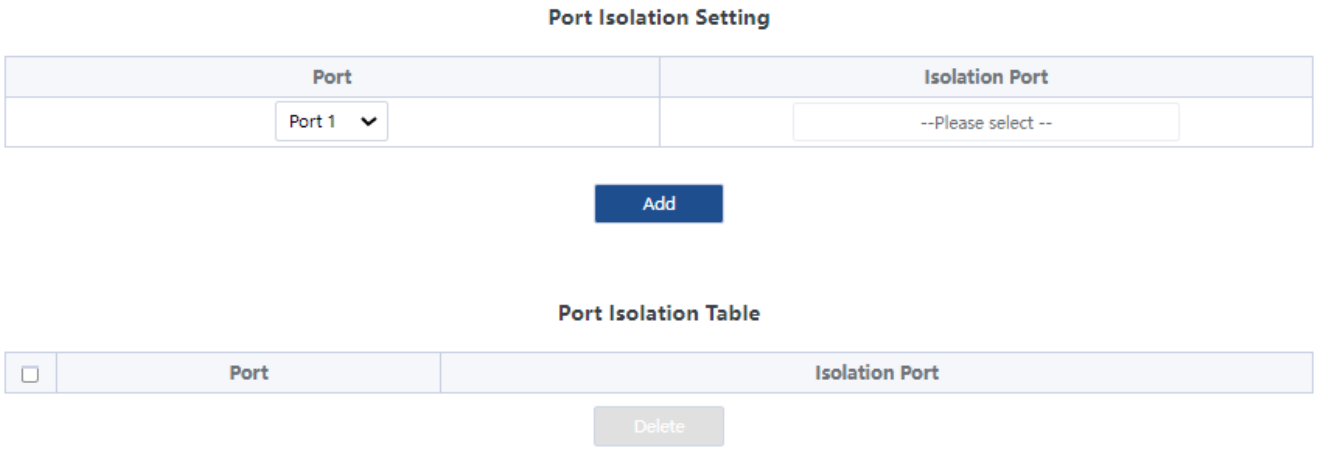


Tips:

1. Source port and destination port cannot be the same
2. Another mirror group is using the destination port
3. Supports 4 Session IDs

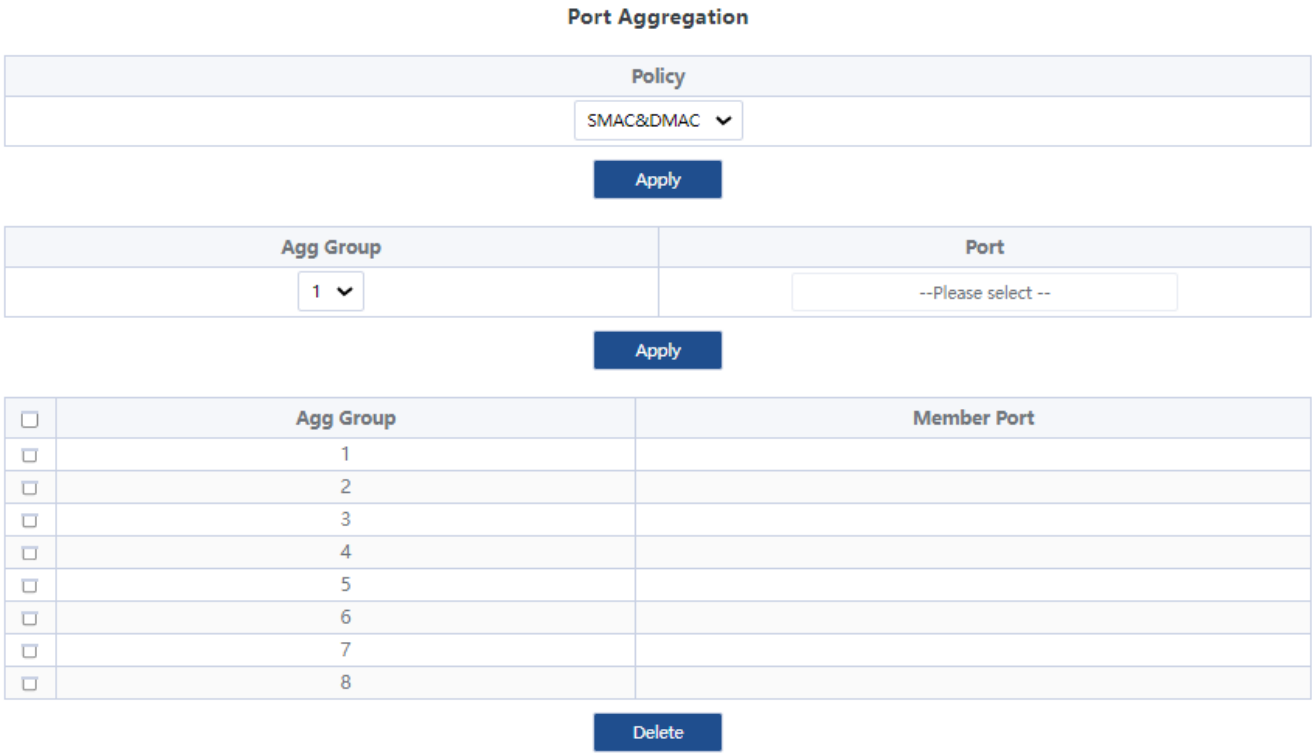
4.4.3. Port Isolation

Configure isolation port group



4.4.4. Port Aggregation

Configure the port aggregation information of the device, including Policy, Agg Group and Member Port setting.



4.4.5. Jumbo frame

Configure the size of Jumbo Frames that can be forwarded.

Tips：

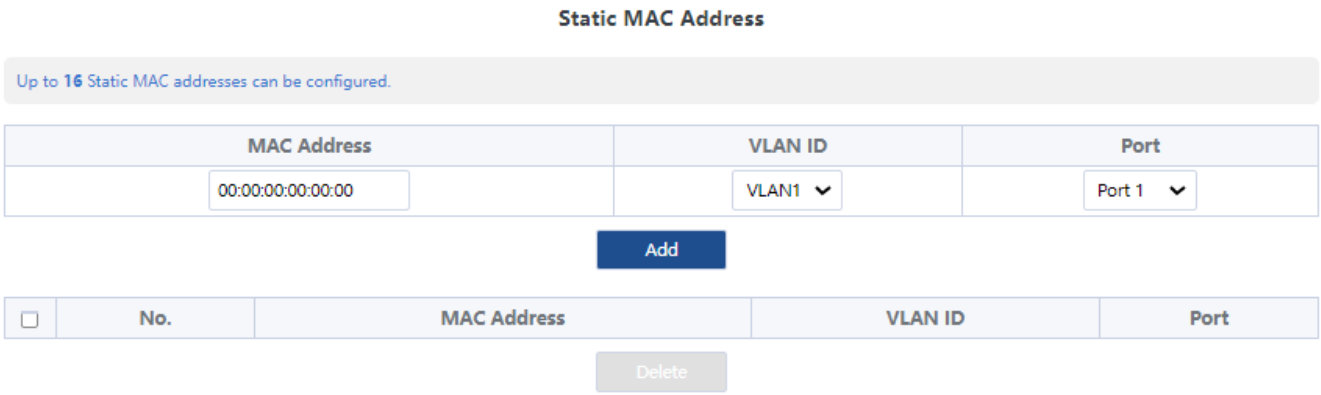
1. Jumbo Frames can be configured with 1522, 1536, 1552, 9216 and 10000;
2. The default value of Jumbo Frames is 1522.

