USER MANUAL

SWG 24AX

334201

24-port GE PoE+ managed switch with 4 SFP ports

ITS Partner O.B.S S.L · Av. Cerdanyola 79-81 Local C
08172 Sant Cugat del Vallés · Barcelona (Spain)
Phone:+34935839543 · info@ek.plus · www.ek.plus

Copyright

Disclaimer

The products, services, or features you purchase are subject to commercial contracts and terms. Some or all ofthe products, services or features described in this document may not be within the scope of your purchase or use. Unless otherwise agreed in the contract, Ekselans by ITS does not make any express or implied statementor guarantee for the content of this document.

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Ekselans by ITS reserves the right to modify the content of the document without any notice or prompt.

This manual is for reference only. Ekselans by ITS endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

Preface

Intended Audience

This document is intended for:

- Network engineers
- Technical support and servicing engineers
- Network administrators

Technical Support

- Company Website: https://www.ek.plus/
- Consult Website: https://www.ek.plus/contacto/
- Support Email: soporte@ek.plus

Conventions

1. Signs

The signs used in this document are described as follows:

❗ **Warning**

An alert that calls attention to important rules and information that if not understood or followed can result in data loss or equipment damage.

⚠ **Caution**

An alert that calls attention to essential information that if not understood or followed can result in function failure or performance degradation.

ℹ **Note**

An alert that contains additional or supplementary information that if not understood or followed will not lead to serious consequences.

✓ **Specification**

An alert that contains a description of product or version support.

2. Note

The manual offers configuration information (including model, port type and command line interface) for indicative purpose only. In case of any discrepancy or inconsistency between the manual and the actual version, the actual version prevails.

1 Product Overview

The SWG 24-AX switch is a next-generation intelligent switch that features high performance, high security, multiple services and ease of use to meet the needs of the current networks. The SWG 24-AX switch can provide the complete end-to-end Quality of Service (QoS), flexible and abundant security policies and policy-based network management for various networks. It is greatly ideal for such applications as campus network, enterprise network, government network, service network, residential broadband access and business building network, providing high-speed, high-efficiency, secure and intelligent access solutions.

Table 1-1 SWG 24-AX

Model	10/100/1000 Base-T Auto-sensing Ethernet Port	1000Base-X SFP Port	Console Port
SWG 24-AX	24 (All are PoE+ capable)	4	1

ⓘ 1000Base-T is compatible with 100Base-TX and 10Base-T in the downlink direction.

ⓘ For detailed information about the PoE capability, see the PoE description in the Technical Specifications table.

1.1 SWG 24-AX

Technical Specifications

Model	SWG 24-AX
CPU	Built-in CPU, single-core processor, 1GHz
Flash Memory	256MB
SDRAM	DDRIII 512MB
Optical Module	For details, see Appendix B.
SFP Port	Supports 1000Base-X modules. Does not support 100Base-FX.
Power Supply	● AC input Rated voltage range: 100V to 240V Maximum voltage range: 90V to 264V Frequency: 50/60 Hz Rated current: 6.8A ● HVDC input Voltage range: 192V to 290V Current range: 2.5A to 3.5A
Earth Leakage Current	≤ 0.5mA
EEE	Supported
PoE	All the RJ45 ports are PoE-capable. Ports 1-24 support the maximum power output of 30W.

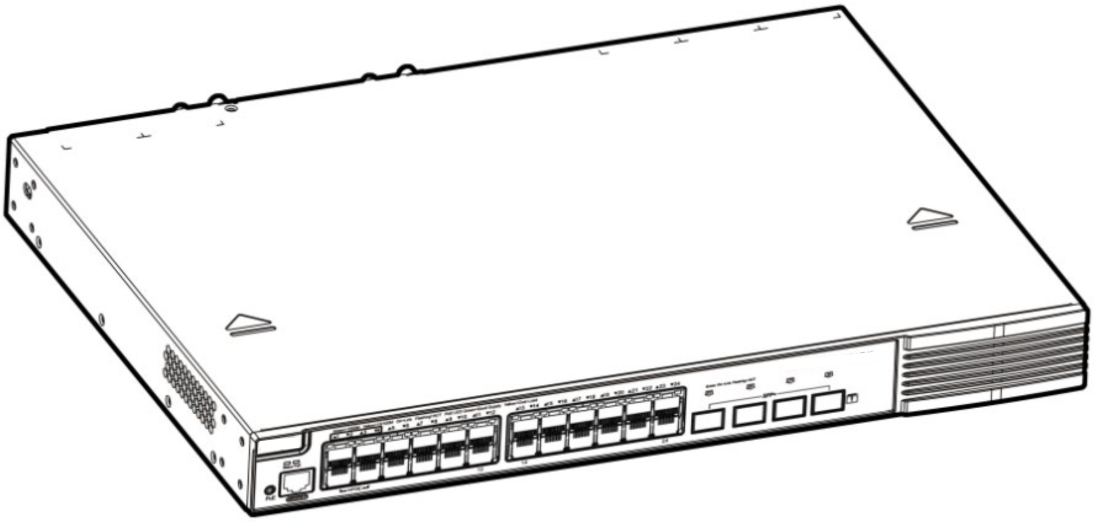
	The maximum output power of PoE/PoE+ is 370W. ⓘ The available number of PDs is determined by PSE output power and PD input power in practice.
Power Consumption	Less than 40W with no PoE load Less than 460W with PoE full load
Operating Temperature	0℃ to 50℃ (32°F to 122°F)
Storage Temperature	-40℃ to 70℃ (-40°F to 158°F)
Operating Humidity	10% to 90% RH
Storage Humidity	5% to 95% RH
Fan	Speed adjustment and fault alarm
Temperature Warning	Supported
EMCStandards	GB/T 9254.1
Security Standards	GB 4943.1
Dimensions (W x D x H)	440 mm x 260 mm x 44 mm
Weight	≤5.5 kg (with package)

⚠ In a domestic environment, this product may cause radio interference.

Product Appearance

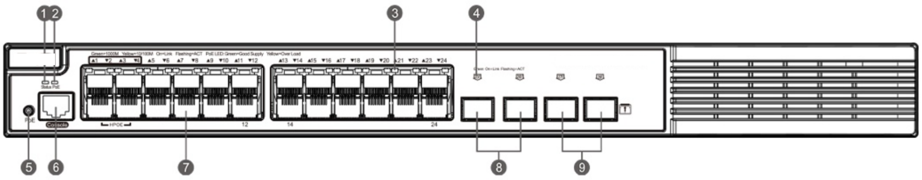
On the front panel, the SWG 24-X Ethernet switch provides 24 10/100/1000Base-T Ethernet ports, 4 SFP ports, and 1 Console port. On the back panel, it provides AC power ports.

Figure 1-1 Appearance of SWG 24-X



Front Panel

Figure 1-2 Front Panel of SWG 24-X

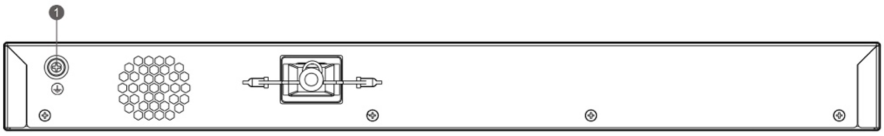


Note:	1. System status LED 2. PoE status LED 3. Copper port status LED 4. Fiber port status LED 5. PoE Mode Switch-Over Button	6. Console port 7. 10/100/1000Base-T auto-sensing Ethernet port 8. 1000Base-X SFP port 9. 1000Base-X SFP port

⚠ Long press PoE Mode Switch-Over Button for above 2 seconds to switch the display mode between PoE mode and port rate mode.

Back Panel

Figure 1-3 Back Panel of SWG 24-X



Note:	1. Grounding pole	

Power Supply

The SWG 24-X switch adopts AC or HVDC power input.

- AC input

Rated voltage range: 100V to 240V

Maximum voltage range: 90V to 264V

Frequency range: 50/60 Hz

Rated current: 6.8A

Power cord specification: 10A

- HVDC input

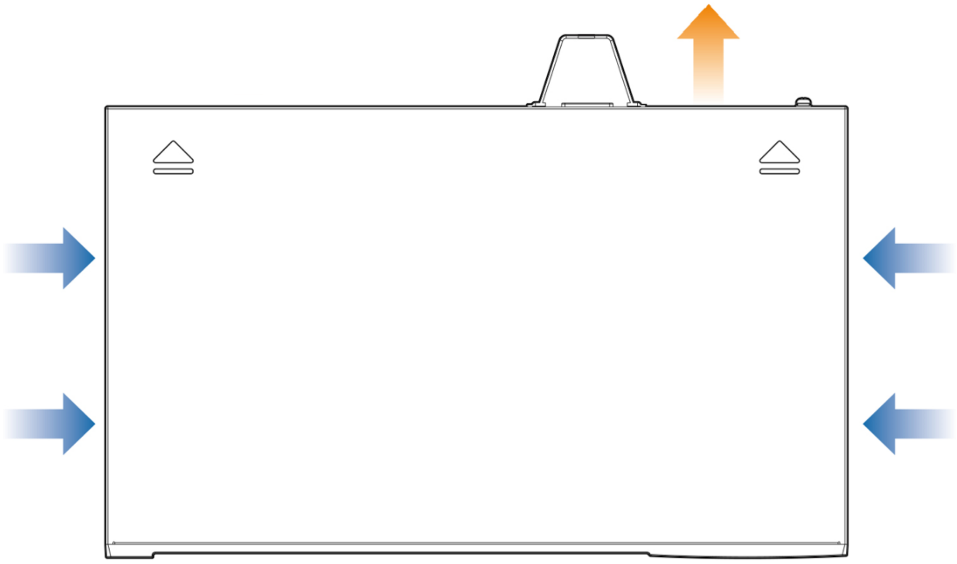
Voltage range: 192V to 290V

Current range: 2.5A to 3.5A

Heat Dissipation

The SWG 24-X adopts turbine fans for heat dissipation, thereby ensuring normal function of the device in the specified environment. 10 cm distance space should be reserved at both sides and the back plane of the cabinet to allow air circulation. It is recommended to clean the device once every 3 months to avoid dust from blocking vents. Figure 1-4 shows the flow scheme of heat dissipation.

Figure 1-4 Flow Scheme of Heat Dissipation



LEDs

LED	Panel Identification	State	Meaning
System status LED	Status	Off	The switch is not receiving power.
		Blinking green	The system is being initialized. Continuous blinking indicates errors.
		Solid green	The switch is operational.

		Solid yellow	Temperature warning Check the working environment of the switch immediately.
		Solid red	The switch is faulty.
PoE status LED	PoE	Solid green	Indicates the switching state.
		Solid yellow	Indicates the PoE state.
1000Mbps RJ-45 port status LED	1-24	Off	The port is not connected.
		Solid green	The port is connected at 1000 Mbps.
		Blinking green	The port is receiving or transmitting traffic at 1000 Mbps.
		Solid yellow	The port is connected at 10/100 Mbps.
		Blinking yellow	The port is receiving or transmitting traffic at 10/100 Mbps.
RJ45 port PoE status LED	1-24	Off	PoE is not enabled.
		Solid green	PoE is enabled. The port is operational.
		Solid yellow	The PoE port is abnormally operational.
1000Mbps SFP port status LED	25F-28F	Off	The port is not connected.
		Solid green	The port is connected at 1000 Mbps.
		Blinking green	The port is receiving or transmitting traffic at 1000 Mbps.

2 Preparation before Installation

2.1 Safety Suggestions

ℹ To avoid personal injury and equipment damage, please carefully read the safety suggestions before you install the SWG 24-X switch.

ℹ The following safety suggestions do not cover all possible dangers.

2.1.1 Installation

- Keep the chassis clean and free from any dust.
- Do not place the equipment in a walking area.
- Do not wear loose clothes or accessories that may be hooked or caught by the device during installation and maintenance.
- Turn off all power supplies and remove the power sockets and cables before installing or uninstalling the device.

2.1.2 Movement

- Do not frequently move the device.
- When moving the device, note the balance and avoid hurting legs and feet or straining the back.
- Before moving the device, turn off all power supplies and dismantle all power modules.

2.1.3 Electricity

- Observe local regulations and specifications when performing electric operations. Relevant operators must be qualified.
- Before installing the device, carefully check any potential danger in the surroundings, such as ungrounded power supply, and damp/wet ground or floor.
- Before installing the device, find out the location of the emergency power supply switch in the room. First cut off the power supply in the case of an accident.
- Try to avoid maintaining the switch that is powered-on alone.
- Be sure to make a careful check before you shut down the power supply.
- Do not place the equipment in a damp location. Do not let any liquid enter the chassis.

⚠ Any nonstandard and inaccurate electric operation may cause an accident such as fire or electrical shock, thus causing severe even fatal damages to human bodies and equipment.

⚠ Direct or indirect touch through a wet object on high-voltage and mains supply may bring a fatal danger.

⚠ If a power supply system is equipped with a leakage protector (also referred to as "leakage current switch" or "leakage current breaker"), the rated leakage action current of each leakage protector is greater than twice of the theoretical maximum leakage current of all the power supplies in the system. For example, if a system is equipped with sixteen identical power supplies, the leakage current of each power supply is equal to or less than 3.5mA, and the leakage current of the system totals 56mA. A leakage protector with 30mA rated action current supports less than five power supplies (that is, Action current of the leakage protector/2/Maximum leakage current of each power supply =30/2/3.5≈4.28). In other words, the leakage protector with 30mA rated action current supports no more than four power supplies. In this case, the sixteen power supplies in the system require at least four leakage protectors with 30mA rated action current and each leakage protector supports four power supplies. If power supplies in a system differ in models, the rated leakage action current of each leakage protector divided by two is greater than the sum of maximum leakage current of all the power supplies. The rated leakage non-action current of a leakage protector shall be 50% of the leakage action current. Take a leakage protector with 30mA rated leakage action current as an example. The rated leakage non-action current shall be 15mA. When the leakage current is below 15mA, the protector shall not act. Otherwise, misoperation may easily occur due to high sensitivity and thus the leakage protector trips, devices are powered off, and services are interrupted.

⚠ To guarantee personal safety, the rated leakage action current of each leakage protector in the system must be equal to or less than 30mA (human body safety current is 30mA). When twice of the total leakage current of the system is greater than 30mA, the system must be equipped with two or more leakage protectors.

⚠ For the leakage current value of power supply, see the parameter table in Chapter 1.

2.1.4 Static Discharge Damage Prevention

To prevent damage from static electricity, pay attention to the following:

- Proper grounding of grounding screws on the back panel of the device. Use of a three-wire single-phase socket with protective earth wire (PE) as the AC power socket.
- Indoor dust prevention
- Proper humidity conditions

2.1.5 Laser

The SWG 24-X switch supports varying models of optical modules sold on the market which are Class I laser products. Improper use of optical modules may cause damage. Therefore, pay attention to the following when you use them:

- When a fiber transceiver works, ensure that the port has been connected with an optical fiber or is covered with a dust cap, to keep out dust and avoid burning your eyes.
- When the optical module is working, do not pull out the fiber cable and stare into the transceiver interface or you may hurt your eyes.

⚠ Do not stare into any optical port under any circumstances, as this may cause permanent damage to your eyes.

2.1.6 Storage Security

To ensure the normal operation of the device, maintain a proper storage environment in accordance with the storage temperature/storage humidity requirements in the technical specifications table of the device.

⚠ If the storage time exceeds 18 months, you must power on the device and keep it running for 24 hours without interruption for device activation.

2.2 Installation Site Requirements

To ensure the normal working and a prolonged durable life of the equipment, the installation site must meet the following requirements.

2.2.1 Ventilation

For the SWG 24-X, a sufficient space (at least 10 cm distances from both sides and the back plane of the cabinet) should be reserved at the ventilation openings to ensure the normal ventilation. After various cables have been connected, they should be arranged into bundles or placed on the cabling rack to avoid blocking the air inlets. It is recommended to clean the switch at regular intervals (like once every 3 months). Especially, avoid dust from blocking the screen mesh on the back of the cabinet.

2.2.2 Temperature and Humidity

To ensure the normal operation and prolong the service life of SWG 24-X switch, you should keep proper temperature and humidity in the equipment room.

If the equipment room has temperature and humidity that do not meet the requirements for a long time, the equipment may be damaged.

- In an environment with high relative humidity, the insulating material may have bad insulation or even leak electricity. Sometimes the materials may suffer from mechanical performance change and metallic parts may get rusted.
- In an environment with low relative humidity, however, the insulating strip may dry and shrink. Static electricity may occur easily and endanger the circuit on the equipment.
- In an environment with high temperature, the equipment is subject to even greater harm, as its performance may degrade significantly, and various hardware faults may occur.

Therefore, the ambient temperature and humidity of the SWG 24-X must meet the requirements listed in Table 2-1:

Table 2-1 Temperature and Humidity Requirements of the SWG 24-X Switch

Temperature	Relative Humidity
0 °C to 50°C (32°F to 122°F)	10% to 90%

ⓘ The requirements for the sampling site of the temperature and humidity in the operating environment of the device are as follows:

There is no protective plate at the front or back of the equipment rack.

The vertical height is 1.5 m above the floor.

The distance from the front panel of the equipment is 0.4 m.

2.2.3 Cleanness

Dust poses a severe threat to the running of the equipment. The indoor dust falling on the equipment may be adhered by the static electricity, causing bad contact of the metallic joint. Such electrostatic adherence may occur more easily when the relative humidity is low, not only affecting the useful life of the equipment, but also causing communication faults. Table 2-2 shows the requirements for the dust content and granularity in the equipment room.

Table 2-2 Requirements for the Dust Content and Granularity in the Equipment Room

Dust	Unit	Density
Diameter≥0.5μm	Particles/m^3	$\leq 3.5\times10^6$
Diameter≥5μm	Particles/m^3	$\leq 3\times10^4$

Apart from dust, the salt, acid and sulfide in the air in the equipment room must also meet strict requirements, as such poisonous substances may accelerate the corrosion of the metal and the aging of some parts. The equipment room should be protected from the intrusion of harmful gases such as sulfur dioxide, sulfured hydrogen, nitrogen dioxide, and chlorine), whose requirements are listed in Table 2-3.

Table 2-3 Requirements for Harmful Gases in the Equipment Room

Gas	Average (mg/m^3)	Maximum (mg/m^3)
SO_2	0.3	1.0
H_2S	0.1	0.5
NO_2	0.5	1.0
Cl_2	0.1	0.3

Both average and maximum value are measured for a week. The switch cannot be placed in the environment with the maximum density for over 30 minutes every day.

2.2.4 Grounding

A good grounding system is the basis for the stable and reliable operation of the SWG 24-X switch. It is the chief condition to prevent lightning stroke and resist interference. Please carefully check the grounding conditions on the installation site according to the grounding requirements, and perform grounding operations properly as required.

Effective grounding of the switch is an important guarantee for lightning protection and interference resistance. Therefore, connect the grounding line of the switch properly.

Safety Grounding

The equipment using AC power supply must be grounded by using the yellow/green safety grounding cable. Otherwise, when the insulating resistance decreases the power supply and the enclosure in the equipment, electric shock may occur.

- ⚠ The building must provide protective grounding connection to ensure that the device is connected to the protection location.
- ⚠ The installation and maintenance personnel must check whether the A.C. socket is well connected to the protection location of the building, if not, they should use a protective grounding wire to connect the grounding end of the A.C. socket to the building's protection location.
- ⚠ Power cords should be connected to a grounded output socket.
- ⚠ The power supply socket must be installed in a place that is near to the device and where users can operate the device easily.
- ⚠ Before the installation of the device, make sure that ground connection is connected at first and disconnected finally.
- ⚠ The sectional area of the protective grounding wire should be at least 1 mm^2 (18 AWG).
- ⚠ Use the 3-core power supply line. The sectional area of each pin should be at least 1 mm^2 or 16 AWG.

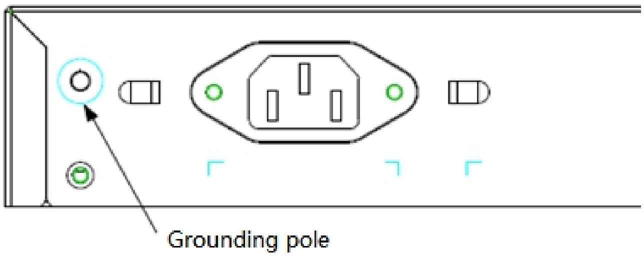
Lightning Grounding

The lightning protection system of a facility is an independent system that consists of the lightning rod, download conductor and the connector to the grounding system, which usually shares the power reference ground and yellow/green safety cable ground. The lightning discharge ground is for the facility only, irrelevant to the equipment.

EMC Grounding

The grounding required for EMC design includes shielding ground, filter ground, noise and interference suppression, and level reference. All the above constitute the comprehensive grounding requirements. The resistance of earth wires should be less than 1 ohm. The SWG 24-X switch back plane is reserved with one grounding pole, as shown in Figure 2-1.

Figure 2-1 Grounding of SWG 24-X



2.2.5 Lightning Resistance

When the AC power cable is imported outdoors and directly connected to the power port of the SWG 24-X switch, lightning line bank should be adopted to prevent the switch from being hit by lightning shocks. Usage of the lightning line bank: Connect the mains supply AC cable to the lightning line bank. Then, connect the switch to the lightning line bank. This can help to prevent the current of high-voltage lightning from passing the switch directly through the mains supply cable to a certain extent.

ⓘ The lightning line banks are not provided and should be purchased by users as required.
For the usage of lightning line banks, refer to their related manuals.

2.2.6 EMI

Electro-Magnetic Interference (EMI), from either outside or inside the equipment or application system, affects the system in the conductive ways such as capacitive coupling, inductive coupling, and electromagnetic radiation.

There are two types of electromagnetic interference: radiated interference and conducted interference, depending on the type of the transmission path.

When the energy, often RF energy, from a component arrives at a sensitive component via the space, the energy is known as radiated interference. The interference source can be either a part of the interfered system or a completely electrically isolated unit. Conducted interference results from the electromagnetic wire or signal cable connection between the source and the sensitive component, along which cable the interference conducts from one unit to another. Conducted interference often affects the power supply of the equipment but can be controlled by a filter. Radiated interference may affect any signal path in the equipment and is difficult to shield.