4.4.6. Static MAC

The static MAC configuration is divided into two parts.

Static MAC add:

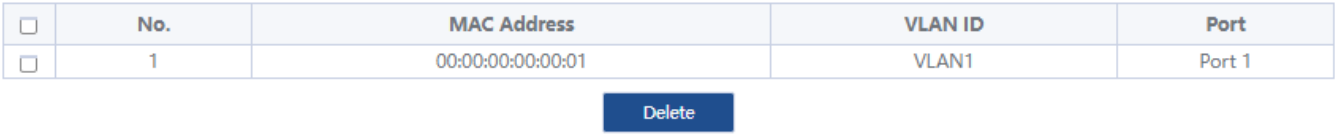
Enter the legitimate MAC address, VLAN ID, and select the configured port number. Click 《**Add**》 to add static MAC.



Static MAC deletion and display:

After adding a legal static Mac, the corresponding data will be displayed; Check the static Mac and click《**Delete**》.

After the configuration is successful, the MAC address, VLAN and corresponding port will be unbound.

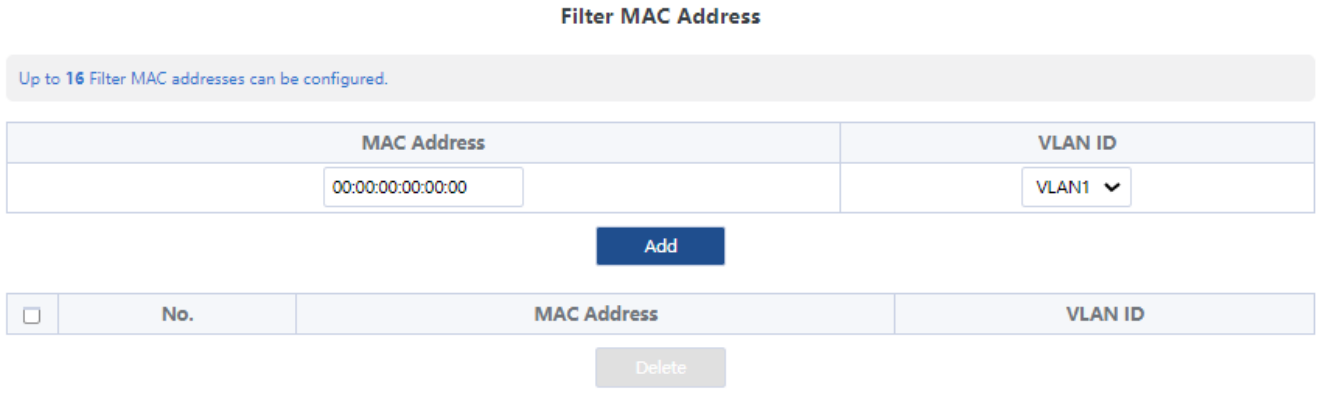


Tips:

1. Static MAC addresses maximum can be configured 16.

4.4.7. Filter MAC

Configure filtered MAC address

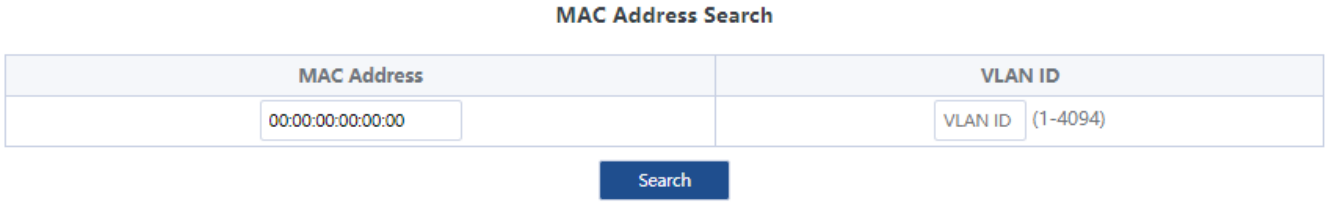


Tips:

1. Filter MAC addresses maximum can be configured 16.

4.4.8. Search MAC

Search the MAC table learned by the device (support fuzzy search?)

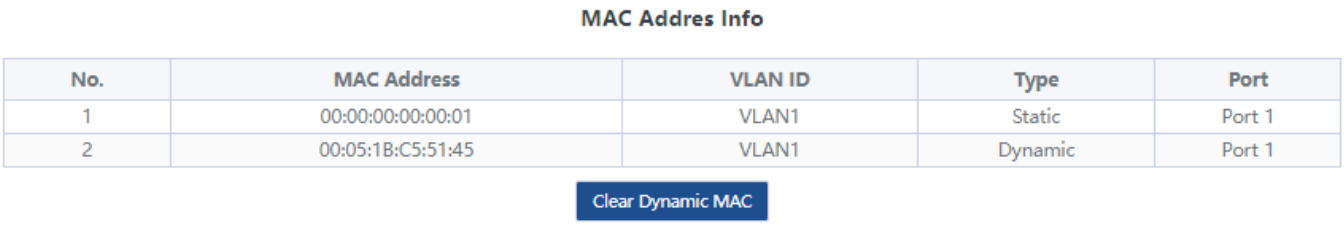


Tips:

1. The inquiry waiting process will interrupt the communication with the equipment

4.4.9. MAC List

Displays the list of MAC learned by the device



Click《**Clear Dynamic MAC**》and the device will get the learning MAC list again.

Tips:

1. The display waiting process will interrupt communication with the device

4.4.10. DHCP Snooping

Configure DHCP Snooping function, which is disabled by default.

When DHCP Snooping is enabled, you can choose to trust ports or not. As shown in the following figure, the device sets the selected ports as trusted ports, and if it is not selected, all ports are untrusted ports; Click《**Apply**》to set the selected port as a trusted port and complete the configuration of DHCP snooping.

Tips:

1. Enable DHCP snooping to filter DHCP messages. For the request message from DHCP client, only forward it to the trust port; for the response message from DHCP server, only forward the response message from the trust port.

2. Generally, the DHCP server port (upper connection port) is set as the trust port.

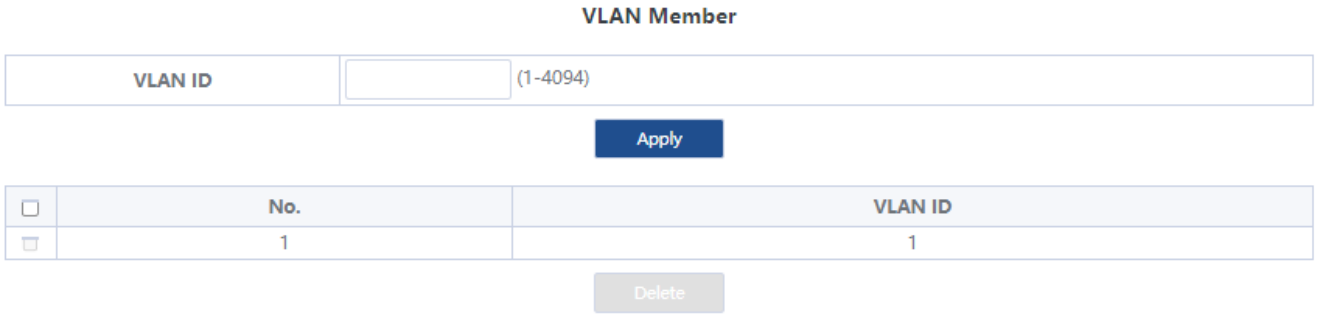
4.5. VLAN Settings

Add or delete device VLAN members and port VLAN configuration

4.5.1. VLAN Member

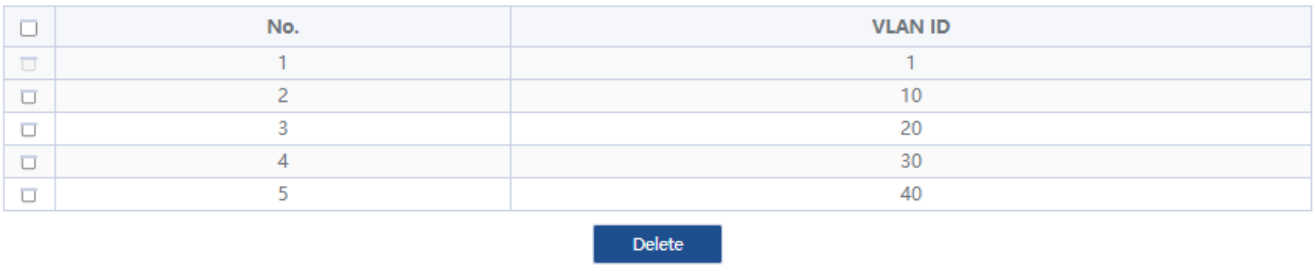
Configuration part:

Enter a valid VLAN ID and click 《**Apply**》to configure a new VLAN member;



Display part:

Displays the VLAN members newly added by the device, Select VLAN members in the VLAN member list and click 《**Delete**》to delete VLAN members in batch



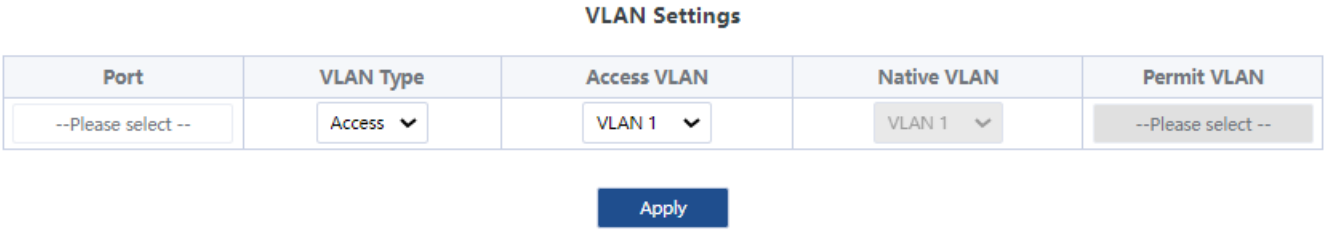
Tips:

1. Configure up to 16 VLAN members;
2. When VLAN ID is bound by port, it cannot be deleted.

4.5.2. VLAN Settings

Port VLAN configuration is divided into two parts:

Part I: Port VLAN configuration, select port, VLAN type (access and trunk, allow VLAN can be configured under trunk), allow VLAN and native VLAN, and click《**Apply**》to configure and save port VLAN (Permit VLAN and Native VLAN are selected from the VLAN members configured above);



Part II: Port VLAN list, which displays the VLAN configuration of the device port.

Tips: the message under Native VLAN does not have VLAN tag.

Port	VLAN Type	Access VLAN	Native VLAN	Permit VLAN
Port 1	Access	1	--	--
Port 2	Access	1	--	--
Port 3	Access	1	--	--
Port 4	Access	1	--	--
Port 5	Access	1	--	--
Port 6	Access	1	--	--
Port 7	Access	1	--	--
Port 8	Access	1	--	--
Port 9	Access	1	--	--
Port 10	Access	1	--	--
Port 11	Access	1	--	--
Port 12	Access	1	--	--
Port 13	Access	1	--	--
Port 14	Access	1	--	--
Port 15	Access	1	--	--
Port 16	Access	1	--	--
Port 17	Access	1	--	--
Port 18	Access	1	--	--
Port 19	Access	1	--	--
Port 20	Access	1	--	--
Port 21	Access	1	--	--
Port 22	Access	1	--	--
Port 23	Access	1	--	--
Port 24	Access	1	--	--
Port 25	Access	1	--	--
Port 26	Access	1	--	--
Port 27	Access	1	--	--
Port 28	Access	1	--	--

4.6. QoS Settings

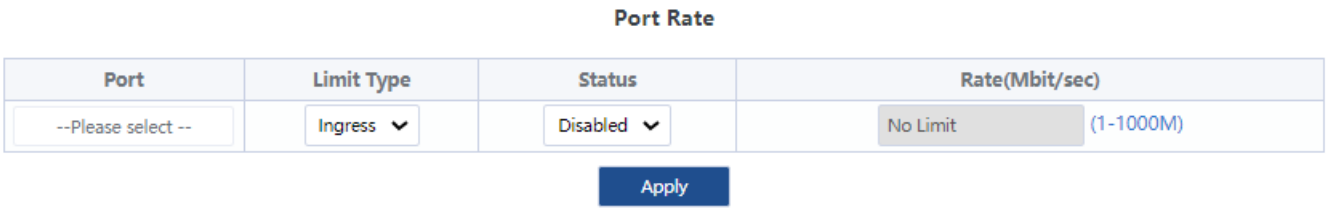
Including port rate limit and storm control functions.

4.6.1. Port Rate

Configure the port ingress and egress rate, which is divided into two parts:

Configuration part:

Select one or more ports, select the configuration type and whether to enable the port speed limit (enter the value of the port speed limit when it is enabled), and click《**Apply**》 to configure the port rate.



Display part: displays the ingress rate and egress rate of the device port configuration.