- For the AC power supply system TN, single-phase three-core power socket with protective earthing conductors (PE) should be adopted to effectively filter out interference from the power grid through the filtering circuit.
- The grounding device of the switch must not be used as the grounding device of the electrical equipment or anti-lightning grounding device. In addition, the grounding device of the switch must be deployed far away from the grounding device of the electrical equipment and anti-lightning grounding device.
- Keep the equipment away from high-power radio transmitter, radar transmitting station, and high-frequency large-current device.
- Measures must be taken to shield static electricity.
- Interface cables should be laid inside the equipment room. Outdoor cabling is prohibited, avoiding damages to device signal interfaces caused by over-voltage or over-current of lightning.

2.3 Requirements of Installation Tools

Table 2-4 List of Installation Tools

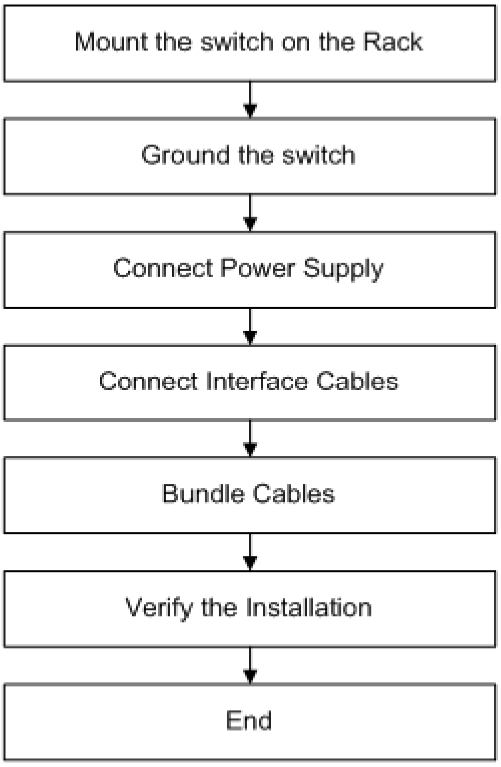
Common Tools	Phillips screwdriver, flathead screwdriver, related electric cables and optical cables, bolts, diagonal pliers, straps
Special Tools	Anti-static tools
Meters	Multimeter

ℹ The tool kit is customer-supplied.

3 Product Installation

Please ensure that you have carefully read Chapter 2.
Make sure that the requirements set forth in Chapter 2 have been met.

3.1 Installation Flowchart



3.2 Confirmations before Installation

Before installation, please confirm the following points:

- Whether ventilation requirements are met for the switch
- Whether the requirements of temperature and humidity are met for the switch
- Whether power cables are already laid out and whether the requirements of electrical current are met
- Whether related network adaption lines are already laid out

3.3 Installing the SWG 24-X

Precautions

During installation, note the following points:

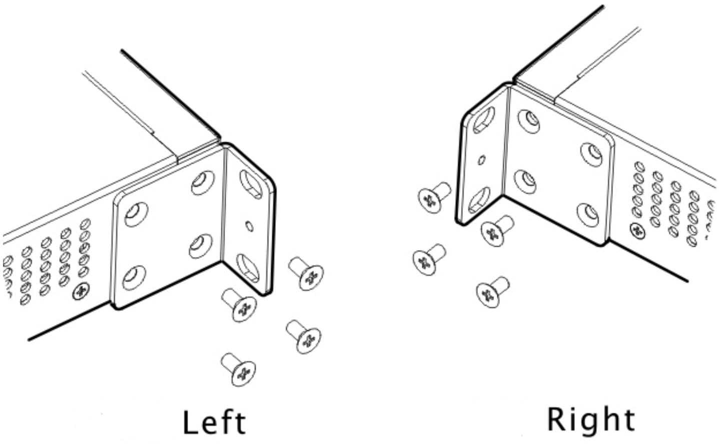
- Connect the power cables of different colors to the corresponding grounding posts.
- Ensure that the interface of the power supply cable is well connected to the power interface of the device. The power cables must be protected using power cable retention clips after they are connected to the device.
- Do not place any articles on the SWG 24-X switch.
- Reserve a spacing of at least 10 cm around the chassis for good ventilation. Do not stack the devices.
- The switch should be located at places free from the large power radio launch pad, radar launch pad, and high-frequency large-current devices. If necessary, electromagnetic shielding should be adopted. For example, use interface cables to shield cables.
- 100-meter network cables should be laid inside the equipment room and outdoor cabling of such cables is prohibited. If outdoor cabling is necessary, take relevant measures for lightning protection.

3.3.1 Mounting the Switch to a Standard 19-inch Rack

The SWG 24-X switch follow the EIA standard dimensions and can be installed in 19-inch distribution cabinets.

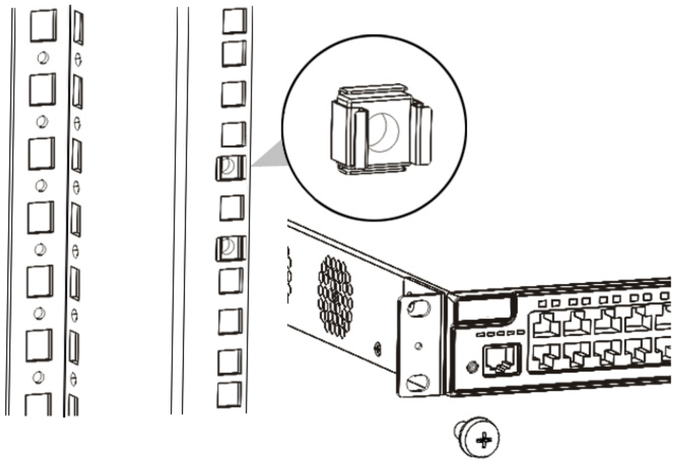
Attach the mounting brackets to the switch with the supplied screws, as shown in Figure 3-1.

Figure 3-1 Attaching the Mounting Bracket to the Switch



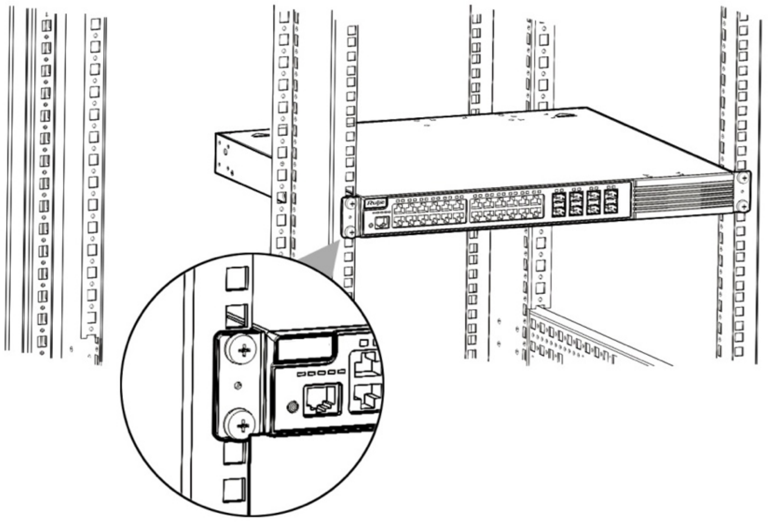
Align the mounting holes in the mounting bracket with the mounting holes in the rack, as shown in Figure 3-2.

Figure 3-2



Use the supplied M6 screws and cage nuts to securely attach the mounting brackets to the rack, as shown in Figure 3-3.

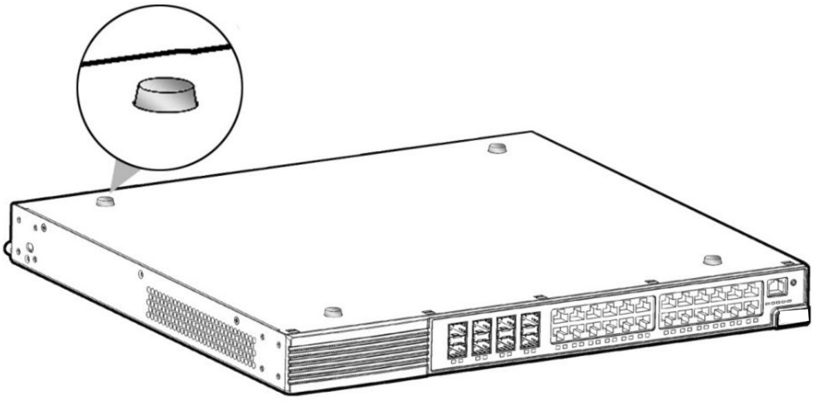
Figure 3-3



3.3.2 Mounting the Switch on a Table

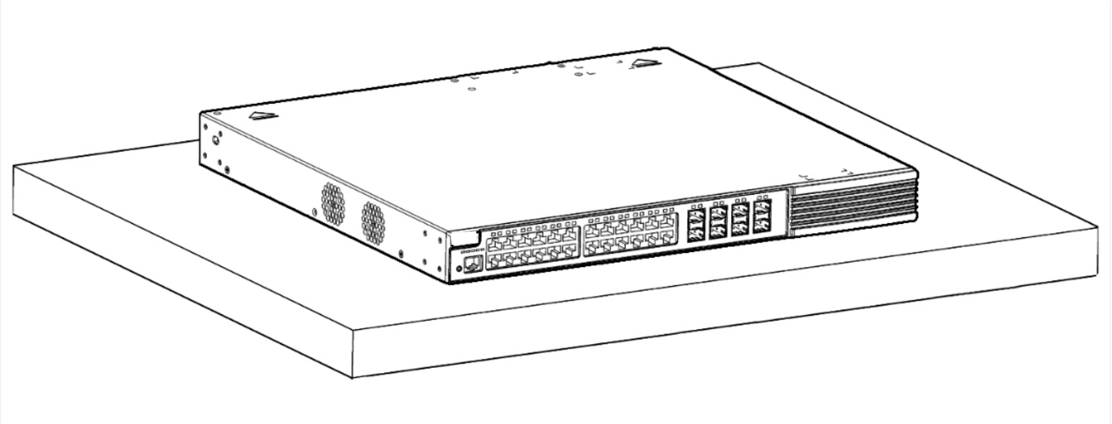
Attach the four rubber feet to the recessed areas on the bottom of the switch, as shown in Figure 3-4.

Figure 3-4 Attaching the Rubber Feet to the Recessed Areas



Place the switch on the table, as shown in Figure 3-5.

Figure 3-5 Mounting the Switch on the Table



⚠ The device must be installed and operated in the place that can restrict its movement.

3.4 Checking after Installation

⚠ Before checking the installation, switch off the power supply to avoid any personal injury or damage to the component due to connection errors.

- Check that the ground line is connected.
- Check that the cables and power input cables are correctly connected.
- Check that all interface cables are laid out inside the equipment room. In the case of external cabling, check that the lightning resistance socket or network interface lightning protector is connected.
- Check that sufficient airflow is available around the device (over 10 cm)

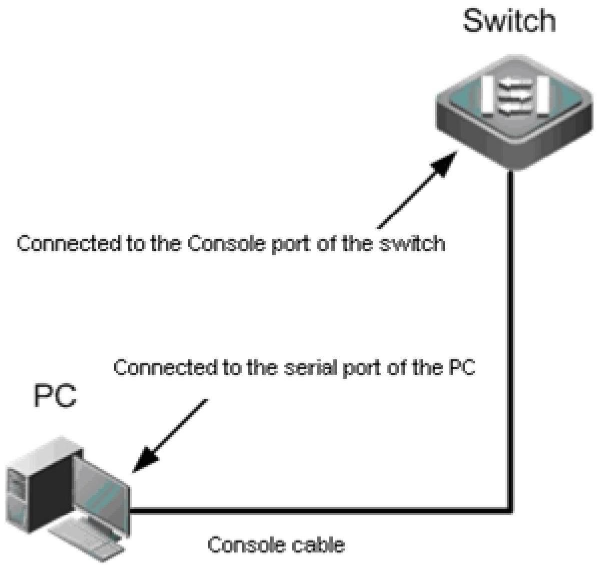
4 System Debugging

4.1 Establishing the Debugging Environment

Establishing the Debugging Environment

Connect the PC to the console port of the switch through the console cable, as shown in Figure 4-1.

Figure 4-1 Schematic Diagram of the Configuration Environment


Switch
Connected to the Console port of the switch
Connected to the serial port of the PC
PC
Console cable

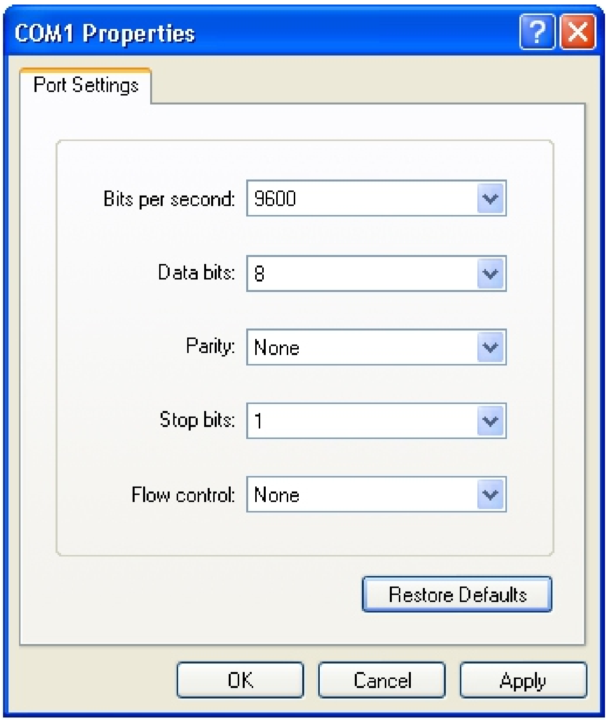
Connecting the Console Cable

- Step 1: Connect the end of the console cable with DB-9/USB jack to the serial port of the PC.
- Step 2: Connect the end of the console cable with RJ45 to the console port of the switch.

Setting HeperTerminal Parameters

- Step 1: Start the PC and run the terminal simulation program on the PC, such as HyperTerminal.
- Step 2: Set terminal parameters. The parameters are as follows: baud rate 9600, data bit 8, parity check none, stop bit 1, and flow control as none.

Figure 4-1



COM1 Properties

Port Settings

Bits per second: 9600

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

4.2 Startup Check

4.2.1 Checking before the Device is Powered on

- The switch is fully grounded.
- The power cable is correctly connected.
- The power supply voltage complies with the requirement of the switch.
- The control cable of the PC is properly connected to the console port of the switch. The HyperTerminal is started, and the parameter settings are correct.

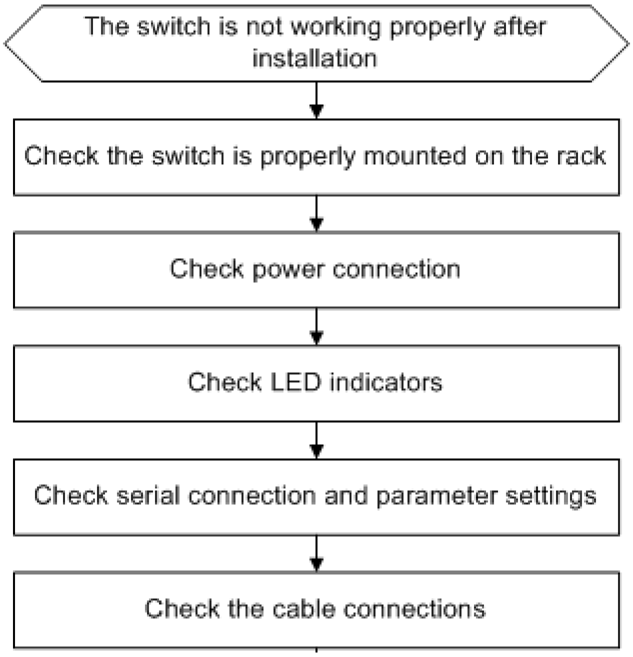
4.2.2 Checking after Program Startup (Recommended)

After power-on, you are recommended to perform the following checks to ensure the normal operation of follow-up configurations.

- Check whether information is displayed on the terminal interface.
- Check whether the status of the switch indicator is normal.
- Check whether the main program of the device is normally loaded.
- Check whether the time on the device is consistent with the current Beijing time.
- Check whether the service interface forwards data normally.

5 Maintenance and Troubleshooting

5.1 General Troubleshooting Procedure


The switch is not working properly after installation
Check the switch is properly mounted on the rack
Check power connection
Check LED indicators
Check serial connection and parameter settings
Check the cable connections

5.2 Troubleshooting Common Faults

Symptom	Possible Causes	Solution
Forgetting the management interface login password	A password is manually configured but it is forgotten.	Please contact EK for technical support.
The status indicator is not on after the switch is started.	The power supply module does not supply power. The power cable is in loose contact.	Check whether the power socket at the equipment room is normal and whether the power cable of the switch is in good contact.
The status indicator is red.	Fan alarm Temperature alarm	Check whether the fan stops working or is damaged. Temperature alarm: the switch already stops the normal service exchanges. Check in time the working environment of the switch, clean the dust on the cabinet and reinforce the refrigeration effect.

The serial port console has no output or outputs illegible characters.	The serial port connected to the switch does not match that opened by the configuration software. The serial port is not configured correctly.	Change the serial port opened by the configuration software to be the one connected to the switch. Check that the parameter configuration of the serial port matches that specified in the instructions.
The RJ45 port is not in connectivity, or it is erroneous in receiving/transmitting frames.	The connected twisted pair cable is faulty. The length of the cable exceeds 100 m. The port has special configuration that has no common working mode with the connected switch.	Replace the twisted pair cable. Check that the port configuration has the common working mode with the connected switch.
The fiber port cannot be connected.	The Rx and Tx ends are connected reversely. The interconnected optical module type does not match. The fiber type is not correct. The length of the optical fiber exceeds that rated of the optical module.	Switch the Rx and Tx ends of the optical fiber. Replace the optical module with one of the matched types. Replace the optical fiber with one of the appropriate types. Replace the optical fiber with one of the appropriate lengths.

Appendix A: Connectors and Connection Media

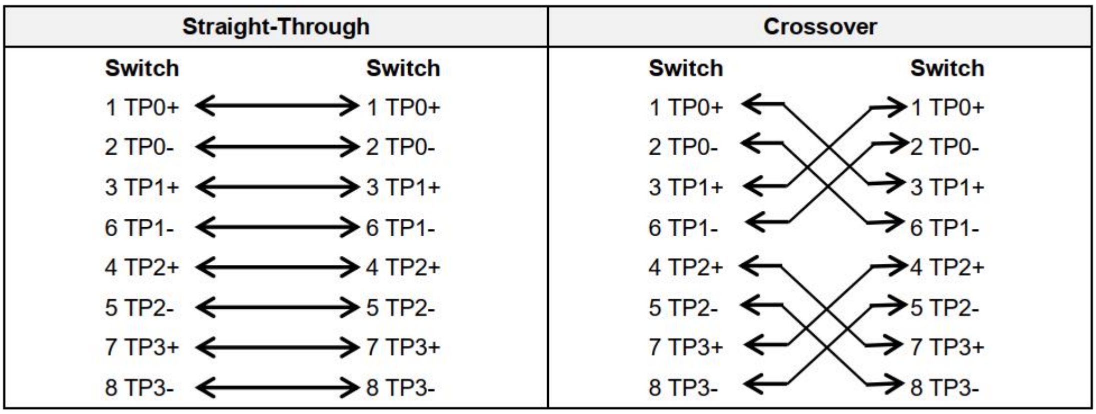
1000BASE-T/100BASE-TX/10BASE-T Ports

The 1000BASE-T/100BASE-TX/10BASE-T is a port that supports adaptation of three rates, and automatic MDI/MDIX Crossover at these three rates.

The 1000BASE-T complies with IEEE 802.3ab, and uses the cable of 100-ohm Category-5 or Supper Category-5 UTP or STP, which can be up to 100 m.

The 1000BASE-T port uses four pairs of wires for transmission, all of which must be connected. Figure A-1 shows the connections of the twisted pairs used by the 1000BASE-T port.

Figure A-1 Four Twisted Pairs of the 1000BASE-T



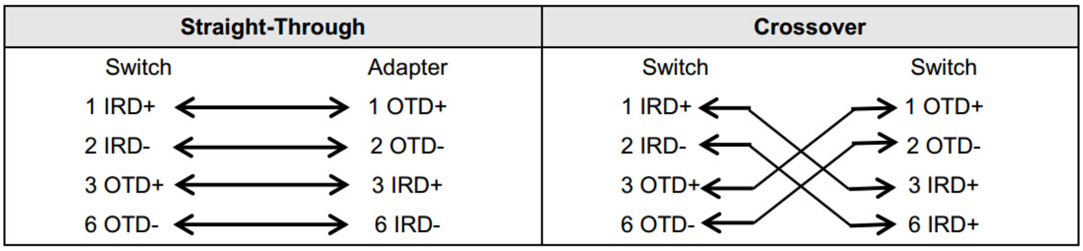
In addition to the above cables, the 100BASE-TX/10BASE-T can also use 100-ohm Category-3, 4, 5 cables for 10 Mbps, and 100-ohm Category-5 cables for 100 Mbps, both of which can be up to 100 m. Figure A-2 shows the pinouts of the 100BASE-TX/10BASE-T.

Figure A-2 Pinouts of the 100BASE-TX/10BASE-T

Pin	Socket	Plug
1	Input Receive Data+	Output Transmit Data+
2	Input Receive Data-	Output Transmit Data-
3	Output Transmit Data+	Input Receive Data+
6	Output Transmit Data-	Input Receive Data-
4,5,7,8	Not used	Not used

Figure A-3 shows the straight-through and crossover cable connections for the 100BASE-TX/10BASE-T.

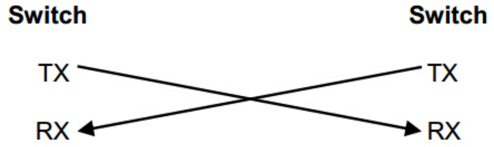
Figure A-3 Connections of the Twisted Pairs of the 100BASE-TX/10BASE-T



Optical Fiber Connection

For the optical fiber ports, select single-mode or multiple-mode optical fibers for connection according to the fiber module connected. The connection schematic diagram is shown in Figure A-4:

Figure A-4 Optical Fiber Connections



Appendix B: Mini-GBIC and SPF+ Module

SFP modules (Mini-GBIC module) are available to address the requirements of interface types of switch modules. You can select the Mini-GBIC module to suit your specific needs. The models and technical specifications of some Mini-GBIC SFP modules are listed below.