Entry	Port	Ingress		Egress	
		Status	Rate(Mbit/sec)	Status	Rate(Mbit/sec)
1	Port1	Disabled	1000	Disabled	1000
2	Port2	Disabled	1000	Disabled	1000
3	Port3	Disabled	1000	Disabled	1000
4	Port4	Disabled	1000	Disabled	1000
5	Port5	Disabled	1000	Disabled	1000
6	Port6	Disabled	1000	Disabled	1000
7	Port7	Disabled	1000	Disabled	1000
8	Port8	Disabled	1000	Disabled	1000
9	Port9	Disabled	1000	Disabled	1000
10	Port10	Disabled	1000	Disabled	1000
11	Port11	Disabled	1000	Disabled	1000
12	Port12	Disabled	1000	Disabled	1000
13	Port13	Disabled	1000	Disabled	1000
14	Port14	Disabled	1000	Disabled	1000
15	Port15	Disabled	1000	Disabled	1000
16	Port16	Disabled	1000	Disabled	1000
17	Port17	Disabled	1000	Disabled	1000
18	Port18	Disabled	1000	Disabled	1000
19	Port19	Disabled	1000	Disabled	1000
20	Port20	Disabled	1000	Disabled	1000
21	Port21	Disabled	1000	Disabled	1000
22	Port22	Disabled	1000	Disabled	1000
23	Port23	Disabled	1000	Disabled	1000
24	Port24	Disabled	1000	Disabled	1000
25	Port25	Disabled	1000	Disabled	1000
26	Port26	Disabled	1000	Disabled	1000
27	Port27	Disabled	1000	Disabled	1000
28	Port28	Disabled	1000	Disabled	1000

Tips:

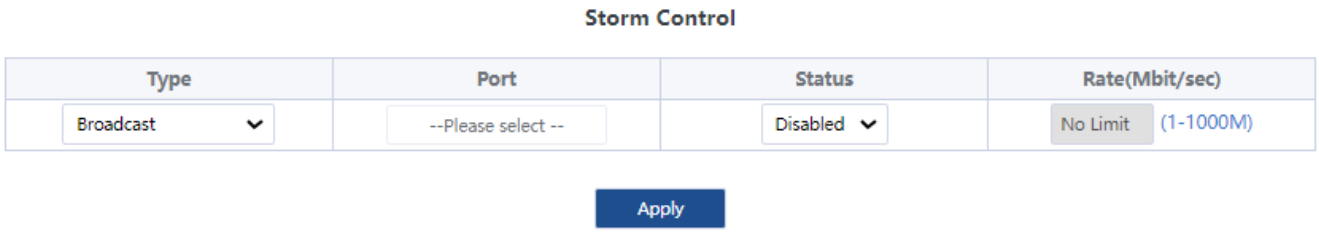
1. Rate limit range: 1-1000M

4.6.2. Storm Control

Including port storm control configuration and display:

Configuration part:

Select the configured storm control type, one or more ports and whether to enable storm control (when enabled, enter the rate of storm control configuration), and click《**Apply**》 to configure storm control.



Display part:

Display the storm control type and corresponding rate configured by the device port (display the corresponding control rate when it is turned on).

No.	Port	Broadcast(Mbit/sec)	Unknown Multicast(Mbit/sec)	Unknown Unicast(Mbit/sec)
1	Port 1	Disabled	Disabled	Disabled
2	Port 2	Disabled	Disabled	Disabled
3	Port 3	Disabled	Disabled	Disabled
4	Port 4	Disabled	Disabled	Disabled
5	Port 5	Disabled	Disabled	Disabled
6	Port 6	Disabled	Disabled	Disabled
7	Port 7	Disabled	Disabled	Disabled
8	Port 8	Disabled	Disabled	Disabled
9	Port 9	Disabled	Disabled	Disabled
10	Port 10	Disabled	Disabled	Disabled
11	Port 11	Disabled	Disabled	Disabled
12	Port 12	Disabled	Disabled	Disabled
13	Port 13	Disabled	Disabled	Disabled
14	Port 14	Disabled	Disabled	Disabled
15	Port 15	Disabled	Disabled	Disabled
16	Port 16	Disabled	Disabled	Disabled
17	Port 17	Disabled	Disabled	Disabled
18	Port 18	Disabled	Disabled	Disabled
19	Port 19	Disabled	Disabled	Disabled
20	Port 20	Disabled	Disabled	Disabled
21	Port 21	Disabled	Disabled	Disabled
22	Port 22	Disabled	Disabled	Disabled
23	Port 23	Disabled	Disabled	Disabled
24	Port 24	Disabled	Disabled	Disabled
25	Port 25	Disabled	Disabled	Disabled
26	Port 26	Disabled	Disabled	Disabled

Tips:

1. Rate limit range: 1-1000M

4.7. PoE Settings

Tips:

Some models support Poe function

4.7.1. PoE Global Info

Displays the global information of the device Poe function

PoE Global Info

PoE Hardware Version	V1.0
PoE Work Status	Normal
PoE Support Type	802.3af/802.3at
PoE Consumption Power	2W
PoE Port Number	24
PoE Total Power	260W
PoE Voltage	54 V
Software Version	V1.0.7

4.7.2. PoE Basic settings

Includes port PoE configuration and display:

Configuration part:

Select the PoE power supply status, priority and limited power of the configured port, and click 《**Apply**》 to configure PoE.

PoE Basic Settings

Port	PoE Control Status	Priority	PoE Limit
--Please select --	Enabled	Low	32 (1-32W)

Apply

Display part:

Display the power of port PoE and the current power supply status;

Entry	Port	PoE Control Status	Power Status	PoE Limit(1-32W)	Power	Priority	Class
1	Port1	Enabled	Off	32W	0W	Low	N/A
2	Port2	Enabled	Off	32W	0W	Low	N/A
3	Port3	Enabled	Off	32W	0W	Low	N/A
4	Port4	Enabled	Off	32W	0W	Low	N/A
5	Port5	Enabled	Off	32W	0W	Low	N/A
6	Port6	Enabled	Off	32W	0W	Low	N/A
7	Port7	Enabled	Off	32W	0W	Low	N/A
8	Port8	Enabled	Off	32W	0W	Low	N/A
9	Port9	Enabled	On	32W	3W	Low	0
10	Port10	Enabled	Off	32W	0W	Low	N/A
11	Port11	Enabled	Off	32W	0W	Low	N/A
12	Port12	Enabled	Off	32W	0W	Low	N/A
13	Port13	Enabled	Off	32W	0W	Low	N/A
14	Port14	Enabled	Off	32W	0W	Low	N/A
15	Port15	Enabled	Off	32W	0W	Low	N/A
16	Port16	Enabled	Off	32W	0W	Low	N/A
17	Port17	Enabled	Off	32W	0W	Low	N/A
18	Port18	Enabled	Off	32W	0W	Low	N/A
19	Port19	Enabled	Off	32W	0W	Low	N/A
20	Port20	Enabled	Off	32W	0W	Low	N/A
21	Port21	Enabled	Off	32W	0W	Low	N/A
22	Port22	Enabled	Off	32W	0W	Low	N/A
23	Port23	Enabled	Off	32W	0W	Low	N/A
24	Port24	Enabled	Off	32W	0W	Low	N/A

Tips:

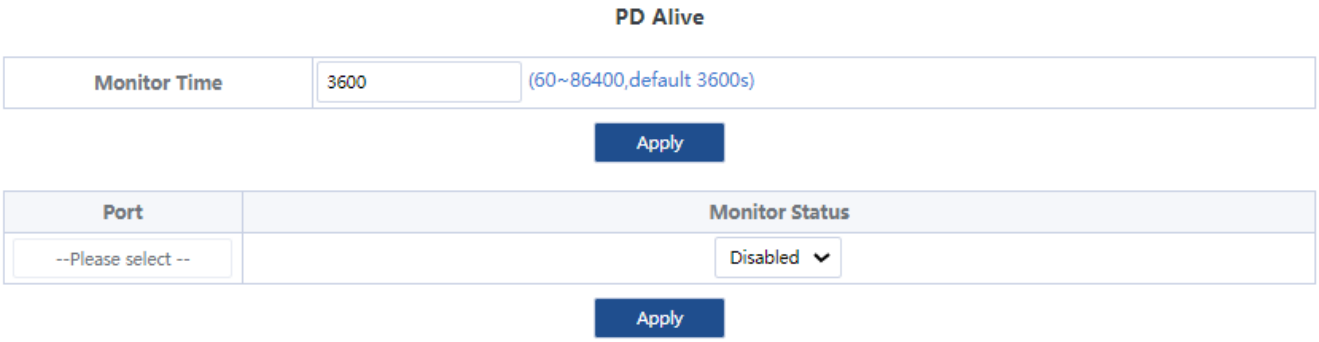
1. Disable port Poe. Port Poe will not be powered.

4.7.3. PD Alive

Includes PD Alive configuration and display:

Configuration part:

Configure the detection time of PD Alive (60-86400s. When no communication is detected on the port, PoE will be restarted automatically). Click《**Apply**》to configure PD alive.



Display part:

Displays the number of restarts of device PD Alive.

Entry	Port	Monitor Status	Reset Count
1	Port1	Disabled	0
2	Port2	Disabled	0
3	Port3	Disabled	0
4	Port4	Disabled	0
5	Port5	Disabled	0
6	Port6	Disabled	0
7	Port7	Disabled	0
8	Port8	Disabled	0
9	Port9	Disabled	0
10	Port10	Disabled	0
11	Port11	Disabled	0
12	Port12	Disabled	0
13	Port13	Disabled	0
14	Port14	Disabled	0
15	Port15	Disabled	0
16	Port16	Disabled	0
17	Port17	Disabled	0
18	Port18	Disabled	0
19	Port19	Disabled	0
20	Port20	Disabled	0
21	Port21	Disabled	0
22	Port22	Disabled	0
23	Port23	Disabled	0
24	Port24	Disabled	0

4.7.4. PoE Schedule

Support Onvif protocol function to discover devices

Configure the PoE Schedule information of the device, including Port, Timing Switch, Timing Type, Week and Time setting.

PoE Schedule

Port	Timing Switch	Timing Type	Week	Time
--Please select --	Off	Close Time	Mon.	0 Hour 0 Min 0 Sec

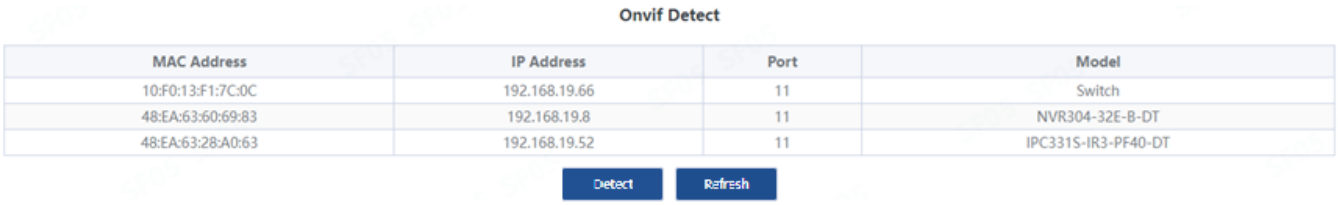
Apply

Port	PoE Status	Open Time	Close Time
Port1	Off	Off	Off
Port2	Off	Off	Off
Port3	Off	Off	Off
Port4	Off	Off	Off
Port5	Off	Off	Off
Port6	Off	Off	Off
Port7	Off	Off	Off
Port8	Off	Off	Off
Port9	On	Off	Off
Port10	Off	Off	Off
Port11	Off	Off	Off
Port12	Off	Off	Off
Port13	Off	Off	Off
Port14	Off	Off	Off
Port15	Off	Off	Off
Port16	Off	Off	Off
Port17	Off	Off	Off
Port18	Off	Off	Off
Port19	Off	Off	Off
Port20	Off	Off	Off
Port21	Off	Off	Off
Port22	Off	Off	Off
Port23	Off	Off	Off
Port24	Off	Off	Off

4.8. Onvif

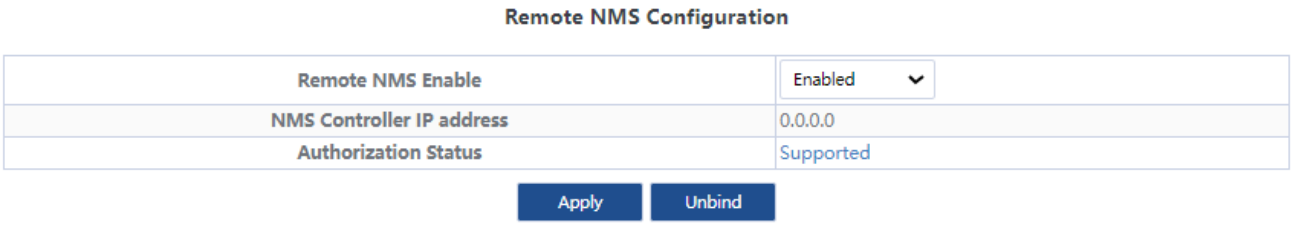
Support Onvif protocol function to discover devices

Click《**Detect**》to find the device.



4.9. Remote Management

Configure the Remote NMS Configuration of the device Enable/Disable setting.



5. SWITCH OPERATION

5.1 Address Table

The **Web Smart Ethernet Switch** is implemented with an address table. This address table is composed of many entries. Each entry is used to store the address information of some nodes in the network, including MAC address, port no, etc. This information comes from the learning process of **Web Smart Ethernet Switch**.

5.2 Learning

When one packet comes in from any port, the **Web Smart Ethernet Switch** will record the source address, port no., and the other related information in address table. This information will be used to decide either forwarding or filtering for future packets.

5.3 Forwarding & Filtering

When one packet comes from some port of the **Web Smart Ethernet Switch**, it will also check the destination address besides the source address learning. The **Web Smart Ethernet Switch** will look up the address-table for the destination address. If not found, this packet will be forwarded to all the other ports except the port, which this packet comes in. And these ports will transmit this packet to the network it connected. If found, and the destination address is located at a different port from this packet comes in, the **Web Smart Ethernet Switch** will forward this packet to the port where this destination address is located according to the information from address table. But, if the destination address is located at the same port with this packet comes in, then this packet will be filtered, thereby increasing the network throughput and availability.

5.4 Store-and-Forward

Store-and-Forward is one type of packet-forwarding techniques. A Store-and-Forward **Web Smart Ethernet Switch** stores the incoming frame in an internal buffer and do the complete error checking before transmission. Therefore, no error packets occur; it is the best choice when a network needs efficiency and stability.

The **Web Smart Ethernet Switch** scans the destination address from the packet-header, searches the routing table provided for the incoming port and forwards the packet, only if required. The fast forwarding makes the switch attractive for connecting servers directly to the network, thereby increasing throughput and availability. However, the switch is most commonly used to segment existence hubs, which nearly always improves the overall performance. An Ethernet switching can be easily configured in any Ethernet network environment to significantly boost bandwidth using the conventional cabling and adapters.