Table B-1 Models and Technical Specifications of the 1000M Mini-GBIC(SFP) Module

Model	Wavelength (nm)	Media Type	DDM (Yes/No)	Intensity of Transmitted Light (dBm)		Intensity of Received Light (dBm)	
				Min	Max	Min	Max
MINI-GBIC-SX-MM850	850	MMF	No	-9.5	-3	-17	0
MINI-GBIC-LX-SM1310	1310	SMF	No	-9.5	-3	-20	-3
GE-SFP-SX	850	MMF	No	-9.5	-3	-17	0
GE-SFP-LX	1310	SMF	No	-9.5	-3	-20	-3
GE-SFP-SX-SM1550-BIDI	1550TX/1310RX	MMF	No	-10	-5	-17	-3
GE-SFP-SX-SM1310-BIDI	1310TX/1550RX	MMF	No	-10	-5	-17	-3
GE-eSFP-SX-MM850	850	MMF	Yes	-9.5	-3	-17	0
GE-eSFP-LX-SM1310	1310	SMF	Yes	-9.5	-3	-20	-3
GE-SFP-LX-SM1310	1310	SMF	No	-9.5	-3	-20	-3
GE-SFP-LX20-SM1310-BIDI	1310TX/1550RX	SMF	Yes	-9	-3	-20	-3
GE-SFP-LX20-SM1550-BIDI	1550TX/1310RX	SMF	Yes	-9	-3	-20	-3
GE-SFP-LH40-SM1310-BIDI	1310TX/1550RX	SMF	Yes	-5	0	-24	-1
GE-SFP-LH40-SM1550-BIDI	1550TX/1310RX	SMF	Yes	-5	0	-24	-1
MINI-GBIC-LH40-SM1310	1310	SMF	Yes	-2	3	-22	-3
MINI-GBIC-ZX50-SM1550	1550	SMF	Yes	-5	0	-22	-3
MINI-GBIC-ZX80-SM1550	1550	SMF	Yes	0	4.7	-22	-3
MINI-GBIC-ZX100-SM1550	1550	SMF	Yes	0	5	-30	-9

Table B-2 Models of 1000M SFP Copper Module

Standard	Model	DDM (Yes/No)
1000Base-T	Mini-GBIC-GT	No

Table B-3 Module Cabling Specification

Model	Interface Type	Fiber Type	Core Size(μm)	Cable Distance (Max.)
MINI-GBIC-SX-MM850	LC	MMF	62.5/125	275m
			50/125	550m

MINI-GBIC-LX-SM1310	LC	SMF	9/125	10km
GE-eSFP-SX-MM850	LC	MMF	62.5/125	275m
			50/125	550m
GE-eSFP-LX-SM1310	LC	SMF	9/125	10km
GE-SFP-LX-SM1310	LC	SMF	9/125	10km
MINI-GBIC-LH40-SM1310	LC	SMF	9/125	40km
GE-SFP-SX-SM1310-BIDI	LC	MMF	50/125	500m
GE-SFP-SX-SM1550-BIDI	LC	MMF	50/125	500m
GE-SFP-LX20-SM1310-BIDI	LC	SMF	9/125	20km
GE-SFP-LX20-SM1550-BIDI	LC	SMF	9/125	20km
GE-SFP-LH40-SM1310-BIDI	LC	SMF	9/125	40km
GE-SFP-LH40-SM1550-BIDI	LC	SMF	9/125	40km
MINI-GBIC-ZX50-SM1550	LC	SMF	9/125	50km
MINI-GBIC-ZX80-SM1550	LC	SMF	9/125	80km
MINI-GBIC-ZX100-SM1550	LC	SMF	9/125	100km
SDH155-SFP-SX-MM850	LC	MMF	62.5/125	500m
SDH155-SFP-SX-MM1310	LC	MMF	62.5/125	2km
SDH155-SFP-LH15-SM1310	LC	SMF	9/125	15km
SDH155-SFP-LH40-SM1310	LC	SMF	9/125	40km
SDH155-SFP-LH80-SM1310	LC	SMF	9/125	80km
GE-SFP-SX	LC	MMF	62.5/125	275m
			50/125	550m
GE-SFP-LX	LC	SMF	9/125	10km
Mini-GBIC-GT	RJ45	Category 5 (or above) UTP or STP		100m

ⓘ For the optical module with transmission distance exceeding 40 km and more, one on-line optical attenuator should be added on the link to avoid the overload of the optical receiver when short single-mode optical fibers are used.

⚠ Optical modules generate laser. Do not stare at light source.

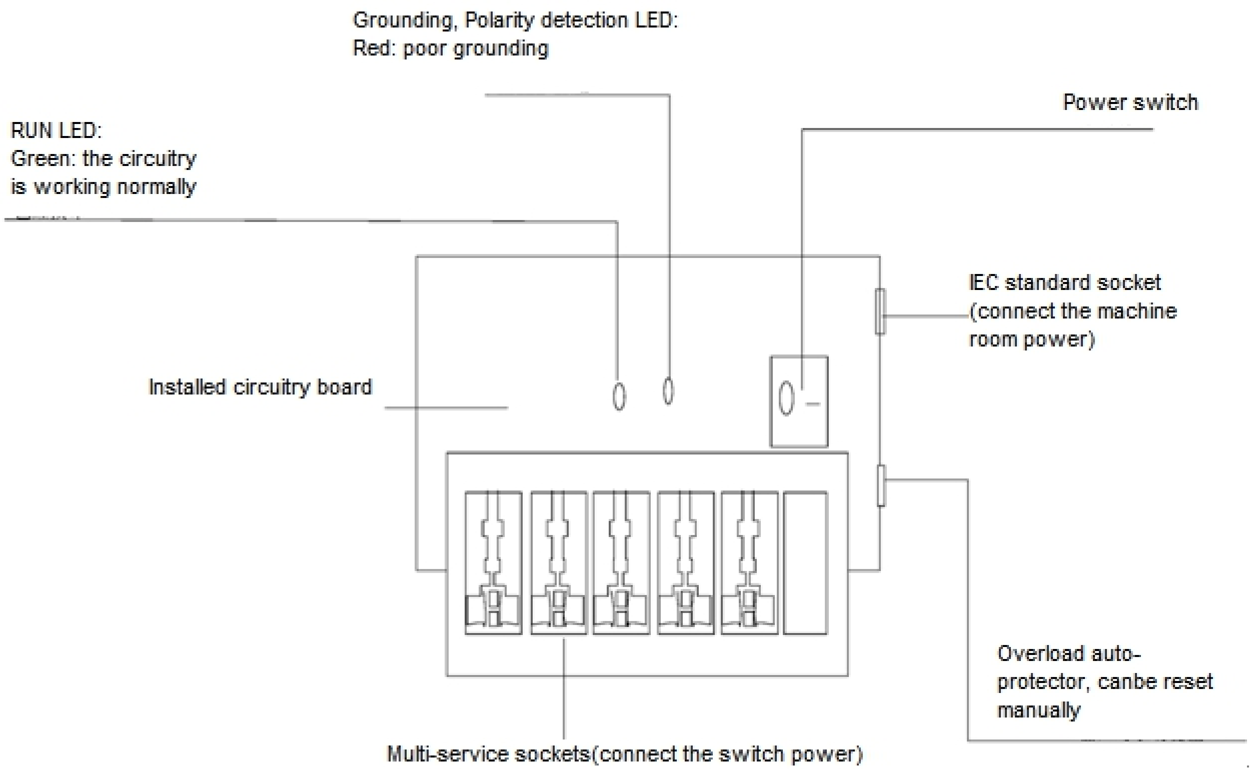
⚠ To keep optical modules clean, please use dust caps when the modules are not connected with fibers.

Appendix C: Lightning Protection

Installing AC Power Arrester (lightning protection cable row)

The external lightning protection cable row shall be used on the AC power port to prevent the switch from being struck by lightning when the AC power cable is introduced from the outdoor and directly connected to the power port of the switch. The lightning protection cable row is fixed on the cabinet, operating table or the wall in the machine room using the line buttons and screws.

Figure C-1 Schematic Diagram for the Power Arrester



The power arrester is not provided, and the user shall purchase it to address the practical requirement.

Precautions for installation:

- Make sure that the PE terminal of the power arrester has been well-grounded.
- After connecting the switch AC power plug to the socket of the power arrester (lightning protection cable row), lightning protection function implements if the RUN LED is Green, and the ALARM LED is OFF.
- If the ALARM LED on the power arrester is Red, you shall check what the reason is, poor grounding connection or the reversed connection of the Null and Live lines: Use the multimeter to check the polarity of the power socket for the arrester when the LED is Red, if the N line is on the left and the L line is on the right, the arrester PE terminal is not grounded; if the L line is on the left and the N line is on the right, the polarity of the arrester power cable shall be reversed; if the LED is still Red, it is confirmed that the arrester PE terminal has not been grounded.

Installing the Ethernet Port Arrester

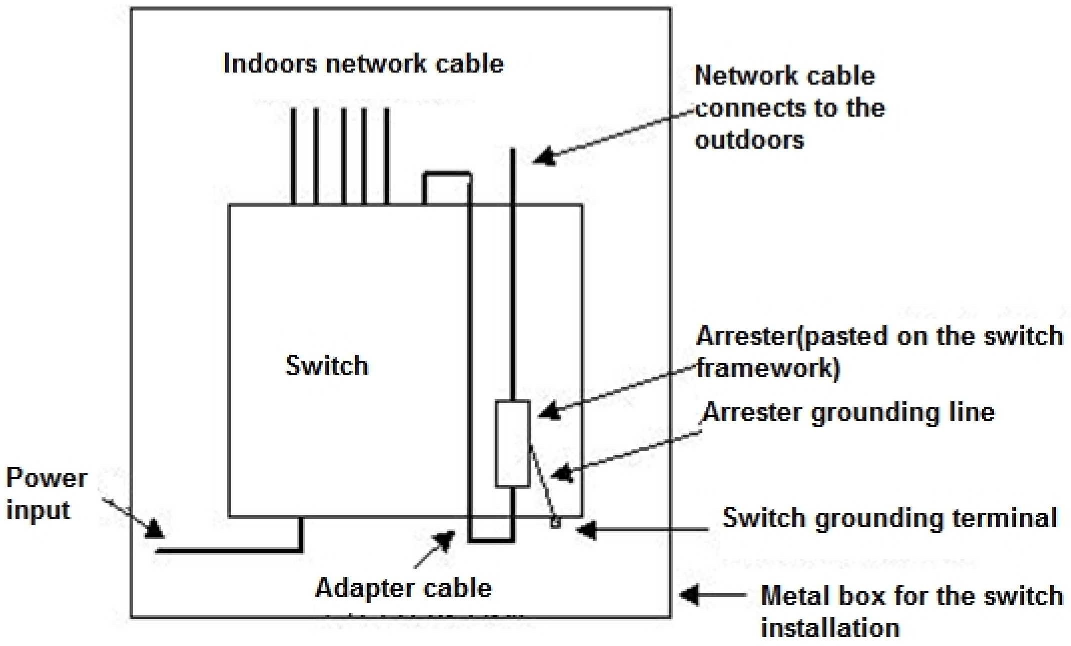
During the switch usage, the Ethernet port arrester shall be connected to the switch to prevent the switch damage by lightning before the outdoor network cable connects to the switch.

Tools: Cross or straight screwdriver, Multimeter, Diagonal pliers

Installation Steps:

1. Tear one side of the protection paper for the double-sided adhesive tape and paste the tape to the framework of the Ethernet port arrester. Tear the other side of the protection paper for the double-sided adhesive tape and paste the Ethernet port arrester to the switch framework. The paste location for the Ethernet port arrester shall be as close to the grounding terminal of the switch.
Based on the distance of the switch grounding terminal, cut the grounding line for the Ethernet port arrester and firmly tighten the grounding line to the grounding terminal of the switch.
Use the multimeter to check whether the grounding line for the arrester is in good contact with the switch grounding terminal and the framework.
According to the description on the Ethernet Port Arrester Hardware Installation Guide, connect the arrester using the adapter cable (note that the external network cable is connected to the end of IN, while the adapter cable connected to the switch is connected to the end of OUT) and observe whether the LED on the board is normal or not.
Use the nylon button to bundle the power cables.

Figure C-2 Schematic Diagram for the Ethernet port Arrester Installation


Indoors network cable
Network cable connects to the outdoors
Switch
Arrester(pasted on the switch framework)
Arrester grounding line
Power input
Switch grounding terminal
Adapter cable
Metal box for the switch installation

The Ethernet port arrester is only for the 10M/100M copper Ethernet ports with the RJ-45 connector.

The Ethernet port arrester is not provided, the user can purchase them to address their own practical requirements. For the detailed information during the arrester installation, please refer to Ethernet Port Arrester Hardware Installation Guide, which contains the technical specification and the maintenance and installation of the arrester.

You may pay attention to the following conditions during the actual installation to avoid influencing the performance of the Ethernet port arrester:

- Reversed direction of the arrester installation. You shall connect the external network cable to the "IN" end and connect the switch Ethernet port to the "OUT" end.
- Poor arrester grounding. The length of the grounding line should be as short as possible to ensure that it is in good contact with the switch grounding terminal. Use the multimeter to confirm the contact condition after the grounding.
- Incomplete arrester installation. If there is more than one port connected to the peer device on the switch, it needs to install the arresters on all connection ports for the purpose of the lightning protection.

Appendix D: Cabling Recommendations in Installation

When SWG 24-X switches are installed in standard 19-inch cabinets, the cables are tied in the binding rack on the cabinet by the cabling rack, and top cabling or bottom cabling is adopted according to the actual situation in the equipment room. All cable connectors should be placed at the bottom of the cabinet in an orderly manner instead of outside the cabinet easy to touch. Power cables are routed beside the cabinet, and top cabling or bottom cabling is adopted according to the actual situation in the equipment room, such as the position of the DC power distribution box, AC socket, or lightning protection box.

Requirement for the minimum cable bend radius

- The bend radius of a power cord, communication cable, and flat cable should be greater than five times their respective diameters. The bend radius of these cables that often bend or suffer removal/insertion should be greater than seven times their respective diameters.
- The bend radius of a common coaxial cable should be greater than seven times its diameter. The bend radius of this type of cables that often bend or suffer removal/insertion should be greater than 10 times its diameter.
- The bend radius of a high-speed cable (SFP cable, for example) should be greater than five times its diameter. The bend radius of this type of cables that often bend or suffer removal/insertion should be greater than 10 times its diameter.

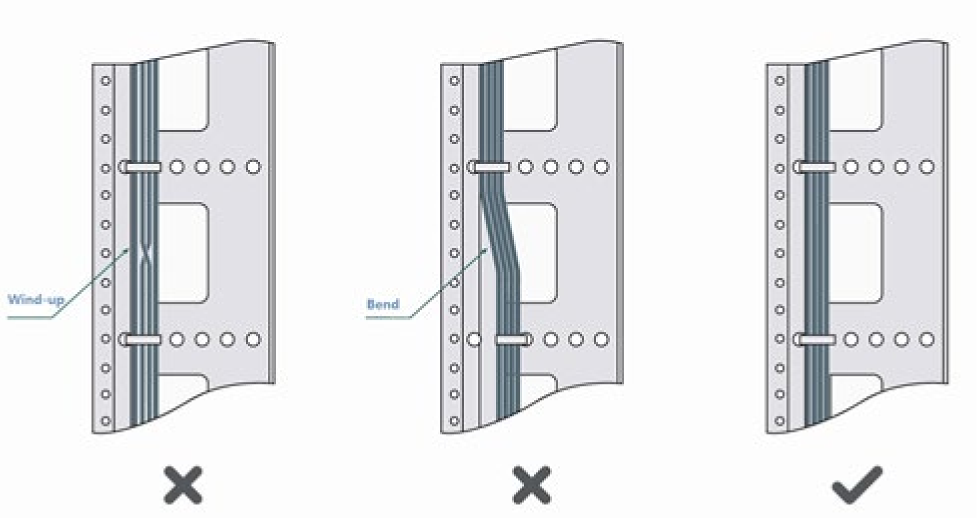
Requirement for the minimum fiber bend radius

- The diameter of a fiber tray to hold fibers cannot be less than 25 times the diameter of the fiber.
- When moving an optical fiber, the bend radius of the fiber should be equal to or greater than 20 times the diameter of the fiber.
- During cabling of an optical fiber, the bend radius of the fiber should be equal to or greater than 10 times the diameter of the fiber.

Precautions for Bundling up Cables

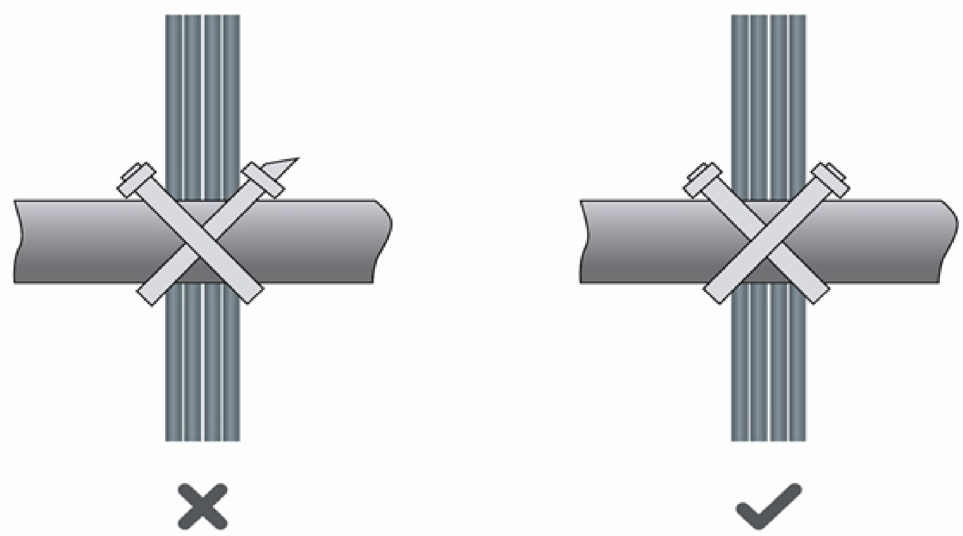
- Before bundling cables, correctly mark labels and stick the labels to cables where appropriate.
- Cables should be neatly and properly bundled, as shown in Figure D-1.

Figure D-1 Bundling Up Cables (1)



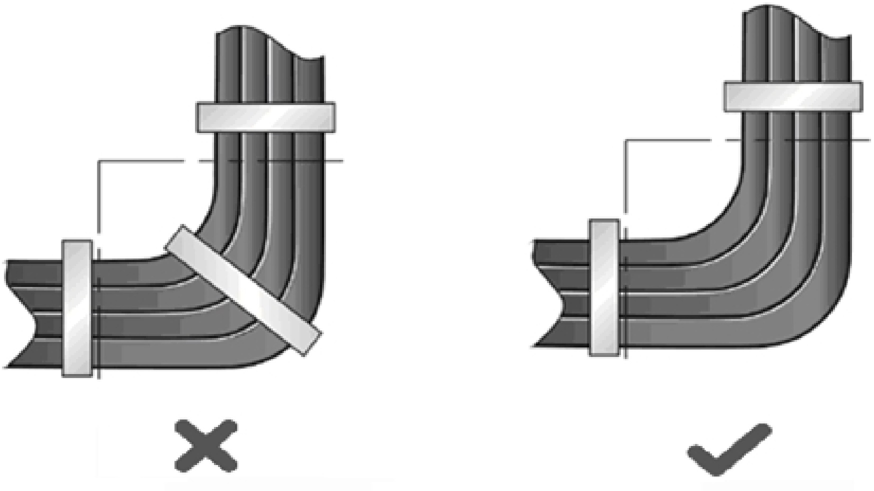
- Cables of different types (such as power cords, signal cables, and grounding cables) should be separated in cabling and bundling. When they are close, crossover cabling can be adopted. In the case of parallel cabling, power cords and signal cables should maintain a space equal to or greater than 30 mm.
- The binding rack and cabling slot inside and outside the cabinet should be smooth, without sharp corners.
- The metal hole traversed by cables should have a smooth and fully rounding surface or an insulated lining.
- Proper buckles should be selected to bundle up cables. It is forbidden to connect two or more buckles to bundle up cables.
- After bundling up cables with buckles, you should cut off the remaining part. The cut should be smooth and trim, without sharp corners, as shown in Figure D-2.

Figure D-2 Bundling Up Cables (2)



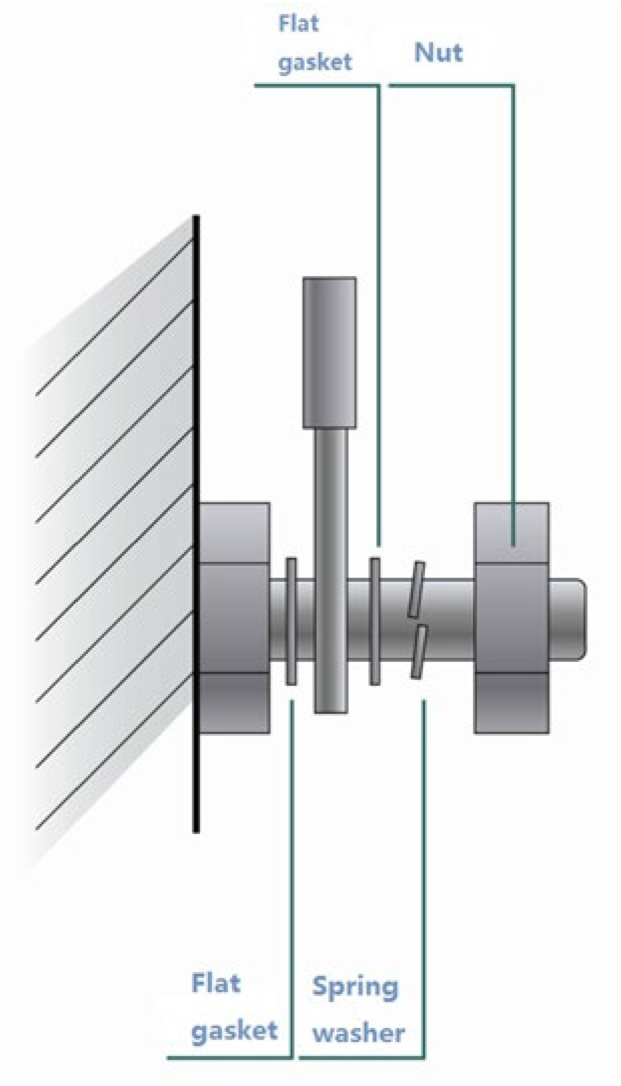
- When cables need to bend, you should first bundle them up. However, the buckle cannot be bundled within the bend area. Otherwise, significant stress may be generated in cables, breaking cable cores. As shown in Figure D-3.