Due to the learning function of the **Web Smart Ethernet Switch**, the source address and corresponding port number of each incoming and outgoing packet are stored in a routing table. This information is subsequently used to filter packets whose destination address is in the same segment as the source address. This confines network traffic to its respective domain and reduce the overall load on the network.

The **Web Smart Ethernet Switch** performs **"Store and Fforward"**; therefore, no error packets occur. More reliably, it reduces the re-transmission rate. No packet loss will occur.

5.5 Auto-Negotiation

The STP ports on the Switch have built-in **"Auto-negotiation"**. This technology automatically sets the best possible bandwidth when a connection is established with another network device (usually at Power On or Reset). This is done by detecting the modes and speeds both connected devices are capable of. Both 10BASE-T and 100BASE-TX devices can connect with the port in either half- or full-duplex mode. 1000BASE-T can be only connected in full-duplex mode.

6. TROUBLESHOOTING

This chapter contains information to help you solve issues. If the Web Smart Ethernet Switch is not functioning properly, make sure the Web Smart Ethernet Switch was set up according to instructions in this manual.

■ **The Link LED is not lit.**

Solution:

Check the cable connection and remove duplex mode of the Web Smart Ethernet Switch.

■ **Some stations cannot talk to other stations located on the other port.**

Solution:

Please check the VLAN settings, trunk settings, or port enabled/disabled status.

■ **Performance is bad.**

Solution:

Check the full duplex status of the Web Smart Ethernet Switch. If the Web Smart Ethernet Switch is set to full duplex and the partner is set to half duplex, then the performance will be poor. Please also check the in/out rate of the port.

■ **Why the Switch doesn't connect to the network.**

Solution:

1. Check the LNK/ACT LED on the switch.
2. Try another port on the Switch.
3. Make sure the cable is installed properly.
4. Make sure the cable is the right type.
5. Turn off the power. After a while, turn on power again.

■ **1000BASE-T port link LED is lit, but the traffic is irregular.**

Solution:

Check that the attached device is not set to dedicate full duplex. Some devices use a physical or software switch to change duplex modes. Auto-negotiation may not recognize this type of full-duplex setting.

■ **Switch does not power up.**

Solution:

1. AC power cord is not inserted or faulty.
2. Check that the AC power cord is inserted correctly.
3. Replace the power cord if the cord is inserted correctly; check that the AC power source is working by connecting a different device in place of the switch.
4. If that device works, refer to the next step.
5. If that device does not work, check the AC power.

APPENDIX A: Networking Connection

A.1 Switch's Data RJ45 Pin Assignments - 1000Mbps, 1000BASE-T

PIN NO	MDI	MDI-X
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

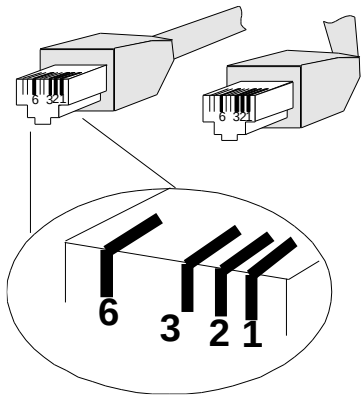
Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

A.2 10/100Mbps, 10/100BASE-TX

When connecting your Switch to another Fast Ethernet switch, a bridge or a hub, a straight or crossover cable is necessary. Each port of the Switch supports auto-MDI/MDI-X detection. That means you can directly connect the Switch to any Ethernet devices without making a crossover cable. The following table and diagram show the standard RJ45 receptacle/ connector and their pin assignments:

RJ45 Connector pin assignment		
PIN NO	MDI Media Dependent Interface	MDI-X Media Dependent Interface-Cross
1	Tx + (transmit)	Rx + (receive)
2	Tx - (transmit)	Rx - (receive)
3	Rx + (receive)	Tx + (transmit)
4, 5	Not used	
6	Rx - (receive)	Tx - (transmit)
7, 8	Not used	

The standard cable, RJ45 pin assignment



The standard RJ45 receptacle/connector

There are 8 wires on a standard UTP/STP cable and each wire is color-coded. The following shows the pin allocation and color of straight-through cable and crossover cable connection:

Straight Cable		SIDE 1	SIDE 2
1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8	SIDE 1 SIDE 2	1 = White / Amber 2 = Amber 3 = White / Green 4 = Blue 5 = White / Blue 6 = Green 7 = White / Brown 8 = Brown	1 = White / Amber 2 = Amber 3 = White / Green 4 = Blue 5 = White / Blue 6 = Green 7 = White / Brown 8 = Brown
Crossover Cable		**SIDE 1**	**SIDE 2**
1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8	SIDE 1 SIDE 2	1 = White / Amber 2 = Amber 3 = White / Green 4 = Blue 5 = White / Blue 6 = Green 7 = White / Brown 8 = Brown	1 = White / Green 2 = Green 3 = White / Amber 4 = Blue 5 = White / Blue 6 = Amber 7 = White / Brown 8 = Brown

Figure A-1: Straight-through and Crossover Cable

Please make sure your connected cables are with the same pin assignment and color as the above picture before deploying the cables into your network.

APPENDIX B : GLOSSARY

A

ACE

ACE is an acronym for **A**ccess **C**ontrol **E**ntry. It describes access permission associated with a particular ACE ID.

There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

ACL

ACL is an acronym for **A**ccess **C**ontrol **L**ist. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.

Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

There are 3 web pages associated with the manual ACL configuration:

ACL|Access Control List: The web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). Default the table is empty. An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a policy, 1 ingress port, or any ingress port (the whole switch). If an ACE Policy is created then that policy can be associated with a group of ports under the "Ports" web page. There are number of parameters that can be configured with an ACE. Read the web page help text to get further information for each of them. The maximum number of ACEs is 64.

ACL|Ports: The ACL Port configuration is used to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic Policy is created under the "Access Control List". You can you also set up specific traffic properties (Action / Rate Limiter / Port copy, etc) for each ingress port. They will though only apply if the frame gets past the ACE matching without getting matched. In that case a counter associated with that port is incremented. See the web page help text for each specific port property.

ACL|Rate Limiters: On this page, you can configure the rate limiters. There can be 15 different rate limiters, each ranging from 1 to 1024K packets per second. Under "Ports" and "Access Control List", you can assign a Rate Limiter ID to the ACE(s) or ingress port(s).

AES

AES is an acronym for **A**dvanced **E**ncryption **S**tandard. The encryption key protocol is applied in 802.1x standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

AMS

AMS is an acronym for **A**uto **M**edia **S**elect. AMS is used for dual media ports (ports supporting both copper (cu) and fiber (SFP) cables. AMS automatically determines if an SFP or a CU cable is inserted and switches to the corresponding media. If both SFP and cu cables are inserted, the port will select the prefered media.

APS

APS is an acronym for **A**utomatic **P**rotection **S**witching. This protocol is used to secure switching that is done bidirectional in both ends of a protection group, as defined in G.8031.

Aggregation

Using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.

(Also *Port Aggregation, Link Aggregation*).

ARP

ARP is an acronym for **A**ddress **R**esolution **P**rotocol. It is a protocol that used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

ARP Inspection

ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

Auto-Negotiation

Auto-negotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.

C

CC

CC is an acronym for **C**ontinuity **C**heck. It is a MEP functionality that is able to detect loss of continuity in a network by transmitting CCM frames to a peer MEP.

CCM

CCM is an acronym for **C**ontinuity **C**heck **M**essage. It is a OAM frame transmitted from a MEP to its peer MEP and used to implement CC functionality.

CDP

CDP is an acronym for **C**isco **D**iscovery **P**rotocol.

D

DEI

DEI is an acronym for **D**rop **E**ligible **I**ndicator. It is a 1-bit field in the VLAN tag.

DES

DES is an acronym for **D**ata **E**ncryption **S**tandard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.

DHCP

DHCP is an acronym for **D**ynamic **H**ost **C**onfiguration **P**rotocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.

DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Relay

DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID. The parameter of "port_no" is the fourth byte and it means the port number.
The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agents MAC address.

DHCP Snooping

DHCP Snooping is used to block intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

DNS

DNS is an acronym for **D**omain **N**ame **S**ystem. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.

DoS

DoS is an acronym for **D**enial of **S**ervice. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting at network sites or network connection, an attacker may be able to prevent network users from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer.

Dotted Decimal Notation

Dotted Decimal Notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets.
An IPv4 dotted decimal address has the form x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255.

DSCP

DSCP is an acronym for **D**ifferentiated **S**ervices **C**ode **P**oint. It is a field in the header of IP packets for packet classification purposes.

E

EEE

EEE is an abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az.

EPS

EPS is an abbreviation for Ethernet Protection Switching defined in ITU/T G.8031.

Ethernet Type

Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.

F

FTP

FTP is an acronym for **F**ile **T**ransfer **P**rotocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP) and provides file writing and reading. It also provides directory service and security features.

Fast Leave

IGMP snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously.

H

HTTP

HTTP is an acronym for **H**ypertext **T**ransfer **P**rotocol. It is a protocol that used to transfer or convey information on the World Wide Web (WWW).

HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested web page. The other main standard that controls how the World Wide Web works is HTML, which covers how web pages are formatted and displayed.

Any Web server machine contains, in addition to the web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

HTTPS

HTTPS is an acronym for **H**ypertext **T**ransfer **P**rotocol over **S**ecure Socket Layer. It is used to indicate a secure HTTP connection.

HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons.

HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

I

ICMP

ICMP is an acronym for **I**nternet **C**ontrol **M**essage **P**rotocol. It is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.

IEEE 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

IGMP

IGMP is an acronym for **I**nternet **G**roup **M**anagement **P**rotocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Querier

A router sends IGMP Query messages onto a particular link. This router is called the Querier.

IMAP

IMAP is an acronym for **I**nternet **M**essage **A**ccess **P**rotocol. It is a protocol for email clients to retrieve email messages from a mail server.

IMAP is the protocol that IMAP clients use to communicate with the servers, and SMTP is the protocol used to transport mail to an IMAP server.

The current version of the Internet Message Access Protocol is IMAP4. It is similar to Post Office Protocol version 3 (POP3), but offers additional and more complex features. For example, the IMAP4 protocol leaves your email messages on the server rather than downloading them to your computer. If you wish to remove your messages from the server, you must use your mail client to generate local folders, copy messages to your local hard drive, and then delete and expunge the messages from the server.

IP

IP is an acronym for **I**nternet **P**rotocol. It is a protocol used for communicating data across a internet network.

IP is a "best effort" system, which means that no packet of information sent over it is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

IPMC

IPMC is an acronym for **IP** **M**ulti**C**ast.

IP Source Guard

IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

L

LACP

LACP is an IEEE 802.3ad standard protocol. The **L**ink **A**ggregation **C**ontrol **P**rotocol allows bundling several physical ports together to form a single logical port.

LLDP

LLDP is an IEEE 802.1ab standard protocol.

The **L**ink **L**ayer **D**iscovery **P**rotocol(LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP-MED

LLDP-MED is an extension of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).

LOC

LOC is an acronym for **L**oss **O**f **C**onnectivity and is detected by a MEP and is indicating lost connectivity in the network. Can be used as a switch criteria by EPS

M

MAC Table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.

MEP

MEP is an acronym for **M**aintenance **E**ntity **E**ndpoint and is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).

MD5

MD5 is an acronym for **M**essage-**D**igest algorithm **5**. MD5 is a message digest algorithm, used cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm.

Mirroring

For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.)

Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

MLD

MLD is an acronym for **M**ulticast **L**istener **D**iscovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

MVR

Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP)-networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs. The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network, instead the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested it/them (Wikipedia).

N

NAS

NAS is an acronym for Network Access Server. The NAS is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.

NetBIOS

NetBIOS is an acronym for **Net**work **B**asic **I**nput/**O**utput **S**ystem. It is a program that allows applications on separate computers to communicate within a Local Area Network (LAN), and it is not supported on a Wide Area Network (WAN).

The NetBIOS giving each computer in the network both a NetBIOS name and an IP address corresponding to a different host name, provides the session and transport services described in the Open Systems Interconnection (OSI) model.

NFS

NFS is an acronym for **N**etwork **F**ile **S**ystem. It allows hosts to mount partitions on a remote system and use them as though they are local file systems.

NFS allows the system administrator to store resources in a central location on the network, providing authorized users continuous access to them, which means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.

NTP

NTP is an acronym for **N**etwork **T**ime **P**rotocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer.

O

OAM

OAM is an acronym for **O**peration **A**dministration and **M**aintenance. It is a protocol described in ITU-T Y.1731 used to implement carrier Ethernet functionality. MEP functionality like CC and RDI is based on this.

Optional TLVs.

An LLDP frame contains multiple TLVs. For some TLVs it is configurable if the switch includes the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLV is disabled the corresponding information is not included in the LLDP frame.

OUI

OUI is the organizationally unique identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of an MAC address.

P

PCP

PCP is an acronym for Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority.

PD

PD is an acronym for **P**owered **D**evice. In a PoE> system the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.

PHY

PHY is an abbreviation for Physical Interface Transceiver and is the device that implement the Ethernet physical layer (IEEE-802.3).

PING

Ping is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.

Ping uses Internet Control Message Protocol (ICMP) packets. The Ping Request is the packet from the origin computer, and the Ping Reply is the packet response from the target.

Policer

A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

POP3

POP3 is an acronym for **P**ost **O**ffice **P**rotocol version 3. It is a protocol for email clients to retrieve email messages from a mail server.

POP3 is designed to delete mail on the server as soon as the user has downloaded it. However, some implementations allow users or an administrator to specify that mail be saved for some period of time. POP can be thought of as a "store-and-forward" service.

An alternative protocol is Internet Message Access Protocol (IMAP). IMAP provides the user with more capabilities for retaining e-mail on the server and for organizing it in folders on the server. IMAP can be thought of as a remote file server.

POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (SMTP). You send e-mail with SMTP, and a mail handler receives it on your recipient's behalf. Then the mail is read using POP or IMAP. IMAP4 and POP3 are the two most prevalent Internet standard protocols for e-mail retrieval. Virtually all modern e-mail clients and servers support both.