Figure D-3 Bundling Up Cables (3)



- Cables not to be assembled or remaining parts of cables should be folded and placed in a proper position of the cabinet or cabling slot. The proper position indicates a position that will not affect device running or cause device damage or cable damage during commissioning.
- The power cords cannot be bundled on the guide rails of moving parts.
- The power cables connecting moving parts such as door grounding wires should be reserved with some access after assembled. When the moving part reaches the installation position, the remaining part should not touch heat sources, sharp corners, or sharp edges. If heat sources cannot be avoided, high-temperature cables should be used.
- When using screw threads to fasten cable terminals, the bolt or screw must be tightly fastened, and anti-loosening measures should be taken, as shown in Figure D-4.

Figure D-4 Cable Fastening



- The hard power cable should be fastened by the terminal connection area to prevent stress.
- Do not use self-tapping screws to fasten terminals.
- Power cables of the same type and in the same cabling direction should be bundled up into cable bunches, with cables in cable bunches clean and straight.
- Binding by using buckles should be performed according to Table D-1.

Cable Bunch Diameter (mm)	Binding Space (mm)
10	80-150
10-30	150-200
30	200-300

- No knot is allowed in cabling or bundling.
- For solder-less terminal blocks (such as air switches) of the cold pressing terminal type, the metal part of the cold pressing terminal should not be exposed outside the terminal block when assembled

Appendix E: Site Selection

- The machine room should be at least 5km away from the heavy pollution source such as the smelter, coal mine and thermal power plant, 3.7km away from the medium pollution source such as the chemical industry, rubber industry and electroplating industry, and 2km away from the light pollution source such as the food manufacturer and leather plant. If the pollution source is unavoidable, the machine room should be located on the windward side of the pollution source perennially with advanced protection.
- The machine room should be at least 3.7km away from the sea or salt lake. Otherwise, the machine room must be sealed, with air conditioner installed for temperature control. Saline soil cannot be used for construction. Otherwise, you should select devices with advanced protection against severe environment.
- Do not build the machine room in the proximity of livestock farms. Otherwise, the machine room should be located on the windward side of the pollution source perennially. The previous livestock house or fertilizer warehouse cannot be used as the machine room.
- The machine room should be firm enough to withstand severe weather conditions such as windstorm and heavy rain as well as away from dust. If the dust is unavoidable, keep the door and window away from the pollution source.
- The machine room should be away from the residential area. Otherwise, the machine room should meet the construction standard in terms of noise.
- Make sure the air vent of the machine room is away from the sewage pipe, septic tank, and sewage treatment tank. Keep the machine room under positive pressure to prevent corrosive gas from entering the machine room to corrode components and circuit boards. Keep the machine room away from industrial boiler and heating boiler.
- The machine room had better be on the second floor or above. Otherwise, the machine room floor should be 600mm higher than the highest flood level ever recorded.
- Make sure there are no cracks or holes in the wall and floor. If there are cable entries in the wall or window, take proper sealing measures. Ensure that the wall is flat, wear-resistant, and dust-free, which should be up to the standard for flame retarding, soundproofing, heat absorption, dust reduction, and electromagnetic shielding.
- Keep the door and the window closed to make the machine room sealed.
- The steel door is recommended for soundproofing.
- Sulfur-containing materials are forbidden.
- Pay attention to the location of the air conditioner. Keep the air conditioner from blowing wind straight toward the device or blowing water drops from the window or air vent toward the device.

EKSELANS BY ITS

USER MANUAL Web

SWG 24AX

334201

24-port GE PoE+ managed switch
with 4 SFP ports

ITS Partner O.B.S S.L · Av. Cerdanyola 79-81 Local C
08172 Sant Cugat del Vallés · Barcelona (Spain)
Phone:+34935839543 · info@ek.plus · www.ek.plus

Copyright

Disclaimer

The products, services, or features you purchase are subject to commercial contracts and terms. Some or all ofthe products, services or features described in this document may not be within the scope of your purchase or use. Unless otherwise agreed in the contract, Ekselans by ITS does not make any express or implied statementor guarantee for the content of this document.

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Ekselans by ITS reserves the right to modify the content of the document without any notice or prompt.

This manual is for reference only. Ekselans by ITS endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

Preface

Intended Audience

This document is intended for:

- Network engineers
- Technical support and servicing engineers
- Network administrators

Technical Support

- Company Website: https://www.ek.plus/
- Consult Website: https://www.ek.plus/contacto/
- Support Email: soporte@ek.plus

Conventions

1. Signs

The signs used in this document are described as follows:

Warming

An alert that calls attention to important rules and information that if not understood or followed can result in data loss or equipment damage.

Caution

An alert that calls attention to essential information that if not understood or followed can result in function failure or performance degradation.

Note

An alert that contains additional or supplementary information that if not understood or followed will not lead to serious consequences.

Specification

An alert that contains a description of product or version support.

2. Note

The manual offers configuration information (including model, port type and command line interface) for indicative purpose only. In case of any discrepancy or inconsistency between the manual and the actual version, the actual version prevails.

1 Configuring Switch Web

1.1 Overview

You can access the web management system (that is, Web) of switches through a browser, such as Chrome, to manage the switches.

Web management involves the web server and web client. The web server, integrated into a switch, is used to receive and process requests from a client (reading web files or executing commands), and return processing results to the client. The web client is usually a web browser, such as Chrome.

✓ **Specification**

This document applies only to SWG 24-AX switches.

1.2 Application

Table 1-1

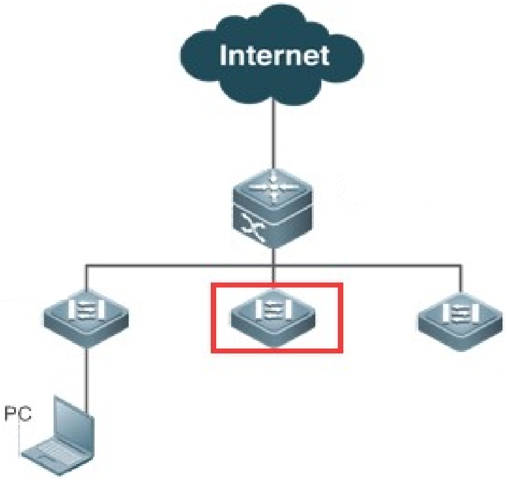
Application	Description
Managing Switches through the Web	After switches are configured, you can access the Web through a browser.

1.2.1 Managing Switches through the Web

1. Scenario

As shown in Figure 1-1, you can access the web of an access switch or aggregation switch through a browser to manage and configure the switch.

Figure 1-1



Note

The device enclosed in the red rectangle in Figure 1-1 is the access switch. Ensure that the switch can be pinged successfully from the PC. Then you can access the Web of the switch.

2. Deployment

(1) Configuration Environment

RequirementsClient requirements:

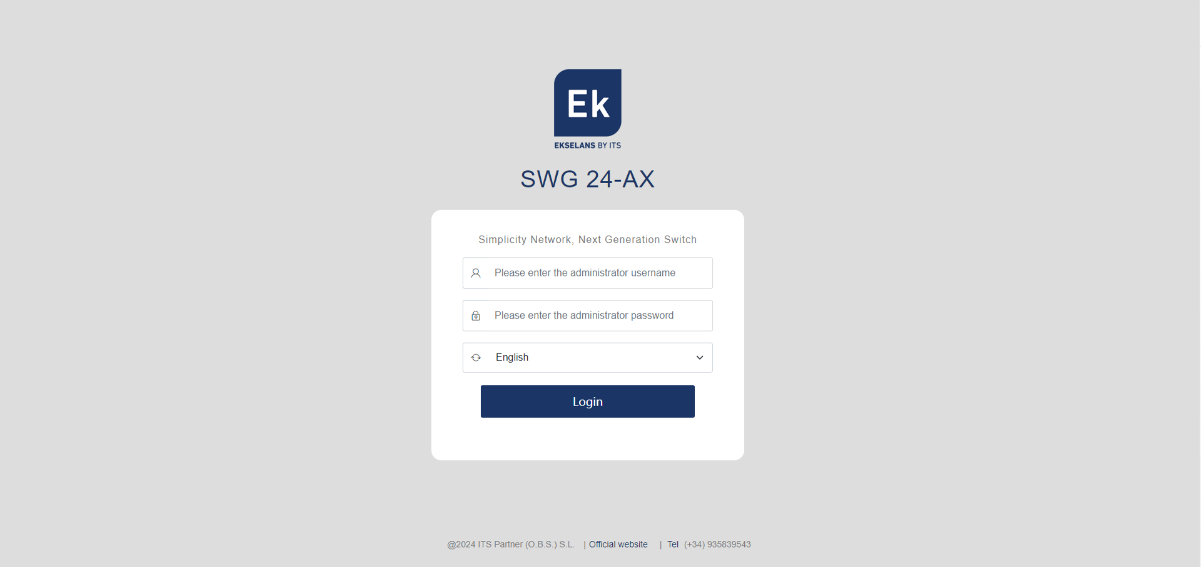
- You can manage the switch by logging in to the web management interface of the switch through the browser of the web management client. Clients refer to PCs or other mobile terminals such as laptops.
- Browser: IE8–IE11, Google Chrome, and 360 Browsers are supported. Exceptions such as garble or format errors may occur if an unsupported browser is used.
- Resolution: The recommended resolution is 1024*768, 1280*1024, 1440*960, or 1920*1080. If other resolutions are used, exceptions such as format errors or misalignment occur.

Web configuration and command line interface (CLI) configuration can be performed simultaneously. After CLI configuration is complete, enter the write command to save the configuration. If you open the web page, refresh the page to ensure that Web and CLI configurations are synchronized.

(2) Logging In to the Web Management Platform

Enter http://X.X.X.X (management IP address) in the browser and press Enter to access the **Login** page, as shown in Figure 1-2.

Figure 1-2 Login Page


Ek
EKSELANS BY ITS
SWG 24-AX
Simplicity Network, Next Generation Switch
Please enter the administrator username
Please enter the administrator password
English
Login
@2024 ITS Partner (O.B.S.) S.L. | Official website | Tel (+34) 935839543

Enter the username and password and click **Login**. The following table provides the default username and password.

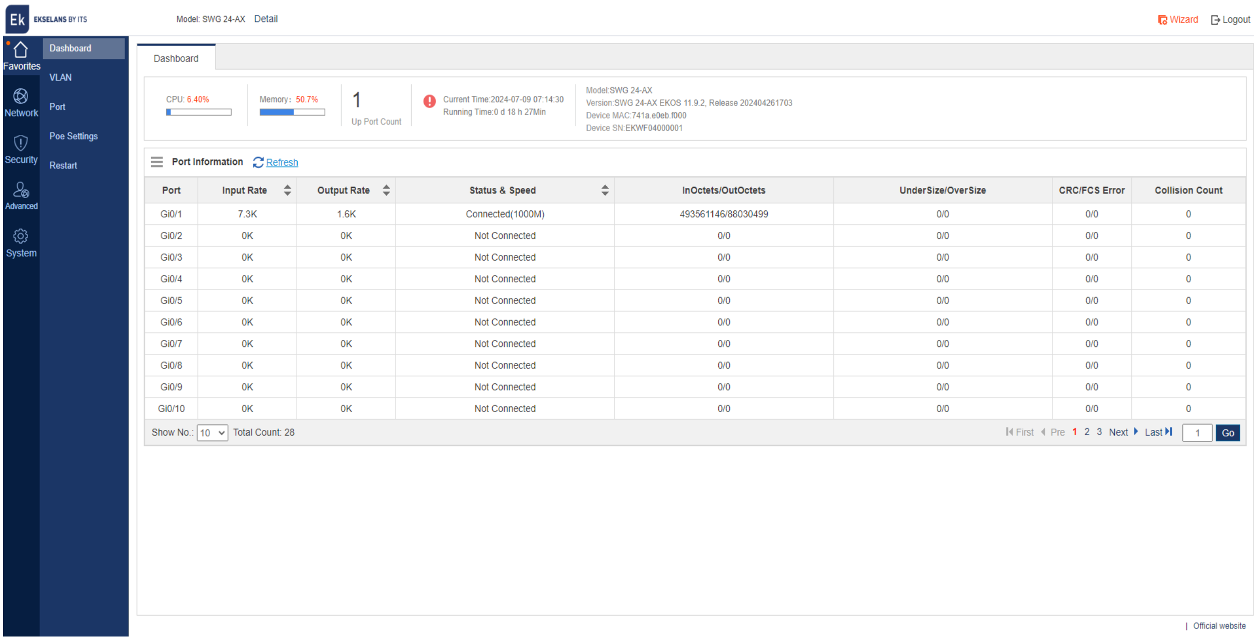
Table 1-2

Default Username/Password	Permission Description
admin/admin	Super administrator with all permissions

When you log in by using the default username and password, the system requests you to change the password to ensure security.

After authentication is successful or the password is changed, the Web homepage is displayed, as shown in Figure 1-3.

Figure 1-3 Web Homepage



CPU: 6.40%

Memory: 50.7%

1 Up Port Count

Current Time:2024-07-09 07:14:30
Running Time:0 d 18 h 27Min

Model:SWG 24-AX
Version:SWG 24-AX EKOS 11.9.2, Release 202404261703
Device MAC:741a.e0eb.f000
Device SN:EKWF04000001

Port Information Refresh

Port	Input Rate	Output Rate	Status & Speed	InOctets/OutOctets	UnderSize/OverSize	CRC/FCS Error	Collision Count
Gi0/1	7.3K	1.6K	Connected(1000M)	493561146/88030499	0/0	0/0	0
Gi0/2	0K	0K	Not Connected	0/0	0/0	0/0	0
Gi0/3	0K	0K	Not Connected	0/0	0/0	0/0	0
Gi0/4	0K	0K	Not Connected	0/0	0/0	0/0	0
Gi0/5	0K	0K	Not Connected	0/0	0/0	0/0	0
Gi0/6	0K	0K	Not Connected	0/0	0/0	0/0	0
Gi0/7	0K	0K	Not Connected	0/0	0/0	0/0	0
Gi0/8	0K	0K	Not Connected	0/0	0/0	0/0	0
Gi0/9	0K	0K	Not Connected	0/0	0/0	0/0	0
Gi0/10	0K	0K	Not Connected	0/0	0/0	0/0	0

Show No.: 10 Total Count: 28 First Pre 1 2 3 Next Last 1 Go

Note

For details about Web pages, see Web Management System.

1.3 Web Management System

Basic Concepts

Icons and Buttons on the GUI

Table 1-3

Icon/Button	Description
Edit	Edit the selected record.
Delete	Delete the selected record.
ON	Enable or disable the function.
□	Available port. After you click or select the icon, the port becomes selected.
■	Unavailable port.
🟦	Selected port.
1	Aggregated port. The digit in the port indicates the number of the aggregated port.

⊓	Trunk port. It is displayed on the panel of the **VLAN Management/VLAN Settings** page.
Save	Submit and save input information.
+	Add settings.
✕	Delete settings.
All Invert Deselec	Batch configuration of panel ports, which is on the right bottom corner of thepanel. Note: You can use this function only when you can select multiple ports on the panel.
*	An input box marked with this symbol indicates that the item is mandatory.

Features

The following table describes feature configurations of secondary menu items in the left navigation tree of the web GUI.

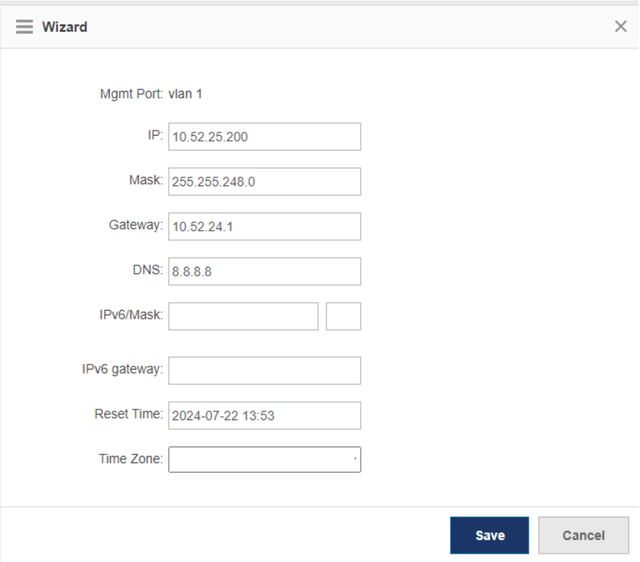
Table 1-4

Feature	Description
Home	Displays port information and overall device information.
VLAN Management	Sets VLANs and trunk ports.
Port	Configures basic information about ports, aggregated ports, port mirroring, andport rate limit.
POE Settings	Configures PoE in the system and on ports.
Restart	Restart the switch.
MAC Address	Sets static addresses and filter addresses.
Routing	Sets routes.
STP	Configures basic information of global STP, STP ports, and RLDP.
IGMP Settings	Sets Internet Group Management Protocol (IGMP) snooping.
DHCP Relay	Sets the DHCP relay.
Authentication	Configures ePortal and advanced settings.
DHCP Snooping	Sets DHCP snooping.
Gateway Anti-ARP-Snooping	Configures anti-ARP-spoofing on the gateway, Address Resolution Protocol(ARP) check, dynamic ARP inspection (DAI), and ARP entries.
IP Source Guard	Configures ports and user binding.

Port Security	Configures port security and binding.
NFPP	Displays information related to Network Foundation Protection Policy (NFPP).
Storm Control	Control storms.
Port Protection	Configures port protection.
DHCP Server	Configures Dynamic Host Configuration Protocol (DHCP), static address allocation, and client list.
ACL	Configures access control lists (ACLs), set the ACL time, and applies ACLs.
QoS	Configures class settings, policy settings and flow settings.
Settings	Sets the system time, changes the password, restores to factory settings, andconfigures the enhancement function, SNMP and DNS.
Upgrade	Performs local upgrade and online upgrade of web packages.
System Logging	Sets the log server and queries system logs.
CWMP	Configures CPE WAN Management Protocol (CWMP).
Detection	Configures ping test, tracert test, cable detection, and one-click collection.
Web Console	Imitates the mechanism of CLI commands.

1.3.1 Initialization Configuration

Figure 1-4 Initialization Configuration



Mgmt Port: vlan 1
IP: 10.52.25.200
Mask: 255.255.248.0
Gateway: 10.52.24.1
DNS: 8.8.8.8
IPv6/Mask:
IPv6 gateway:
Reset Time: 2024-07-22 13:53
Time Zone:

Configure the management VLAN ID, IP address, subnet mask, default gateway and DNS server. Click **Save** and the message “Configuration succeeded.” is displayed.

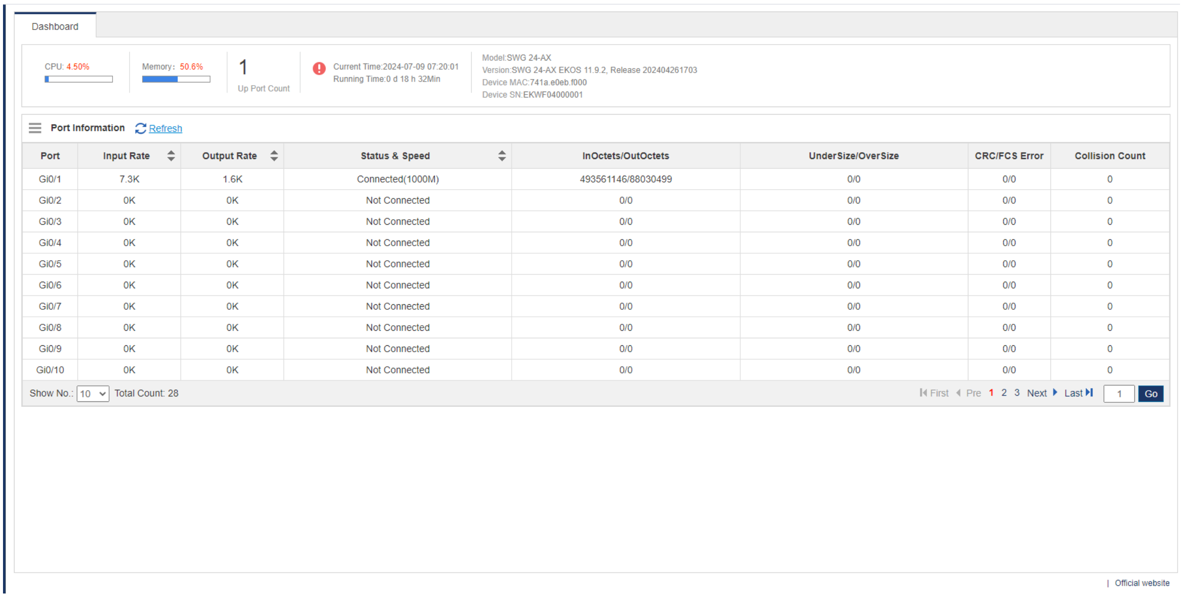
1.3.2 Common

Click the primary menu **Common** to access the secondary menu, including **Home**, **VLAN Management**, **PortManagement**, **PoE Settings** and **Restart**.

1. Home

The **Home** page displays device configurations, basic port information, and port statistics. Figure 1-6 shows the **Home** page.