PPPoE

PPPoE is an acronym for Point-to-Point Protocol over Ethernet. It is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks (Wikipedia).

Private VLAN

In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.

PTP

PTP is an acronym for Precision Time Protocol, a network protocol for synchronizing the clocks of computer systems.

Q

QCE

QCE is an acronym for **Q**oS **C**ontrol **E**ntry. It describes QoS class associated with a particular QCE ID.

There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of 4 different QoS classes: "Low", "Normal", "Medium", and "High" for individual application.

QCL

QCL is an acronym for **Q**oS **C**ontrol **L**ist. It is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects.

Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.

QL

QL In SyncE this is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.

QoS

QoS is an acronym for **Q**uality **o**f **S**ervice. It is a method to guarantee a bandwidth relationship between individual applications or protocols.

A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.

Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

QoS class

Every incoming frame is classified to a QoS class, which is used throughout the device for providing queuing, scheduling and congestion control guarantees to the frame according to what was configured for that specific QoS class. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority.

R

RARP

RARP is an acronym for **R**everse **A**ddress **R**esolution **P**rotocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.

RADIUS

RADIUS is an acronym for **R**emote **A**uthentication **D**ial In **U**ser **S**ervice. It is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

RDI

RDI is an acronym for **R**emote **D**efect **I**ndication. It is an OAM functionality that is used by a MEP to indicate defect detected to the remote peer MEP

Router Port

A router port is a port on the Ethernet switch that leads switch towards the Layer 3 multicast device.

RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of STP: the **R**apid **S**panning **T**ree **P**rotocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

S

SAMBA

Samba is a program running under UNIX-like operating systems that provides seamless integration between UNIX and Microsoft Windows machines. Samba acts as file and print servers for Microsoft Windows, IBM OS/2, and other SMB client machines. Samba uses the Server Message Block (SMB) protocol and Common Internet File System (CIFS), which is the underlying protocol used in Microsoft Windows networking.

Samba can be installed on a variety of operating system platforms, including Linux, most common Unix platforms, OpenVMS, and IBM OS/2.

Samba can also register itself with the master browser on the network so that it would appear in the listing of hosts in Microsoft Windows "Neighborhood Network".

SHA

SHA is an acronym for **S**ecure **H**ash **A**lgorithm. It designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.

Shaper

A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.

SMTP

SMTP is an acronym for **S**imple **M**ail **T**ransfer **P**rotocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.

SNAP

The SubNetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier.

SNMP

SNMP is an acronym for **S**imple **N**etwork **M**anagement **P**rotocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allow diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

SNTP

SNTP is an acronym for **S**imple **N**etwork **T**ime **P**rotocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.

SPROUT

Stack **P**rotocol using **ROU**ting **T**echnology. An advanced protocol for almost instantaneous discovery of topology changes within a stack as well as election of a master switch. SPROUT also calculates parameters for setting up each switch to perform shortest path forwarding within the stack.

SSID

Service **S**et **Id**entifier is a name used to identify the particular 802.11 wireless LANs to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their SSIDs, and can choose one to connect to based on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one (wikipedia).

SSH

SSH is an acronym for **S**ecure **SH**ell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality (Wikipedia).

SSM

SSM In SyncE this is an abbreviation for Synchronization Status Message and is containing a QL indication.

STP

Spanning **T**ree **P**rotocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.

SyncE

SyncE Is an abbreviation for Synchronous Ethernet. This functionality is used to make a network 'clock frequency' synchronized. Not to be confused with real time clock synchronized (IEEE 1588).

T

TACACS+

TACACS+ is an acronym for **T**erminal **A**ccess **C**ontroller **A**ccess **C**ontrol **S**ystem **P**lus. It is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

Tag Priority

Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame.

TCP

TCP is an acronym for **T**ransmission **C**ontrol **P**rotocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.

The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.

Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).

TELNET

TELNET is an acronym for **Tel**etype **Net**work. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client.

TELNET enables the client to control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if they were entering commands directly on the server console.

TFTP

TFTP is an acronym for **T**rivial **F**ile **T**ransfer **P**rotocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provides directory service and security features.

Toss

Toss is an acronym for **T**ype **o**f **S**ervice. It is implemented as the IPv4 Toss priority control. It is fully decoded to determine the priority from the 6-bit Toss field in the IP header. The most significant 6 bits of the Toss field are fully decoded into 64 possibilities, and the singular code that results is compared against the corresponding bit in the IPv4 ToS priority control bit (0~63).

TLV

TLV is an acronym for **T**ype **L**ength **V**alue. A LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as TLV.

TKIP

TKIP is an acronym for **T**emporal **K**ey **I**ntegrity **P**rotocol. It used in WPA to replace WEP with a new encryption algorithm. TKIP comprises the same encryption engine and RC4 algorithm defined for WEP. The key used for encryption in TKIP is 128 bits and changes the key used for each packet.

U

UDP

UDP is an acronym for **U**ser **D**atagram **P**rotocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

UPnP

UPnP is an acronym for **U**niversal **P**lug and **P**lay. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components

User Priority

User Priority is a 3-bit field storing the priority level for the 802.1Q frame.

V

VLAN

A method to restrict communication between switch ports. VLANs can be used for the following applications:

VLAN unaware switching: This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags.

VLAN aware switching: This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.

Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.

VLAN ID

VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.

Voice VLAN

Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

W

WEP

WEP is an acronym for **W**ired **E**quivalent **P**rivacy. WEP is a deprecated algorithm to secure IEEE 802.11 wireless networks. Wireless networks broadcast messages using radio, so are more susceptible to eavesdropping than wired networks. When introduced in 1999, WEP was intended to provide confidentiality comparable to that of a traditional wired network (Wikipedia).

Wi-Fi

Wi-Fi is an acronym for **Wi**reless **Fi**delity. It is meant to be used generically when referring of any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. The term is promulgated by the Wi-Fi Alliance.

WPA

WPA is an acronym for **W**i-Fi **P**rotected **A**ccess. It was created in response to several serious weaknesses researchers had found in the previous system , Wired Equivalent Privacy (WEP). WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is specifically designed to also work with pre-WPA wireless network interface cards (through firmware upgrades), but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards (Wikipedia).

WPA-PSK

WPA-PSK is an acronym for **W**i-Fi **P**rotected **A**ccess - **P**re **S**hared **K**ey. WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia)

WPA-Radius

WPA-Radius is an acronym for **W**i-Fi **P**rotected **A**ccess - Radius (802.1X authentication server). WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia)

WPS

WPS is an acronym for **W**i-Fi **P**rotected **S**etup. It is a standard for easy and secure establishment of a wireless home network. The goal of the WPS protocol is to simplify the process of connecting any home device to the wireless network (Wikipedia).

WRED

WRED is an acronym for **W**eighted **R**andom **E**arly **D**etection. It is an active queue management mechanism that provides preferential treatment of higher priority frames when traffic builds up within a queue. A frame's DP level is used as input to WRED. A higher DP level assigned to a frame results in a higher probability that the frame is dropped during times of congestion.

WTR

WTR is an acronym for **W**ait **T**o **R**estore. This is the time a fail on a resource has to be 'not active' before restoration back to this (previously failing) resource is done.