Figure 1-5 Home



Dashboard

CPU: 4.50%
Memory: 50.6%
1 Up Port Count
Current Time:2024-07-09 07:20:01
Running Time:0 d 18 h 32Min
Model:SWG 24-AX
Version:SWG 24-AX EKOS 11.9.2, Release 202404261703
Device MAC:741a.e0eb.f000
Device SN:EKWF04000001

Port Information Refresh

Port	Input Rate	Output Rate	Status & Speed	InOctets/OutOctets	UnderSize/OverSize	CRC/FCS Error	Collision Count
Gi0/1	7.3K	1.6K	Connected(1000M)	493561146/88030499	0/0	0/0	0
Gi0/2	0K	0K	Not Connected	0/0	0/0	0/0	0
Gi0/3	0K	0K	Not Connected	0/0	0/0	0/0	0
Gi0/4	0K	0K	Not Connected	0/0	0/0	0/0	0
Gi0/5	0K	0K	Not Connected	0/0	0/0	0/0	0
Gi0/6	0K	0K	Not Connected	0/0	0/0	0/0	0
Gi0/7	0K	0K	Not Connected	0/0	0/0	0/0	0
Gi0/8	0K	0K	Not Connected	0/0	0/0	0/0	0
Gi0/9	0K	0K	Not Connected	0/0	0/0	0/0	0
Gi0/10	0K	0K	Not Connected	0/0	0/0	0/0	0

Show No.: 10 Total Count: 28 First Pre 1 2 3 Next Last 1 Go

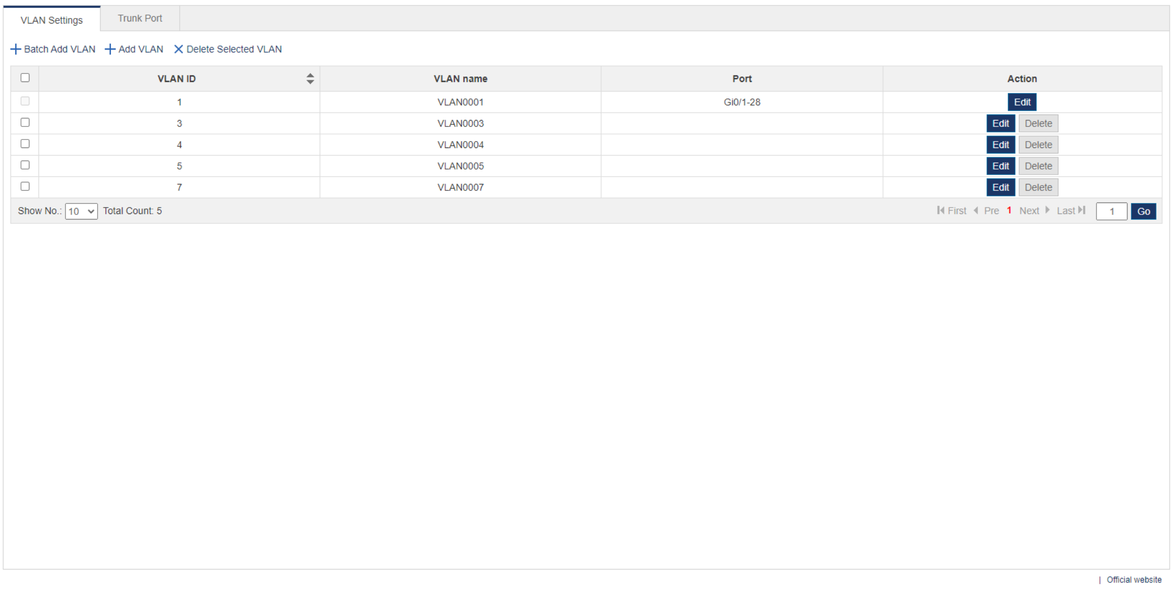
| Official website

2. VLAN Management

The VLAN Management page consists of VLAN Settings and Trunk Port.

(1) VLAN Settings

Figure 1-6 VLAN Settings



VLAN Settings | Trunk Port

+ Batch Add VLAN + Add VLAN × Delete Selected VLAN

□	VLAN ID	VLAN name	Port	Action
□	1	VLAN0001	Gi0/1-28	Edit
□	3	VLAN0003		Edit Delete
□	4	VLAN0004		Edit Delete
□	5	VLAN0005		Edit Delete
□	7	VLAN0007		Edit Delete

Show No.: 10 Total Count: 5 First Pre 1 Next Last 1 Go

| Official website

- Adding a VLAN

  The VLAN ID is mandatory. Other parameters are optional. Click **Save** and the message “Configurationsucceeded.” is displayed. The added VLAN is displayed in the list.

- Editing a VLAN

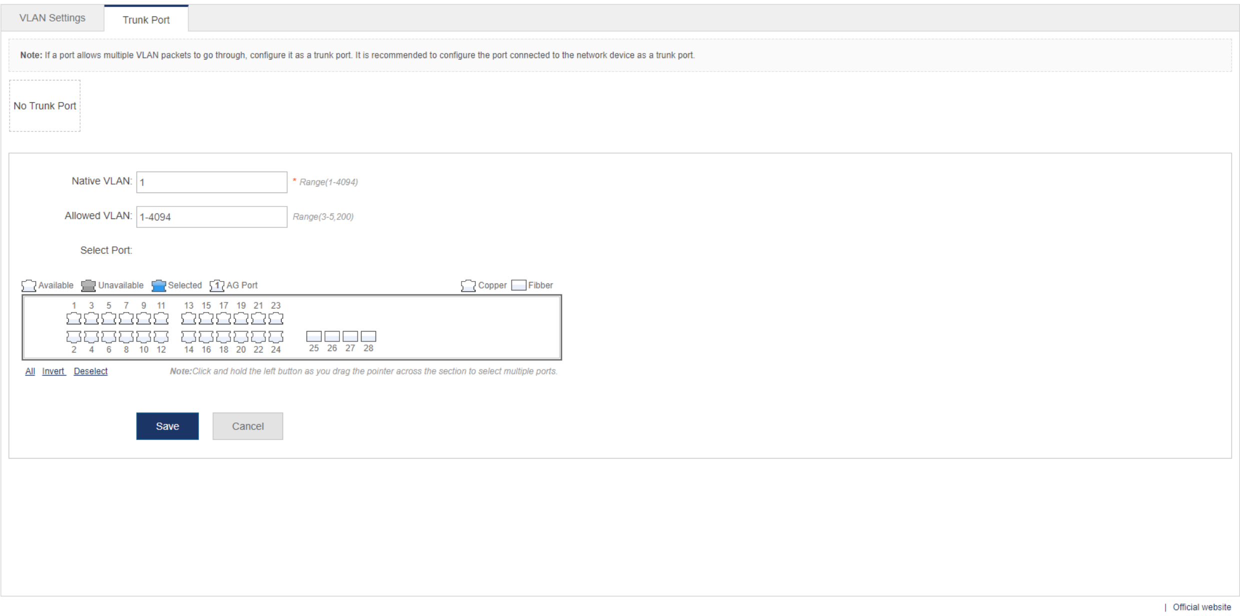
  In the VLAN list, click **Edit** in the **Action** column for a VLAN. Information about the VLAN is displayed. Edit the information, click **Save**. The message “Edit succeeded” is displayed.

- Deleting a VLAN
  - Select multiple records in the VLAN list and click **Delete Selected VLAN** to delete the records in a batch.
  - In the VLAN list, click **Delete** in the **Action** column for a VLAN. The message “Are you sure you want to delete the VLAN?” is displayed. Click **OK**. The message “Delete succeeded.” is displayed, indicating that the VLAN is deleted.

VLAN 1 is the default VLAN. It can be only modified but cannot be deleted.

(2) Trunk Port

Figure 1-7 Trunk Port



Note: If a port allows multiple VLAN packets to go through, configure it as a trunk port. It is recommended to configure the port connected to the network device as a trunk port.

No Trunk Port

Native VLAN: 1 * Range(1-4094)

Allowed VLAN: 1-4094 Range(3-5,200)

Select Port:

Note: Click and hold the left button as you drag the pointer across the section to select multiple ports.

- Adding a Trunk Port

  Select a port on the panel, enter the ranges of Native VLAN and Allowed VLAN (3-5,8,10 for example). Click **Save**. The message “Configuration succeeded” is displayed. The added trunk port is displayed in the trunk portlist.

- Editing a Trunk Port

  Select a trunk port in the trunk port list. Its information is displayed. Edit the information and click Edit. The message “Configuration succeeded” is displayed.

- Deleting a Trunk Port

  Move the cursor to a trunk port in the trunk port list, click **Delete**. The message “Are you sure you want to delete the trunk port?” is displayed. Click **OK**. The message “Delete succeeded.” is displayed, indicating that the trunk port is deleted.

- Batch Deleting Trunk Ports

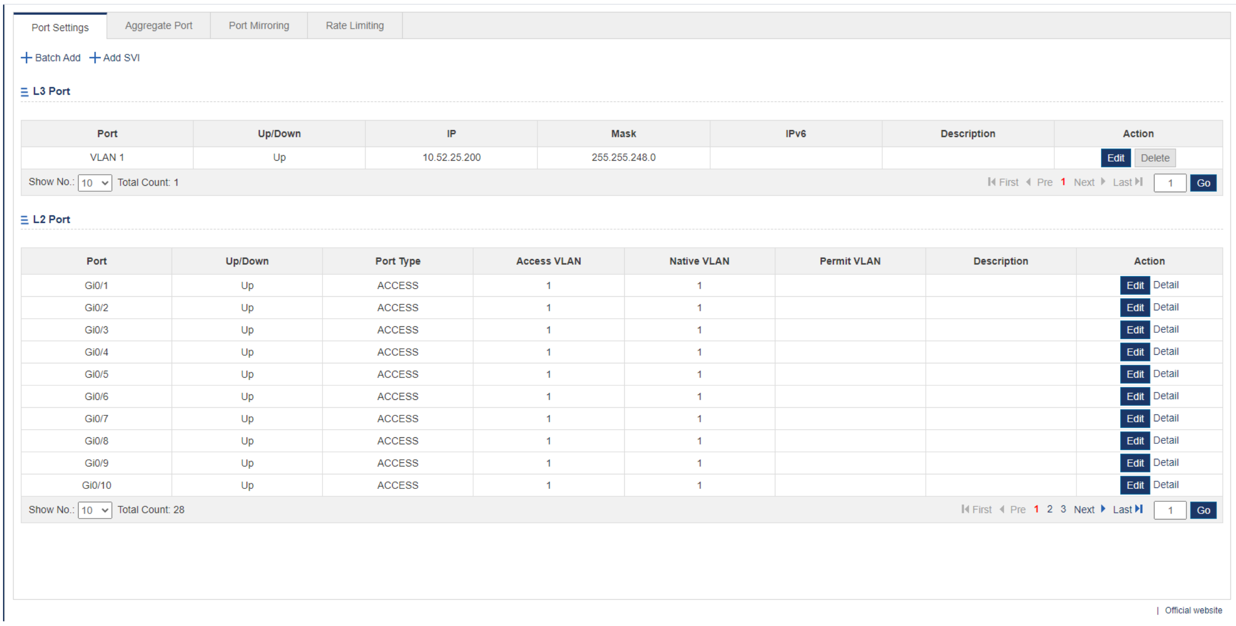
In the trunk port list, select trunk ports to be deleted and click **Batch Del**. The message "Are you sure you want to delete the trunk port?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the trunk ports are deleted.

3. Port Management

The **Port** page allows you to configure basic settings about ports, and configure link aggregation, port mirroring,and port rate limit.

(1) Port Settings

Figure 1-8 Port Settings



L3 Port

Port	Up/Down	IP	Mask	IPv6	Description	Action
VLAN 1	Up	10.52.25.200	255.255.248.0			Edit Delete

Show No.: 10 Total Count: 1 First Pre 1 Next Last 1 Go

L2 Port

Port	Up/Down	Port Type	Access VLAN	Native VLAN	Permit VLAN	Description	Action
Gi0/1	Up	ACCESS	1	1			Edit Detail
Gi0/2	Up	ACCESS	1	1			Edit Detail
Gi0/3	Up	ACCESS	1	1			Edit Detail
Gi0/4	Up	ACCESS	1	1			Edit Detail
Gi0/5	Up	ACCESS	1	1			Edit Detail
Gi0/6	Up	ACCESS	1	1			Edit Detail
Gi0/7	Up	ACCESS	1	1			Edit Detail
Gi0/8	Up	ACCESS	1	1			Edit Detail
Gi0/9	Up	ACCESS	1	1			Edit Detail
Gi0/10	Up	ACCESS	1	1			Edit Detail

Show No.: 10 Total Count: 28 First Pre 1 2 3 Next Last 1 Go

- Batch Configuring Ports

Select ports to be configured and select the port status, rate, and mode. Keep indicates that the system retains the original configuration. You can set Keep for some settings to batch configure only one or two settings.

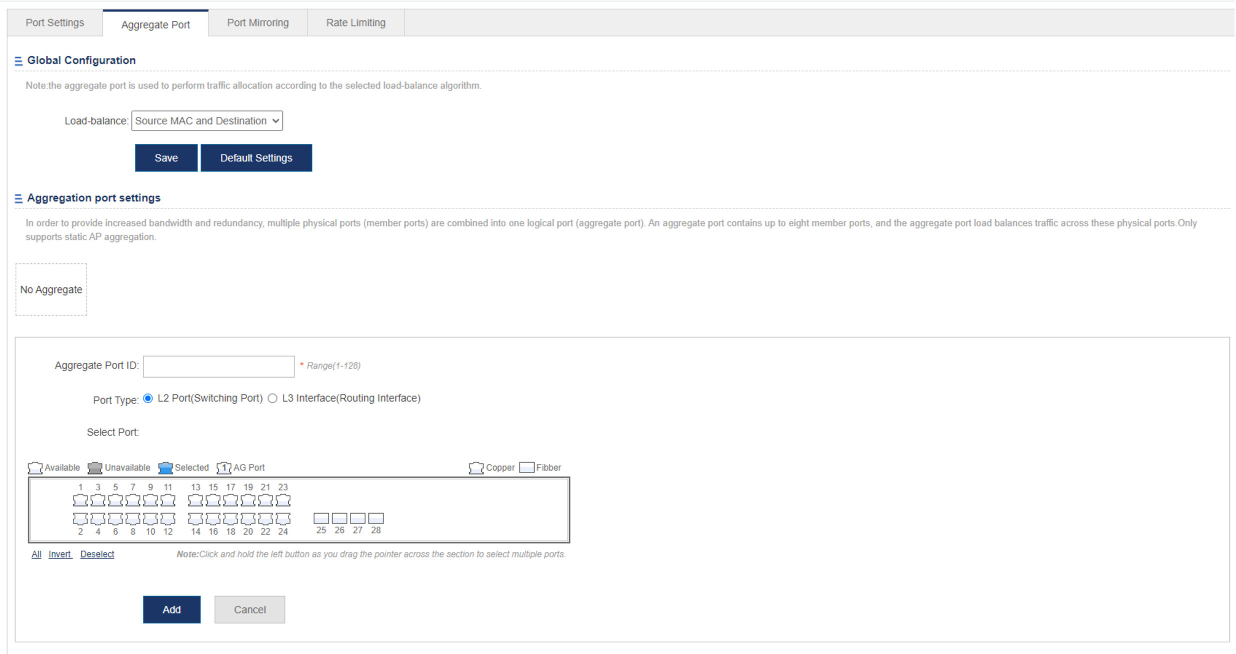
- Editing a Port

Click **Edit** in the **Action** column of the port list. The port information is displayed. Edit the information and click

Save. The message "Configuration succeeded" is displayed.

(2) Port Aggregation

Figure 1-9 Aggregate Port



Global Configuration

Note:the aggregate port is used to perform traffic allocation according to the selected load-balance algorithm.

Load-balance: Source MAC and Destination

Aggregation port settings

In order to provide increased bandwidth and redundancy, multiple physical ports (member ports) are combined into one logical port (aggregate port). An aggregate port contains up to eight member ports, and the aggregate port load balances traffic across these physical ports.Only supports static AP aggregation.

No Aggregate

Aggregate Port ID: * Range(1-128)

Port Type: ● L2 Port(Switching Port) ○ L3 Interface(Routing Interface)

Select Port:

Note:Click and hold the left button as you drag the pointer across the section to select multiple ports.

- Adding an Aggregated Port

  Enter an aggregated port ID, select member ports, and click **Add**. The message "Configuration succeeded." indicating that the aggregated port is added. The port panel displays the successfully added aggregated port.

- Editing an Aggregated Port

  Aggregated ports displayed on the panel cannot be selected. To edit an aggregated port, click the aggregated port in the aggregated port list. Its member ports become selected. Click a port to cancel selection and then click **Edit** to modify the aggregated port.

- Deleting an Aggregated Port

  In the aggregated port list, move the cursor to an aggregated port and click **Delete**. The message "Are you sure you want to delete the aggregate port?" is displayed. Click **OK** to delete the aggregated port. After being deleted, the aggregated port on the panel will become available.

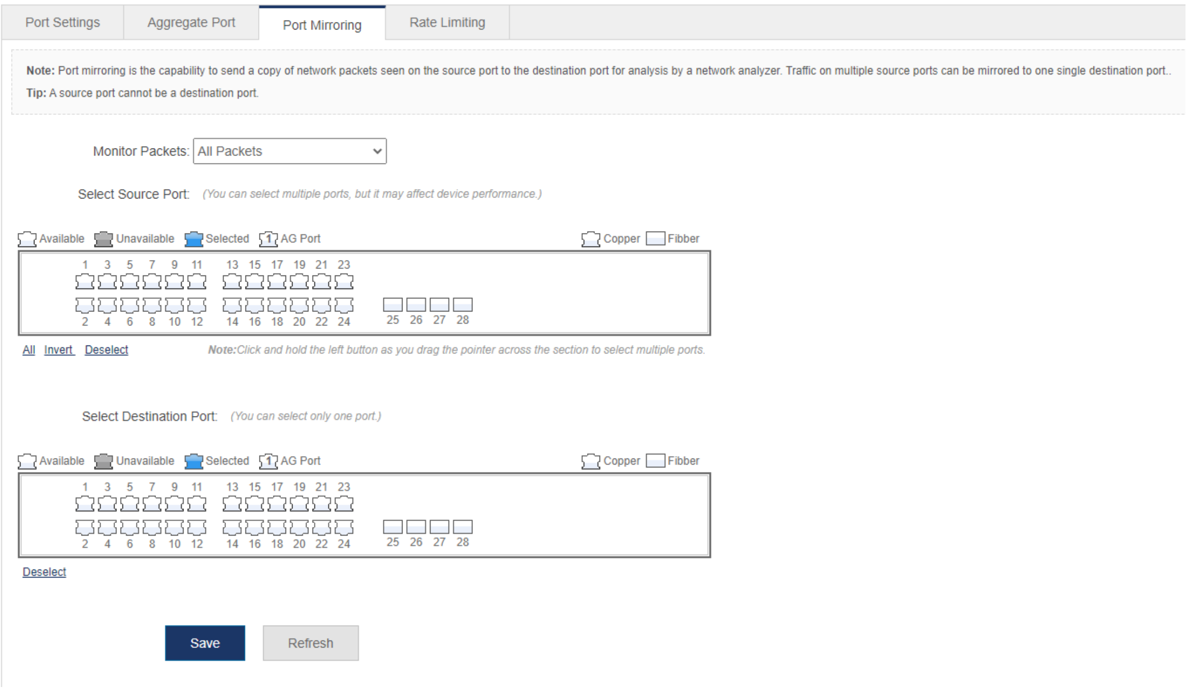
- Batch Deleting Aggregated Ports

  In the aggregated port list, select aggregated ports to be deleted and click **Batch Del**. The message "Are you sure you want to delete the aggregate port?" is displayed. Click **OK** to delete the aggregated ports. After being deleted, the aggregated ports on the panel will become available.

⚠ Ports enabled with ARP check, anti-ARP-spoofing, or MAC VLAN and observing ports in port mirroring cannot be added to an aggregated port, and these ports are unavailable on the panel. When you move the cursor over an unavailable port, a message is displayed, indicating that the functions are enabled on the port and the port cannot be selected.

(3) Port Mirroring

Figure 1-10 Port Mirroring



Note: Port mirroring is the capability to send a copy of network packets seen on the source port to the destination port for analysis by a network analyzer. Traffic on multiple source ports can be mirrored to one single destination port..
Tip: A source port cannot be a destination port.

Monitor Packets: All Packets

Select Source Port: *(You can select multiple ports, but it may affect device performance.)*

Note:*Click and hold the left button as you drag the pointer across the section to select multiple ports.*

Select Destination Port: *(You can select only one port.)*

The initial port mirroring page is in editing state because only one mirrored port can be configured on the Web.There are two panels on the interface. The port selected on the top panel will serve as the mirrored port. You can select multiple mirrored ports. You can select only one port on the bottom panel to serve as the observing port. Select or modify the port on the panel, click **Save**. The message “Configuration succeeded.” is displayed.

Note

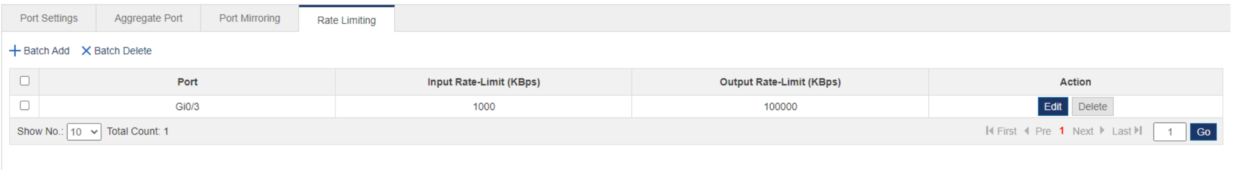
The panel displays the current port mirroring status, and both the source and destination ports can be edited. To cancel modification of port information, click Refresh to restore the panel to the current port mirroring status.

Caution

A member port of the aggregated port cannot be configured as the mirrored or observing port, and the mirrored and observing ports must be different.

(4) Rate Limiting

Figure 1-11 Rate Limiting



□	Port	Input Rate-Limit (KBps)	Output Rate-Limit (KBps)	Action
□	Gi0/3	1000	100000	Edit Delete

Show No.: 10 Total Count: 1

- Adding a Rate-limited Port

You must enter the inbound or outbound rate limit. Click **Save**. The message “Configuration succeeded.” isdisplayed. The added rate limits of the port will be displayed in the port rate limit list.

- Editing a Rate-limited Port

In the port rate limit list, click **Edit** in the **Action** column for a port. Rate-limited port information is displayed. Edit the information and click **Save**. The message “Configuration succeeded” is displayed.

- Deleting a Rate-limited Port

o Select multiple records in the port rate limit list and click **Batch Delete** to batch delete the records.

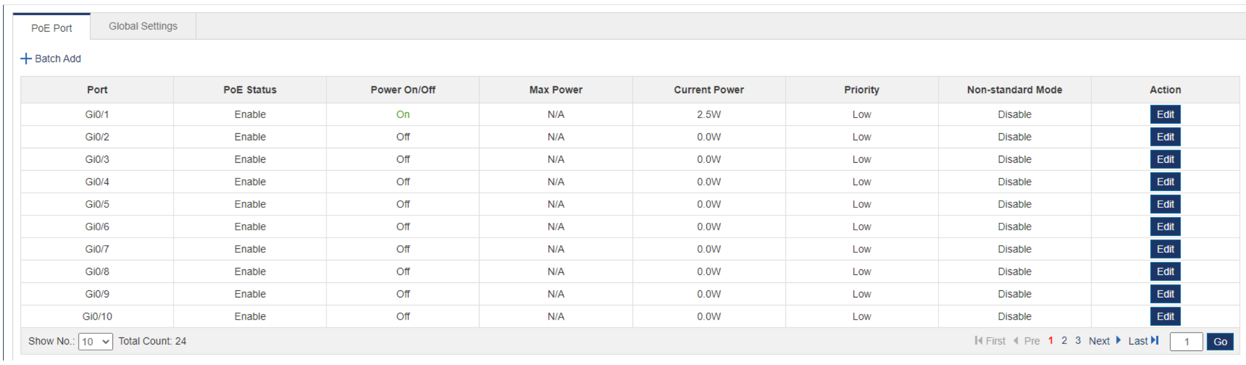
o In the port rate limit list, click **Delete** in the **Action** column for a port. The message "Are you sure you want to delete the port configuration?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the port configuration is deleted.

4. PoE Settings

You can configure PoE on a port or in the system on the **PoE Settings** page. This page is available only forPoE-capable devices.

(1) PoE Port

Figure 1-12 PoE Port Settings



Port	PoE Status	Power On/Off	Max Power	Current Power	Priority	Non-standard Mode	Action
Gi0/1	Enable	On	N/A	2.5W	Low	Disable	Edit
Gi0/2	Enable	Off	N/A	0.0W	Low	Disable	Edit
Gi0/3	Enable	Off	N/A	0.0W	Low	Disable	Edit
Gi0/4	Enable	Off	N/A	0.0W	Low	Disable	Edit
Gi0/5	Enable	Off	N/A	0.0W	Low	Disable	Edit
Gi0/6	Enable	Off	N/A	0.0W	Low	Disable	Edit
Gi0/7	Enable	Off	N/A	0.0W	Low	Disable	Edit
Gi0/8	Enable	Off	N/A	0.0W	Low	Disable	Edit
Gi0/9	Enable	Off	N/A	0.0W	Low	Disable	Edit
Gi0/10	Enable	Off	N/A	0.0W	Low	Disable	Edit

Show No.: 10 Total Count: 24

- Batch Configuring Ports

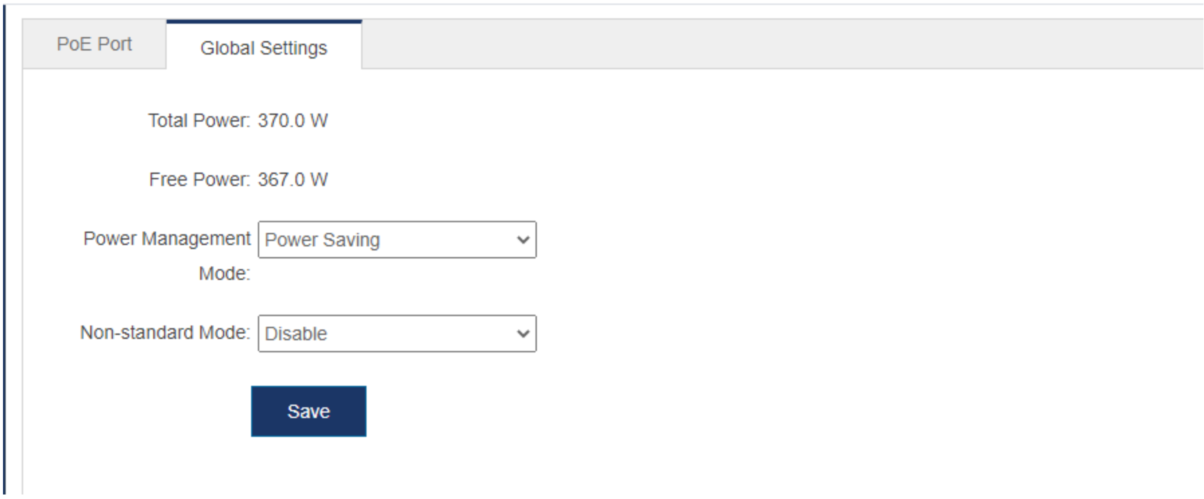
Select ports to be configured, and configure the PoE function, power supply priority, maximum power, currentpower, and non-standard mode. Click **Save**. The message “Configuration succeeded.” is displayed.

- Editing a port

Click **Edit** in the **Action** column of the port list and the port information is displayed. Edit the information and click **Save**. The message “Configuration succeeded” is displayed.

(2) Global Settings

Figure 1-13 Global Settings



Total Power: 370.0 W

Free Power: 367.0 W

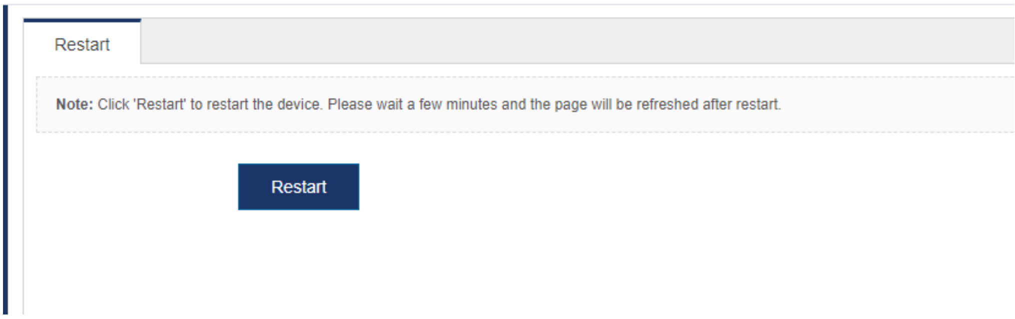
Power Management Mode: Power Saving

Non-standard Mode: Disable

The page displays the total power, free power, and power supply management mode. Select a power supplymanagement mode and click **Save** to configure the port.

5. Restart

Figure 1-14 Restart



Note: Click 'Restart' to restart the device. Please wait a few minutes and the page will be refreshed after restart.

Click **Restart**. The message "Are you sure you want to restart the device?" is displayed. Click **OK** to restart thedevice. Wait for a few minutes. The page will refresh after restart.

1.3.3 Network

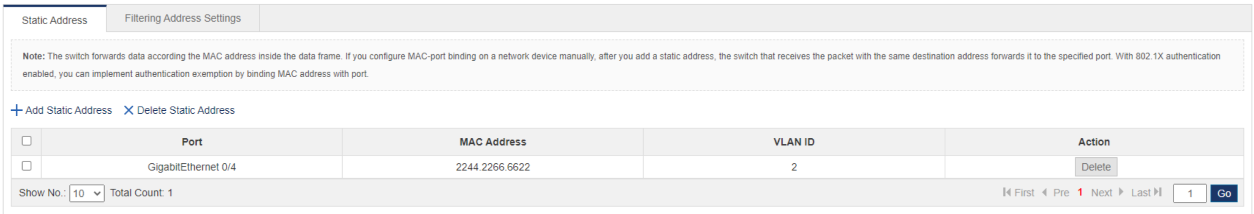
Click the primary menu **Network** to access the secondary menu, including **MAC Address**, **Routing**, **STP**, **IGMPSnooping**, **DHCP Relay** and **Authentication**.

1. MAC Address

The MAC Address page includes **Static Address Settings** and **Filtering Address Settings** pages.

(1) Static Address Settings

Figure 1-15 Static Address Settings



Note: The switch forwards data according the MAC address inside the data frame. If you configure MAC-port binding on a network device manually, after you add a static address, the switch that receives the packet with the same destination address forwards it to the specified port. With 802.1X authentication enabled, you can implement authentication exemption by binding MAC address with port.

□	Port	MAC Address	VLAN ID	Action
□	GigabitEthernet 0/4	2244.2266.6622	2	Delete

Show No.: 10 Total Count: 1

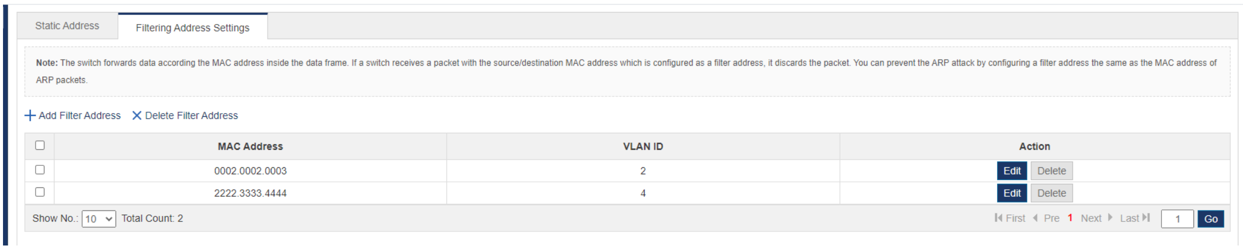
- Adding a Static Address

You must enter a MAC address and a VLAN ID and select a port to add a static address. Click **Save**. The message “Configuration Succeeded.” is displayed. The added static address is displayed in the static address list.

- Deleting a Static Address
  - Select multiple records in the static address list and click Delete Static Address to batch delete the records.
  - In the static address list, click Delete in the Action column for a static address. The message "Are you sure you want to delete the static address?" is displayed. Click OK. The message "Delete succeeded." is displayed.

(2) Filtering Address Settings

Figure 1-16 Filtering Address Settings



Note: The switch forwards data according the MAC address inside the data frame. If a switch receives a packet with the source/destination MAC address which is configured as a filter address, it discards the packet. You can prevent the ARP attack by configuring a filter address the same as the MAC address of ARP packets.

□	MAC Address	VLAN ID	Action
□	0002.0002.0003	2	Edit Delete
□	2222.3333.4444	4	Edit Delete

Show No.: 10 Total Count: 2

- Adding a Filter Address

You must enter an MAC address, a VLAN ID to add a filter address. Click **Save** and the message “ConfigurationSucceeded.” is displayed. The added filter address is displayed in the filter address list.

- Editing a Filter Address

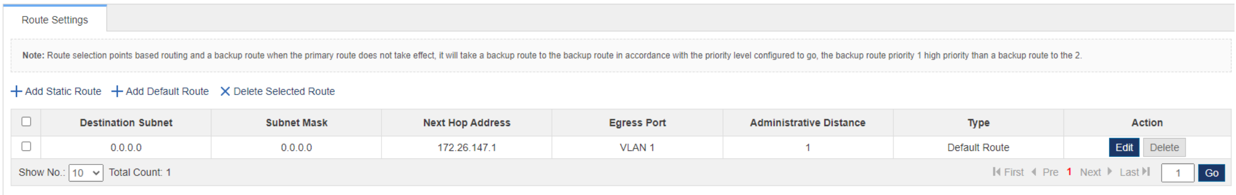
In the filter address list, click **Edit** in the **Action** column for a filter address. The address information is displayed. Edit the information and click **Save**. The message “Configuration succeeded” is displayed.

- Deleting a Filter Address
  - Select multiple records in the static address list and click Delete Filter Address to batch delete the records.
  - In the filter address list, click Delete in the Action column for a filter address. The message "Are you sure you want to delete the filter address?" is displayed. Click OK. The message "Delete succeeded." is displayed.

2. Routing

The **Routing** page allows you to manage routes.

Figure 1-17 Route Settings



Note: Route selection points based routing and a backup route when the primary route does not take effect, it will take a backup route to the backup route in accordance with the priority level configured to go, the backup route priority 1 high priority than a backup route to the 2.

□	Destination Subnet	Subnet Mask	Next Hop Address	Egress Port	Administrative Distance	Type	Action
□	0.0.0.0	0.0.0.0	172.26.147.1	VLAN 1	1	Default Route	Edit Delete

Show No.: 10 Total Count: 1

- Adding a Static Route

You must select an IP type and enter a destination subnet, a subnet mask, and a next-hop address to add a static address. Click **Save**. The message “Configuration Succeeded.” is displayed. The added static route is displayed in the route list.

- Editing a Route

In the route list, click **Edit** in the **Action** column for a route. Route information is displayed. Edit the information and click **Save**. The message “Configuration succeeded” is displayed.

- Deleting a Route
  - Select multiple records in the route list and click **Delete Selected Route** to batch delete the records.
  - In the filter address list, click **Delete** in the **Action** column for a filter address. The message "Are you sure you want to delete the filter address?" is displayed. Click **OK**. The message "Delete succeeded." is displayed.
- Adding a Default Route

Select an IP type and enter a next hop address to add a default route. Click **Save**. The message “Configuration Succeeded.” is displayed. The added default route is displayed in the route list.

Note

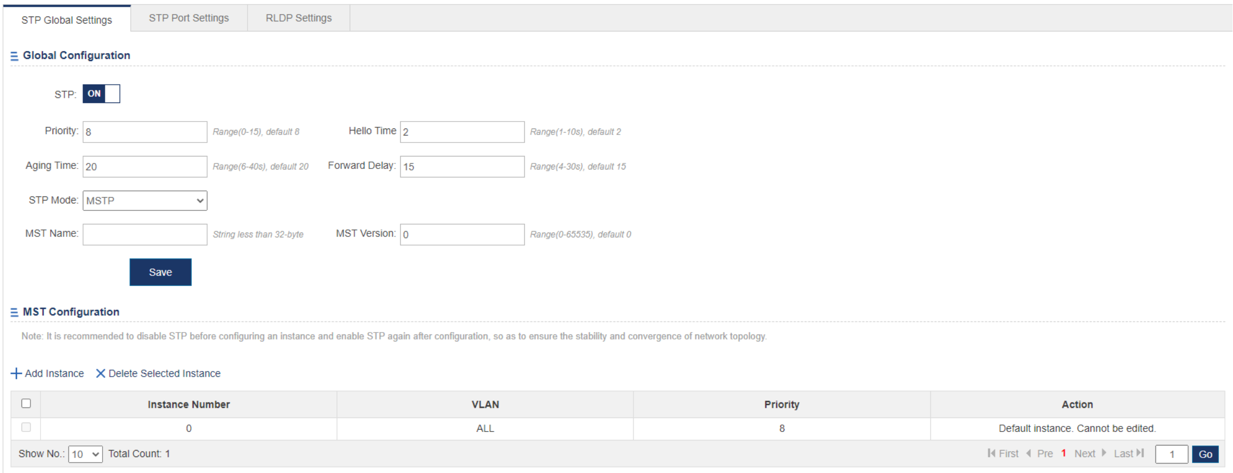
Routes are classified into primary and backup routes. When the primary route becomes unreachable, a backup route takes over services. Backup routes are selected based on their priorities. The priority of backuproute 1 is higher than that of backup route 2.

3. STP

The **STP** page allows you to configure STP global parameters, STP ports, and RLDP.

(1) STP Global Settings

Figure 1-19 STP Global Settings



STP Global Settings | STP Port Settings | RLDP Settings

Global Configuration

STP: ON

Priority: 8 Range(0-15), default 8

Hello Time 2 Range(1-10s), default 2

Aging Time: 20 Range(6-40s), default 20

Forward Delay: 15 Range(4-30s), default 15

STP Mode: MSTP

MST Name: String less than 32-byte

MST Version: 0 Range(0-65535), default 0

Save

MST Configuration

Note: It is recommended to disable STP before configuring an instance and enable STP again after configuration, so as to ensure the stability and convergence of network topology.

+ Add Instance ✕ Delete Selected Instance

□	Instance Number	VLAN	Priority	Action
□	0	ALL	8	Default instance. Cannot be edited.

Show No.: 10 Total Count: 1 First Pre 1 Next Last 1 Go

You can configure STP global parameters. When **STP Mode** is set to **MSTP**, you can configure an MST instance(MSTI).

- Adding a MSTI

The MSTI ID and VLAN range are mandatory. Other parameters are optional. Click **Save**. The message“Configuration Succeeded.” is displayed. The added MSTI is displayed in the MSTI list.

- Editing a MSTI

In the MSTI list, click **Edit** in the **Action** column for an MSTI. MSTI information is displayed. Edit the informationand click **Save**. The message “Configuration succeeded” is displayed.

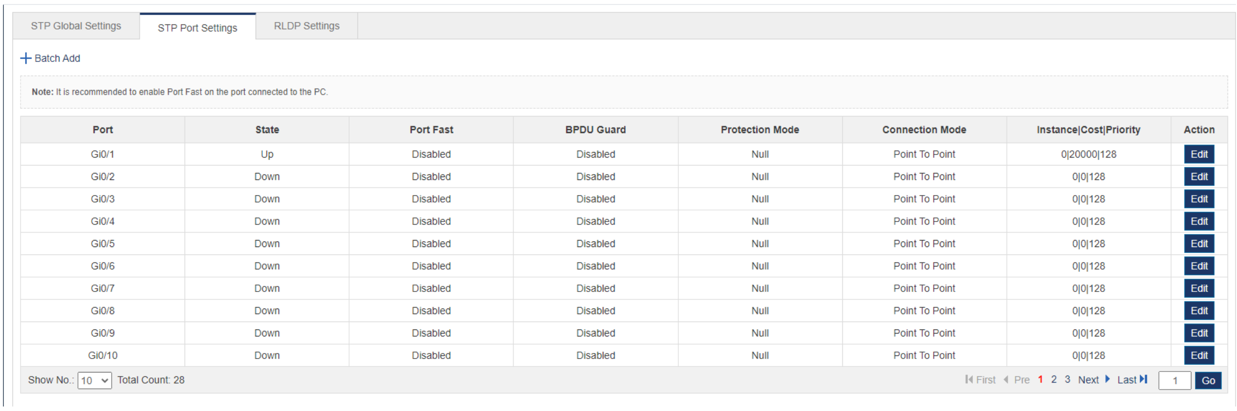
- Deleting a MSTI

Select multiple records in the MSTI list and click **Delete Selected Instance** to batch delete the records.

In the MSTI list, click **Delete** in the **Action** column for an MSTI. The message "Are you sure you want todelete the instance?" is deleted. Click **OK**. The message "Delete succeeded." is displayed, indicating that the MSTI is deleted. MSTI 0 is the default one and cannot be deleted.

(2) STP Port Setting

Figure 1-20 STP Port Settings



STP Global Settings | STP Port Settings | RLDP Settings

+ Batch Add

Note: It is recommended to enable Port Fast on the port connected to the PC.

Port	State	Port Fast	BPDU Guard	Protection Mode	Connection Mode	Instance|Cost|Priority	Action
Gi0/1	Up	Disabled	Disabled	Null	Point To Point	0|20000|128	Edit
Gi0/2	Down	Disabled	Disabled	Null	Point To Point	0|0|128	Edit
Gi0/3	Down	Disabled	Disabled	Null	Point To Point	0|0|128	Edit
Gi0/4	Down	Disabled	Disabled	Null	Point To Point	0|0|128	Edit
Gi0/5	Down	Disabled	Disabled	Null	Point To Point	0|0|128	Edit
Gi0/6	Down	Disabled	Disabled	Null	Point To Point	0|0|128	Edit
Gi0/7	Down	Disabled	Disabled	Null	Point To Point	0|0|128	Edit
Gi0/8	Down	Disabled	Disabled	Null	Point To Point	0|0|128	Edit
Gi0/9	Down	Disabled	Disabled	Null	Point To Point	0|0|128	Edit
Gi0/10	Down	Disabled	Disabled	Null	Point To Point	0|0|128	Edit

Show No.: 10 Total Count: 28 First Pre 1 2 3 Next Last 1 Go

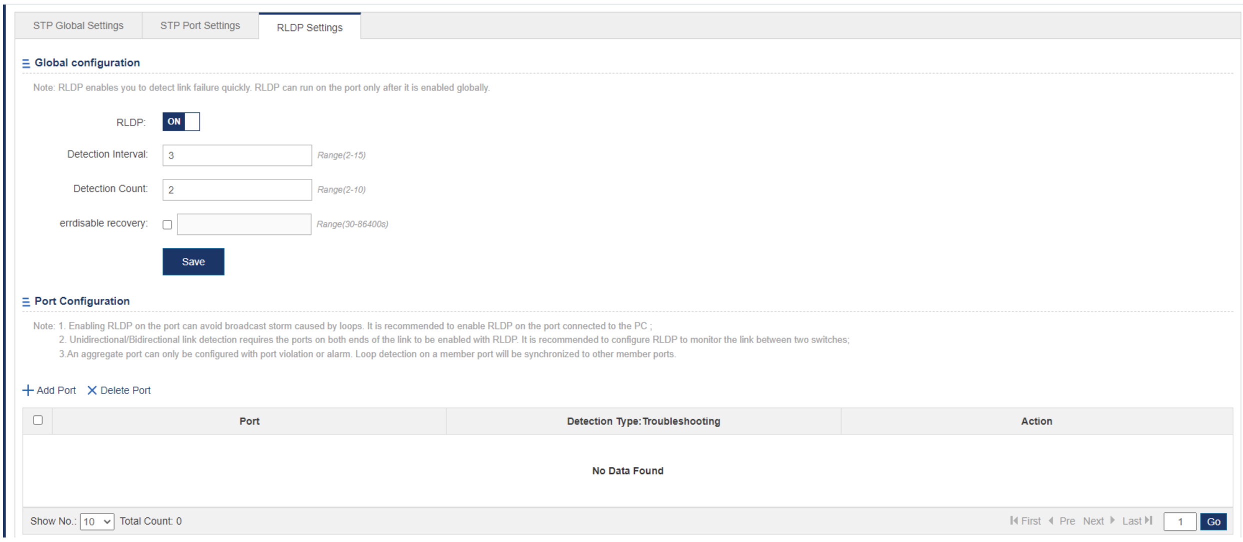
- Batch Adding STP Ports

Select a protection mode, a connection mode, a port priority, and whether to enable Port Fast and BPDU Guard.Select ports to be batch configured and click **Save**.

- Editing an STP Port

In the STP port list, click **Edit** in the **Action** column for an STP port. Port information is displayed. Edit the information and click **Save**. The message “Configuration succeeded” is displayed.

(3) RLDP Settings



Global configuration

Note: RLDP enables you to detect link failure quickly. RLDP can run on the port only after it is enabled globally.

RLDP: ON

Detection Interval: 3 Range(2-15)

Detection Count: 2 Range(2-10)

errdisable recovery: □ Range(30-86400s)

Port Configuration

Note: 1. Enabling RLDP on the port can avoid broadcast storm caused by loops. It is recommended to enable RLDP on the port connected to the PC ;
2. Unidirectional/Bidirectional link detection requires the ports on both ends of the link to be enabled with RLDP. It is recommended to configure RLDP to monitor the link between two switches;
3.An aggregate port can only be configured with port violation or alarm. Loop detection on a member port will be synchronized to other member ports.

□	Port	Detection Type: Troubleshooting	Action
		No Data Found	

Show No.: 10 Total Count: 0

(4) RLDP Global Configuration

Click **RLDP** to enable or disable the RLDP function. When the RLDP function is enabled, set a detection intervaland detection count. Click **Save**. The message “Configuration Succeeded.” is displayed.

(5) RLDP Port Configuration

- Adding an RLDP-enabled Port

Select the detection modes, troubleshooting and a port. Click **Save** and the message “Save Succeeded.” is displayed., indicating that an RLDP-enabled port is added. The added RLDP-enabled port is displayed in the RLDP-enabled list.

- Editing an RLDP Port

In the RLDP-enabled port list, click **Edit** in the **Action** column for an RLDP-enabled port. Port information is displayed. Edit the information and click **Save**. The message “Save succeeded” is displayed.

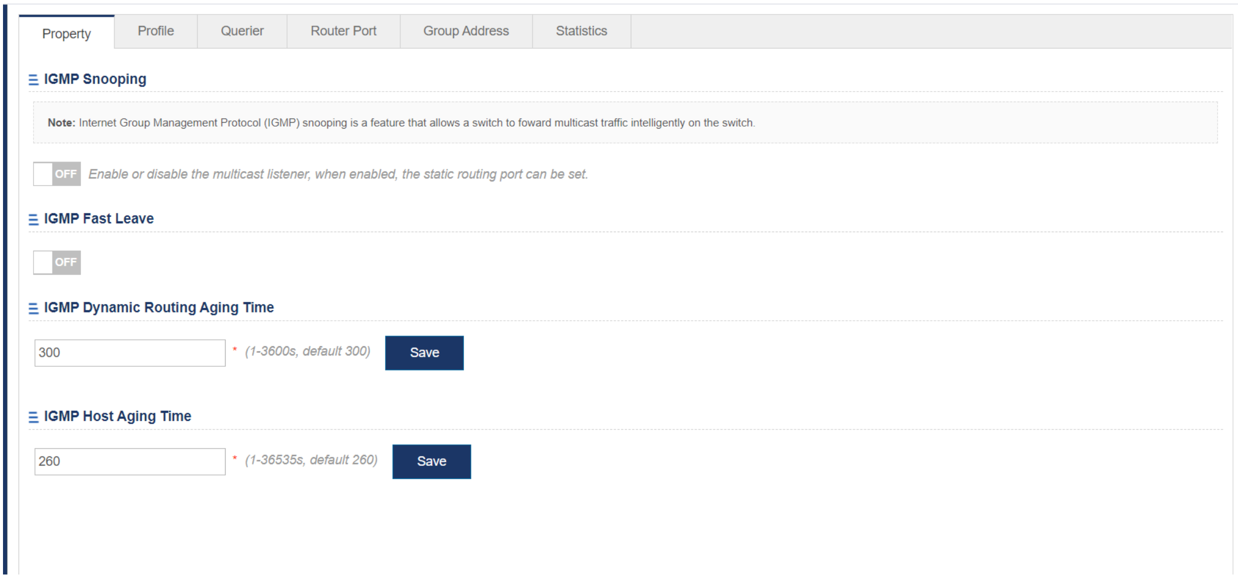
- Deleting an RLDP-enabled Port

  - Select multiple records in the RLDP-enabled port list and click Delete Port to batch delete the records.
  - In the RLDP-enabled port list, click Delete in the Action column for a port. The message "Are you sure you want to delete the item?" is displayed. Click OK. The message "Delete succeeded." is displayed, indicating that the port is deleted.

4. IGMP Settings

Figure 1-21 shows the **IGMP Snooping** page.

Figure 1-21 IGMP Snooping Settings



IGMP Snooping

Note: Internet Group Management Protocol (IGMP) snooping is a feature that allows a switch to foward multicast traffic intelligently on the switch.

OFF *Enable or disable the multicast listener, when enabled, the static routing port can be set.*

IGMP Fast Leave

OFF

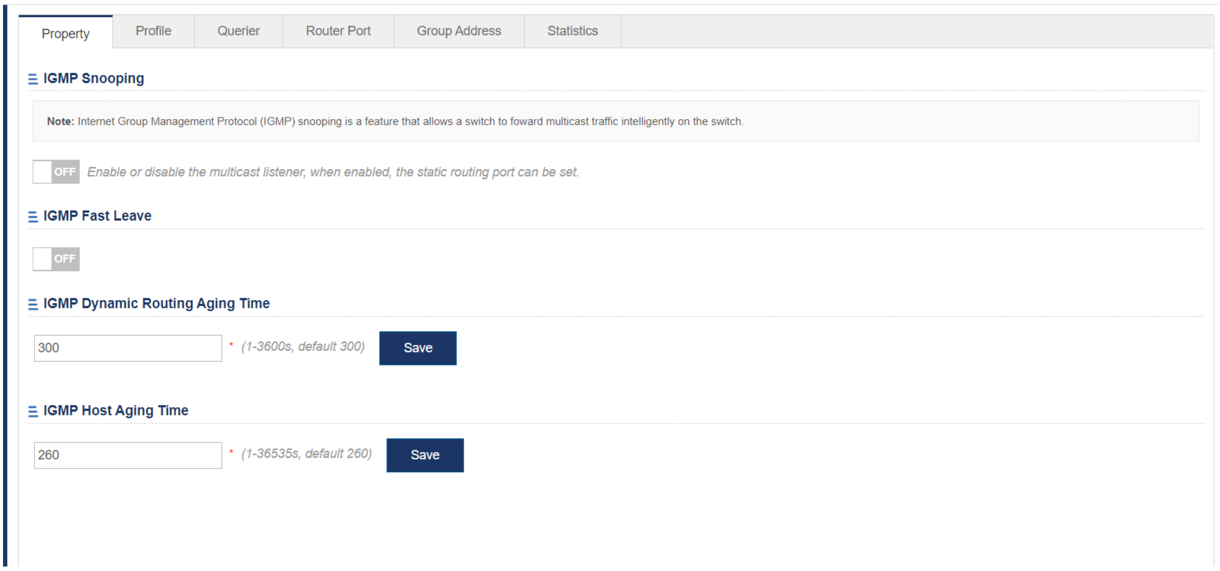
IGMP Dynamic Routing Aging Time

300 * *(1-3600s, default 300)* Save

IGMP Host Aging Time

260 * *(1-36535s, default 260)* Save

(1) IGMP Property



IGMP Snooping

Note: Internet Group Management Protocol (IGMP) snooping is a feature that allows a switch to foward multicast traffic intelligently on the switch.

OFF *Enable or disable the multicast listener, when enabled, the static routing port can be set.*

IGMP Fast Leave

OFF

IGMP Dynamic Routing Aging Time

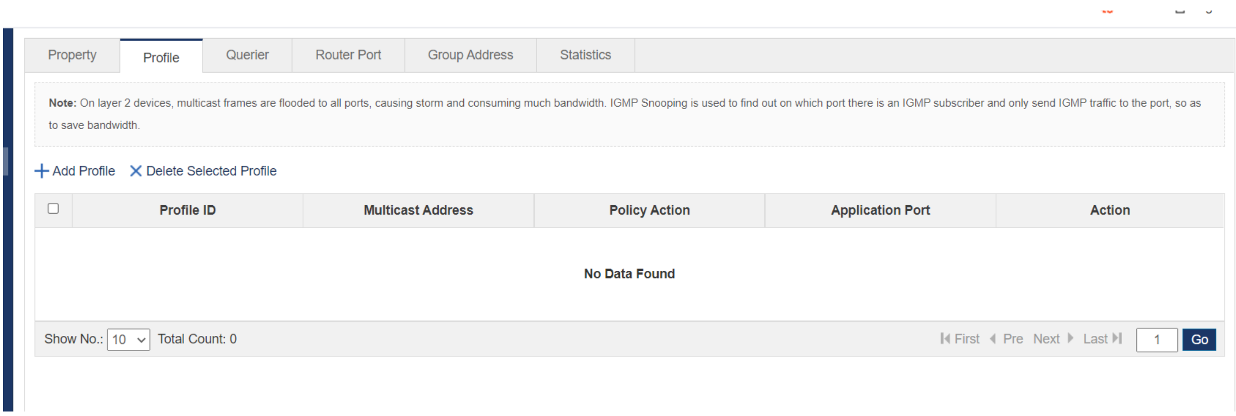
300 * *(1-3600s, default 300)* Save

IGMP Host Aging Time

260 * *(1-36535s, default 260)* Save

Click **IGMP snooping** to enable IGMP snooping function. Click **IGMP Fast Leave** to enable IGMP fast leave function. After the IGMP dynamic routing aging time and IGMP host aging time are specified, click **Save** to save configuration.

(2) IGMP Snooping Profile



Property | Profile | Querier | Router Port | Group Address | Statistics

Note: On layer 2 devices, multicast frames are flooded to all ports, causing storm and consuming much bandwidth. IGMP Snooping is used to find out on which port there is an IGMP subscriber and only send IGMP traffic to the port, so as to save bandwidth.

+ Add Profile   ✕ Delete Selected Profile

□	Profile ID	Multicast Address	Policy Action	Application Port	Action
			No Data Found		

Show No.: 10   Total Count: 0   First Pre Next Last 1 Go

- Adding a Profile

The profile ID and multicast address range are mandatory. Other parameters are optional. Click **Save**. The message "Configuration Succeeded." is displayed. The added profile is displayed in the profile list.

- Editing a Profile

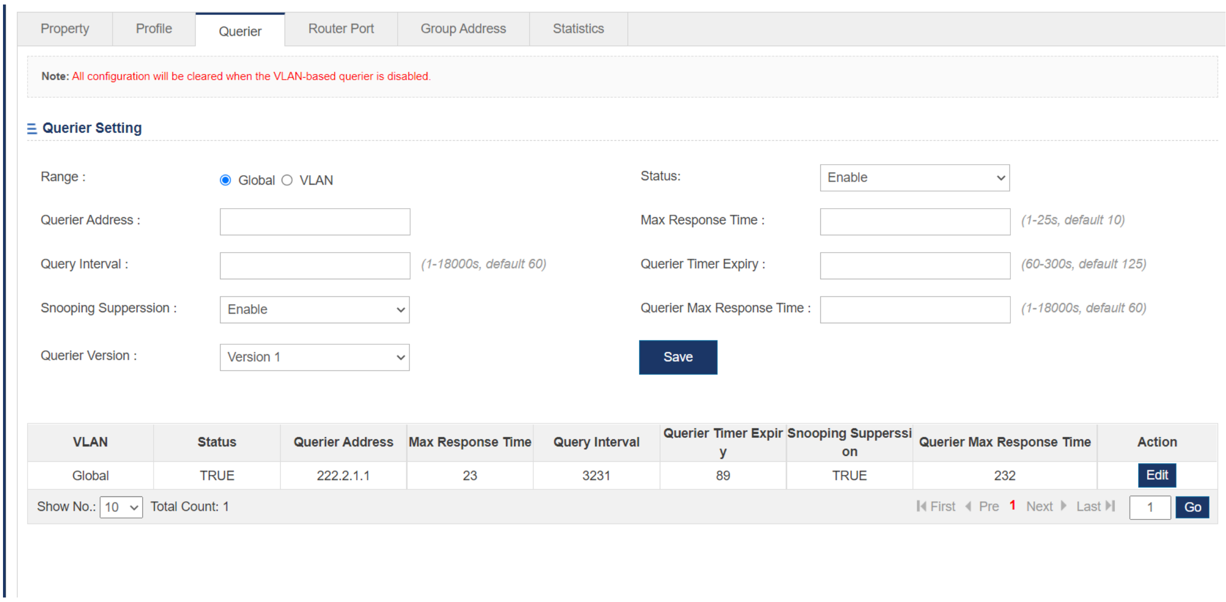
In the profile list, click **Edit** in the **Action** column for a profile. Profile information is displayed. Edit the information and click **Save**. The message "Configuration succeeded" is displayed.

- Deleting a Profile

  - Select multiple records in the profile list and click Delete Selected Profile to batch delete the records.

  - In the profile list, click **Delete** in the **Action** column for a profile. The message "Are you sure you want to delete the profile?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the profile is deleted.

(3) IGMP Snooping Querier



Property | Profile | Querier | Router Port | Group Address | Statistics

Note: All configuration will be cleared when the VLAN-based querier is disabled.

Querier Setting

Range : ● Global ○ VLAN

Status: Enable

Querier Address :

Max Response Time : (1-25s, default 10)

Query Interval : (1-18000s, default 60)

Querier Timer Expiry : (60-300s, default 125)

Snooping Suppersion : Enable

Querier Max Response Time : (1-18000s, default 60)

Querier Version : Version 1

Save

VLAN	Status	Querier Address	Max Response Time	Query Interval	Querier Timer Expiry	Snooping Suppression	Querier Max Response Time	Action
Global	TRUE	222.2.1.1	23	3231	89	TRUE	232	Edit

Show No.: 10   Total Count: 1   First Pre 1 Next Last 1 Go

- Configuring Global Query

Select **Global**, and then configure the attributes of global query. The Status, Querier Address, Max Response Time, Query Interval, Querier Timer Expiry, Snooping Suppression, Querier Max Response Time, Querier Version are available for configuration. If some attributes are left empty, default values will be used automatically.

- Configuring VLAN-based Query

Select VLAN, and the configure the attributes of the VLAN-based query. The Status, Querier Address, Max Response Time, Query Interval, Querier Timer Expiry and Querier Version are available for configuration. If some attributes are left empty, default values will be used automatically.

- Editing the Attributes of Querier

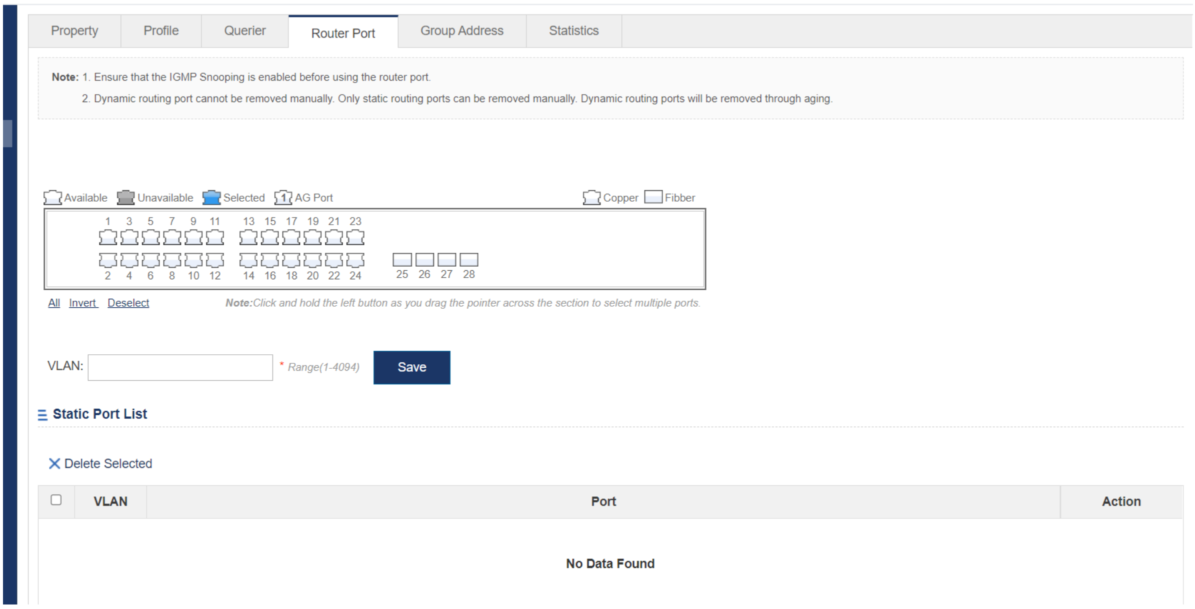
In the querier list, click **Edit** in the **Action** column for a querier. Click **Save** after you change the configuration. Click **Cancel** if you don’t want to save the configuration.

- Deleting a Querier

In the querier list, click **Delete** in the **Action** Column for a VLAN-based querier. Click **OK** when the message "Are you sure you want to delete the item?" is displayed. When the message "Delete succeeded." is displayed, it indicates that the VLAN-based querier is deleted.

(4) Router Port

Router ports fall into two types: static router ports and dynamic router ports. Dynamic router ports cannot be configured and deleted. Static router ports can be configured only after the IGMP Snooping is enabled.



Note: 1. Ensure that the IGMP Snooping is enabled before using the router port.
2. Dynamic routing port cannot be removed manually. Only static routing ports can be removed manually. Dynamic routing ports will be removed through aging.

Note: Click and hold the left button as you drag the pointer across the section to select multiple ports.

VLAN: * Range(1-4094)

Static Port List

□	VLAN	Port	Action
		No Data Found	

- Configuring Static Router Ports

Select the ports in the port panel and specify the VLAN. Then, Click **Save** to save the configuration. After that, the static router ports will be added to the configured VLAN. Please ensure that the port is added to the corresponding VLAN; otherwise, the message “Interface must be in the VLAN you assigned.” will be displayed.

- Editing Static Router Ports

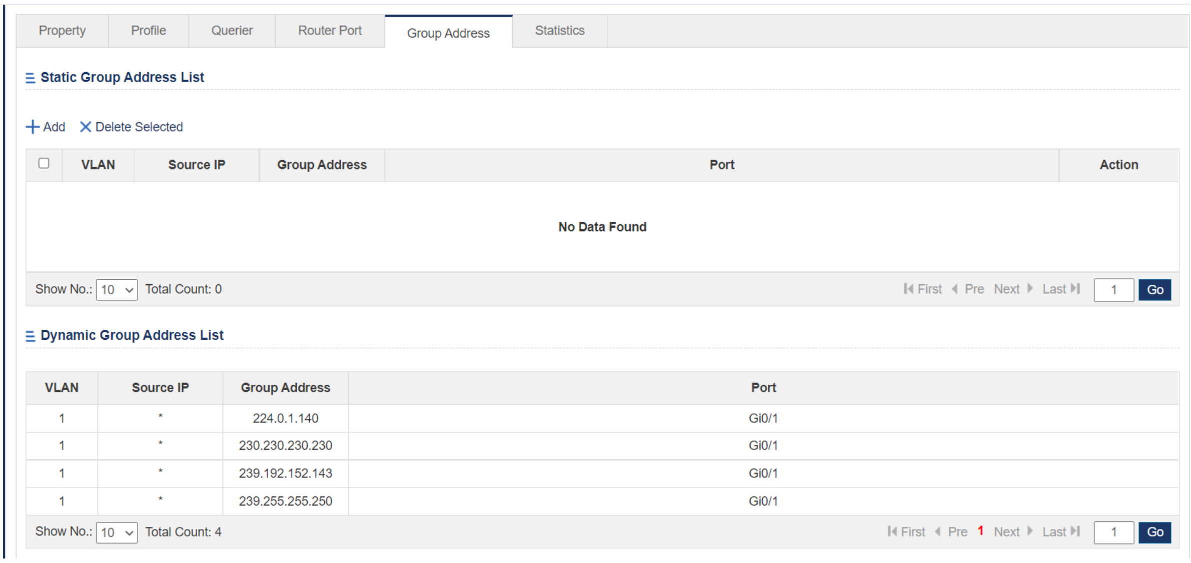
In the static router port list, click **Edit** in the **Action** column for a static router port to edit the port and VLAN. Then, click Save to save the modification.

- Deleting Router Port

In the router port list, select the static router port to be deleted, and then click **Delete Selected**.

(5) Group Address

Group addresses include two types: static group addresses and dynamic group addresses. Dynamic group addresses cannot be configured and deleted. Static group addresses can be enabled only after the IGMP snooping is enabled.



Static Group Address List

□	VLAN	Source IP	Group Address	Port	Action
No Data Found					

Show No.: 10 Total Count: 0 First Pre Next Last 1 Go

Dynamic Group Address List

VLAN	Source IP	Group Address	Port
1	*	224.0.1.140	Gi0/1
1	*	230.230.230.230	Gi0/1
1	*	239.192.152.143	Gi0/1
1	*	239.255.255.250	Gi0/1

Show No.: 10 Total Count: 4 First Pre 1 Next Last 1 Go

- Adding a Static Group Address

Click **Add** to enter the configuration page. Specify the VLAN and group address and select ports. Then, click **Save**. When the message "Save succeeded" is displayed, it indicates that the static group address is added.

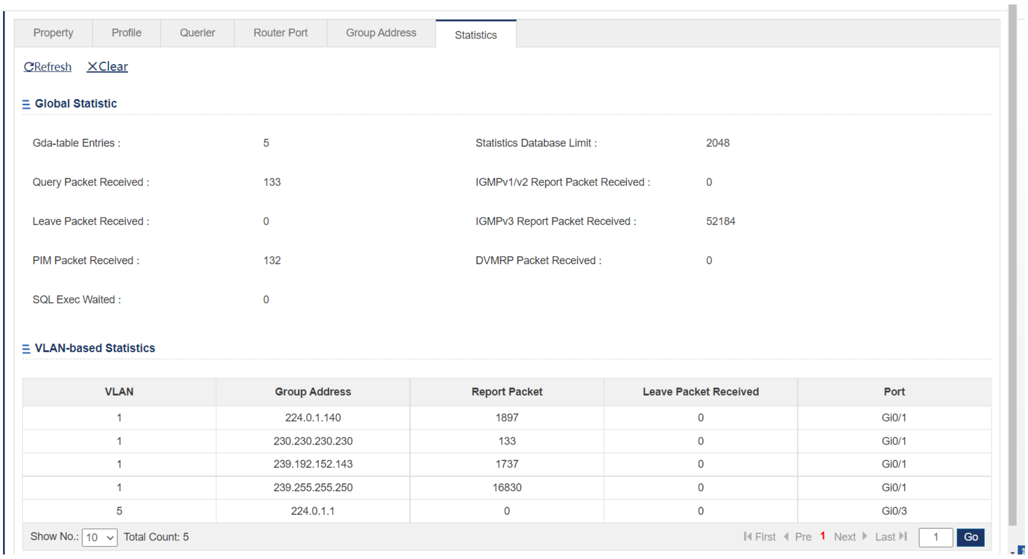
- Editing a Static Group Address

In the static group address list, click **Edit** in the **Action** column for a static group address. After changing the configuration, click **Save**.

- Deleting a Static Group Address
  - Select multiple records in the static group address list and click **Delete Selected** to batch delete the static group addresses.
  - In the static group address list, click **Delete** in the **Action** column for a static group address. When the message "Are you sure you want to delete the item?" is displayed, click **OK**. When the message "Delete succeeded." is displayed, it indicates that the static group address is deleted.

(6) IGMP Statistics

This page allows you to check IGMP statistics. Click **Refresh**, you can refresh the statistics. Click **Clear**, you can clear all statistics.



Global Statistic

Gda-table Entries :	5	Statistics Database Limit :	2048
Query Packet Received :	133	IGMPv1/v2 Report Packet Received :	0
Leave Packet Received :	0	IGMPv3 Report Packet Received :	52184
PIM Packet Received :	132	DVMRP Packet Received :	0
SQL Exec Waited :	0		

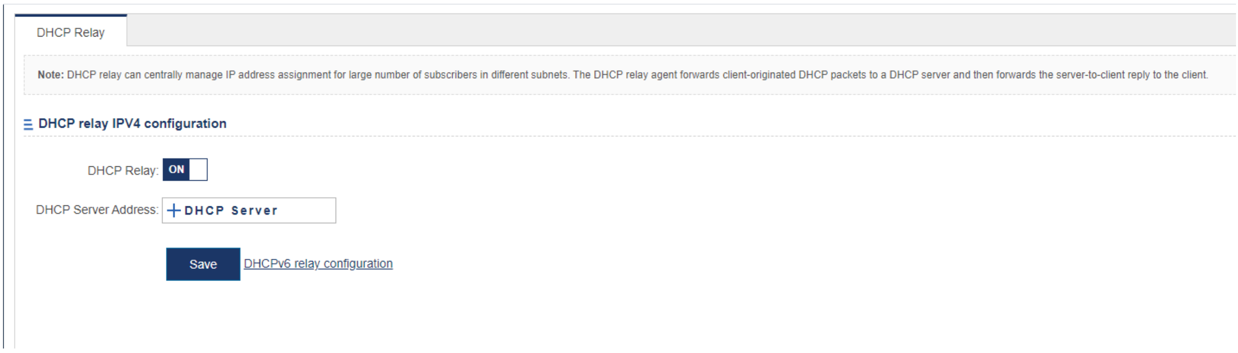
VLAN-based Statistics

VLAN	Group Address	Report Packet	Leave Packet Received	Port
1	224.0.1.140	1897	0	Gi0/1
1	230.230.230.230	133	0	Gi0/1
1	239.192.152.143	1737	0	Gi0/1
1	239.255.255.250	16830	0	Gi0/1
5	224.0.1.1	0	0	Gi0/3

Show No.: 10 Total Count: 5

5. DHCP Relay

Figure 1-22 DHCP Relay



Note: DHCP relay can centrally manage IP address assignment for large number of subscribers in different subnets. The DHCP relay agent forwards client-originated DHCP packets to a DHCP server and then forwards the server-to-client reply to the client.

DHCP relay IPV4 configuration

DHCP Relay: ON

DHCP Server Address: + DHCP Server

Enable or disable DHCP relay. When DHCP relay is enabled, you can set multiple DHCP server addresses.

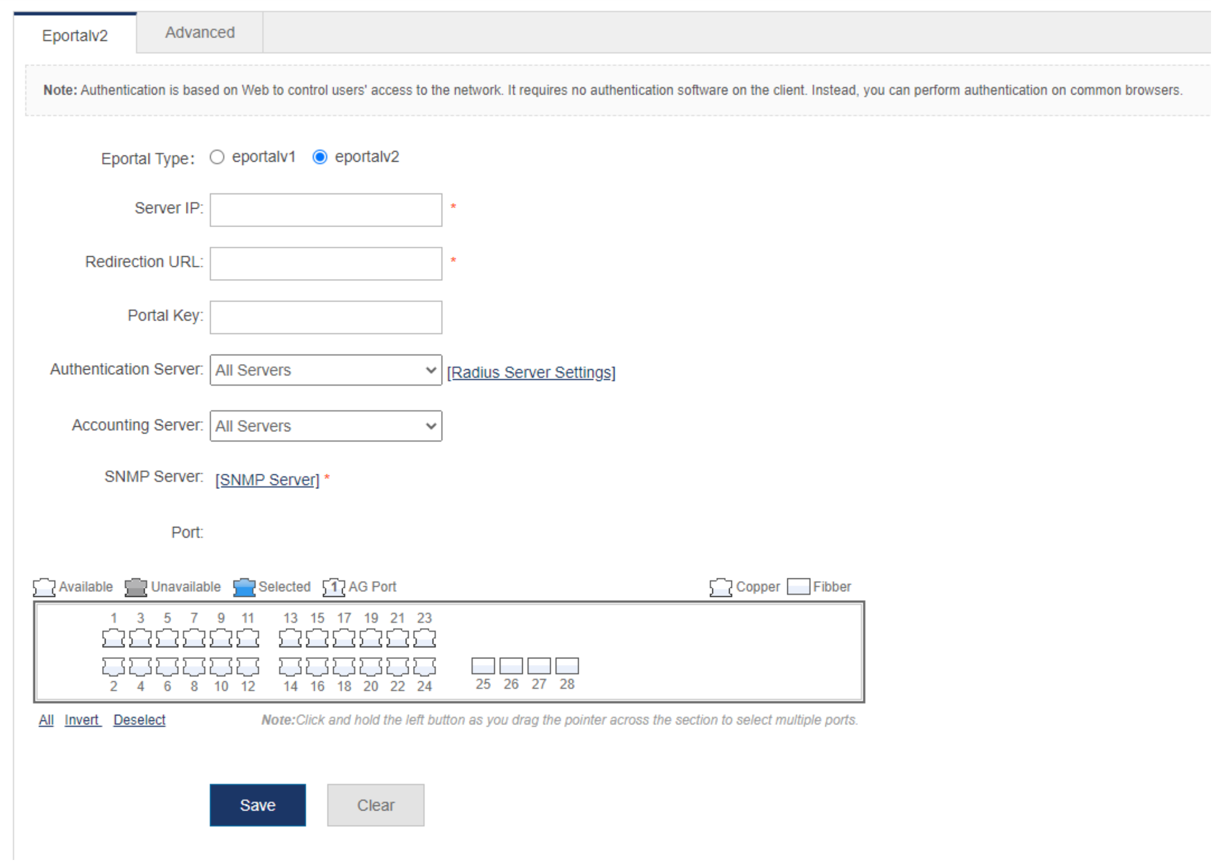
6. Authentication

The **Authentication** page allows you to configure ePortal and advanced settings.

(1) ePortal

Figure 1-23 shows the **ePortal** tab page.

Figure 1-23 ePortal



Note: Authentication is based on Web to control users' access to the network. It requires no authentication software on the client. Instead, you can perform authentication on common browsers.

Eportal Type: ○ eportalv1 ● eportalv2

Server IP: *

Redirection URL: *

Portal Key:

Authentication Server: All Servers [Radius Server Settings]

Accounting Server: All Servers

SNMP Server: [SNMP Server] *

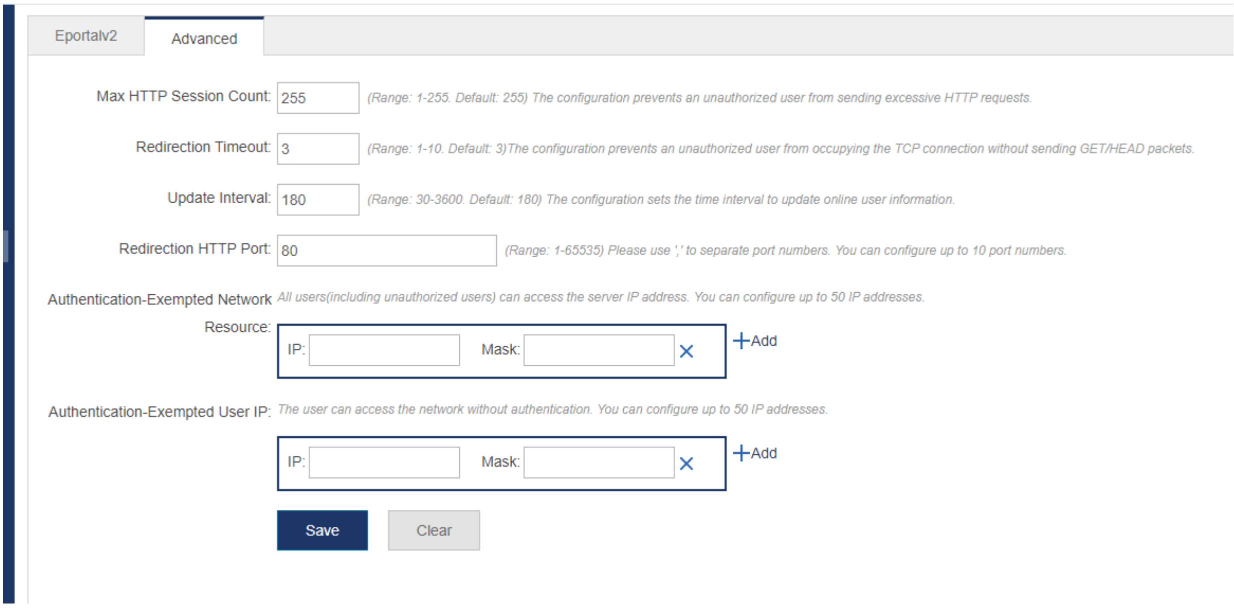
Port:

Note:Click and hold the left button as you drag the pointer across the section to select multiple ports.

The server IP address and redirection URL are mandatory. Other parameters are optional. Click **Save**. Themessage “Configuration Succeeded.” is displayed.

(2) Advanced Settings

Figure 1-24 Advanced Settings



Max HTTP Session Count: 255 *(Range: 1-255. Default: 255) The configuration prevents an unauthorized user from sending excessive HTTP requests.*

Redirection Timeout: 3 *(Range: 1-10. Default: 3)The configuration prevents an unauthorized user from occupying the TCP connection without sending GET/HEAD packets.*

Update Interval: 180 *(Range: 30-3600. Default: 180) The configuration sets the time interval to update online user information.*

Redirection HTTP Port: 80 *(Range: 1-65535) Please use ',' to separate port numbers. You can configure up to 10 port numbers.*

Authentication-Exempted Network Resource: *All users(including unauthorized users) can access the server IP address. You can configure up to 50 IP addresses.*

IP: Mask:

Authentication-Exempted User IP: *The user can access the network without authentication. You can configure up to 50 IP addresses.*

IP: Mask:

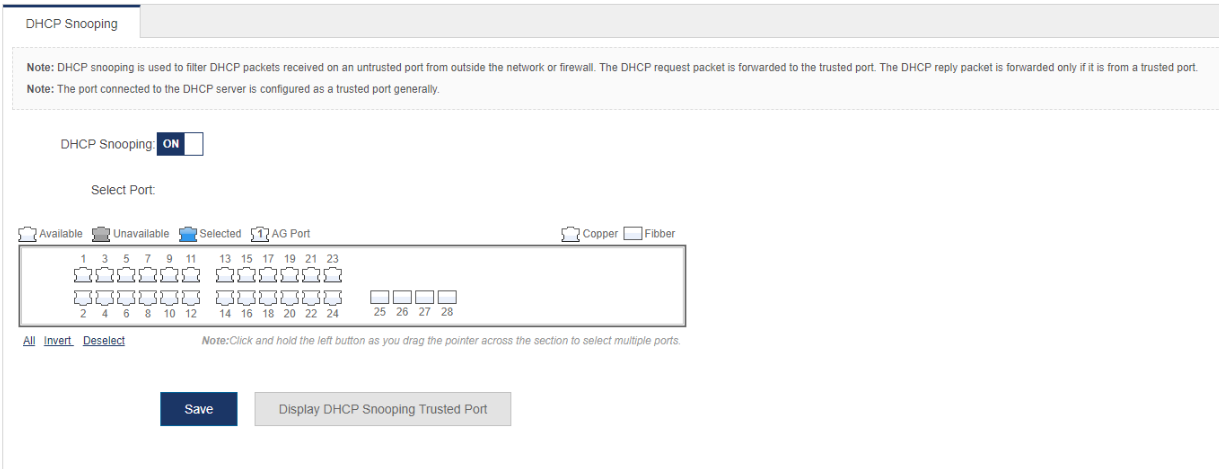
You can configure multiple IP addresses and masks for authentication-free network resources and users. Configure other settings and click **Save**. The message “Configuration Succeeded.” is displayed.

1.3.4 Security

Click the primary menu Security to access the secondary menu, including DHCP Snooping, Gateway Anti-ARP-Snooping, IP Source Guard, Port Security, NFPP and Storm Control.

1. DHCP Snooping

Figure 1-25 DHCP Snooping



DHCP Snooping

Note: DHCP snooping is used to filter DHCP packets received on an untrusted port from outside the network or firewall. The DHCP request packet is forwarded to the trusted port. The DHCP reply packet is forwarded only if it is from a trusted port.

Note: The port connected to the DHCP server is configured as a trusted port generally.

DHCP Snooping: ON

Select Port:

Note:Click and hold the left button as you drag the pointer across the section to select multiple ports.

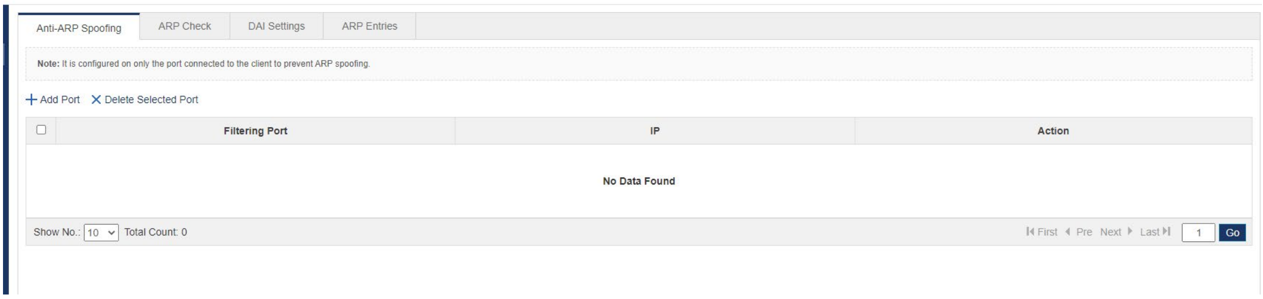
The port connected to a DHCP server needs to be configured as a DHCP trusted port. The DHCP server connected to a non-trusted port cannot work properly. The selected port is configured as a DHCP trusted port. You can select ports on the panel and click **Save**.

2. Gateway Anti-ARP-Snooping

The Gateway Anti-ARP-Snooping page allows you to configure anti-ARP-spoofing, ARP check, DAI settings, and ARP entries.

(1) Anti-ARP-Spoofing

Figure 1-26 Anti-ARP-Spoofing



Note: It is configured on only the port connected to the client to prevent ARP spoofing.

□	Filtering Port	IP	Action
		No Data Found	

Show No.: 10 Total Count: 0

- Adding a Filter Port

You must enter an IP address to add a filter port. Click **Save**. The message “Configuration Succeeded.” isdisplayed. The added filter port is displayed in the filter port list.

- Editing a Filter Port

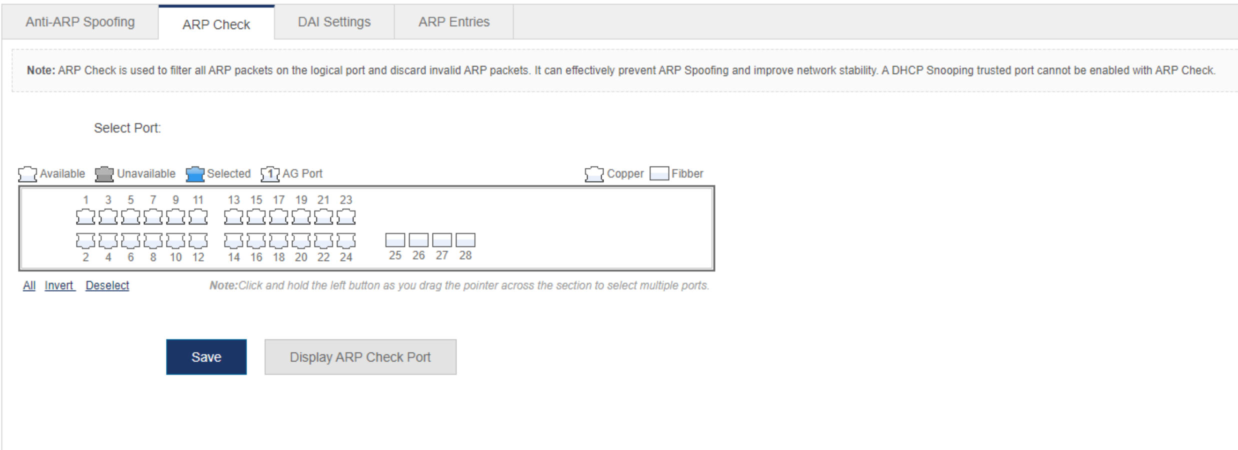
In the filter port list, click **Edit** in the **Action** column for a filter port. Port information is displayed. Edit theinformation and click **Save**. The message “Configuration succeeded” is displayed.

- Deleting a Filter Port
  - Select multiple records in the filter port list and click **Delete Selected Port** to batch delete the records.

- In the filter port list, click **Delete** in the **Action** column for a filter port. The message "Are you sure you want to delete the port?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the profile is deleted.

(2) ARP Check

Figure 1-27 ARP Check



Note: ARP Check is used to filter all ARP packets on the logical port and discard invalid ARP packets. It can effectively prevent ARP Spoofing and improve network stability. A DHCP Snooping trusted port cannot be enabled with ARP Check.

Note: Click and hold the left button as you drag the pointer across the section to select multiple ports.

The selected ports on the panel are enabled with ARP check.

Note

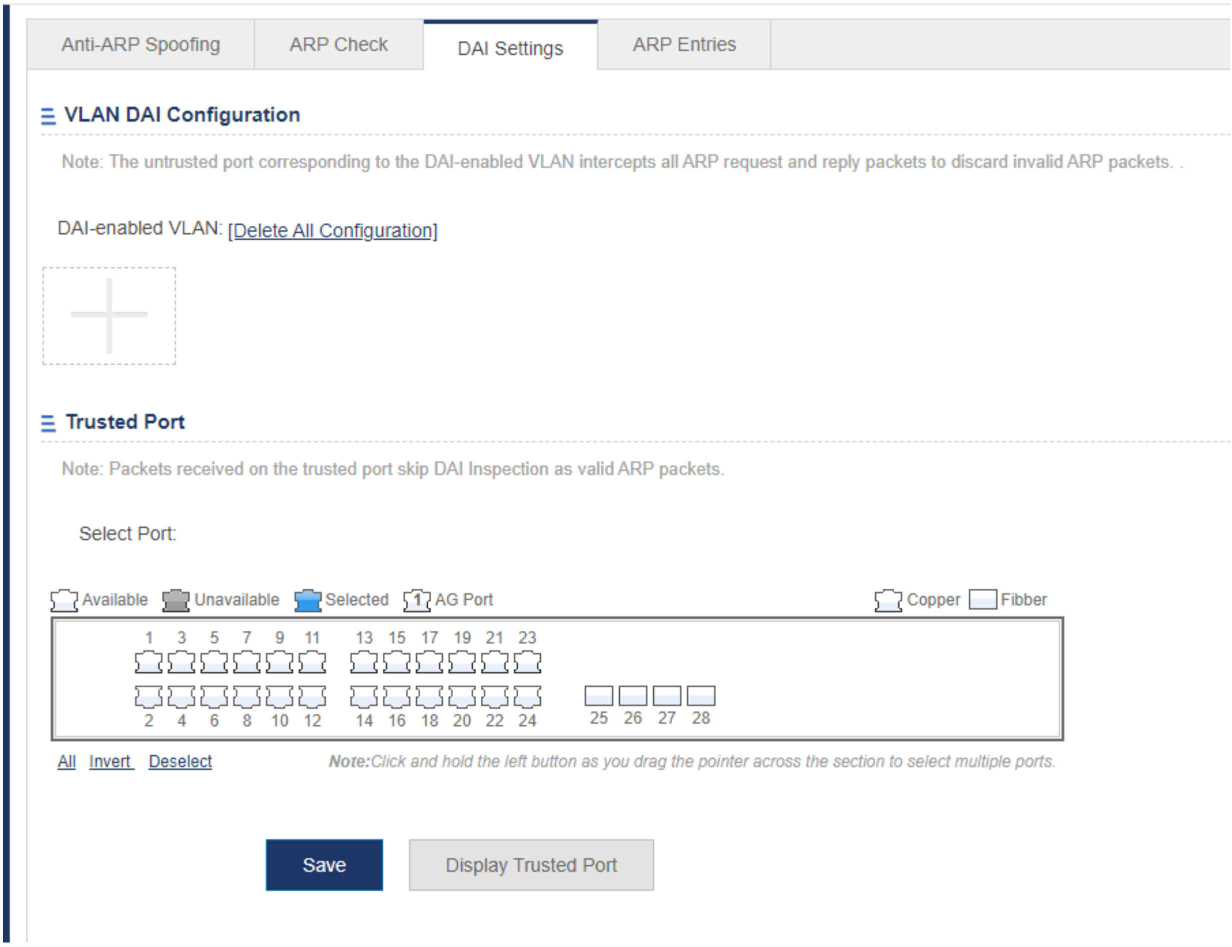
The panel displays ports with the ARP check function enabled and the ports can be edited. To cancel modification of a port, click **Display ARP Check Port** to display the current ports enabled with ARP check onthe panel

Caution

The ARP check function cannot be enabled on DHCP snooping trusted ports.

(1) DAI Settings

Figure 1-28 DAI Settings



Anti-ARP Spoofing | ARP Check | DAI Settings | ARP Entries

VLAN DAI Configuration

Note: The untrusted port corresponding to the DAI-enabled VLAN intercepts all ARP request and reply packets to discard invalid ARP packets. .

DAI-enabled VLAN: [Delete All Configuration]

Trusted Port

Note: Packets received on the trusted port skip DAI Inspection as valid ARP packets.

Select Port:

All Invert Deselect

Note:*Click and hold the left button as you drag the pointer across the section to select multiple ports.*

Save | Display Trusted Port

- VLAN DAI Settings

Click the add icon to add a VLAN where DAI is enabled.

- DAI Trusted Port

Select a port on the panel to enable the DAI trusted port.

Note

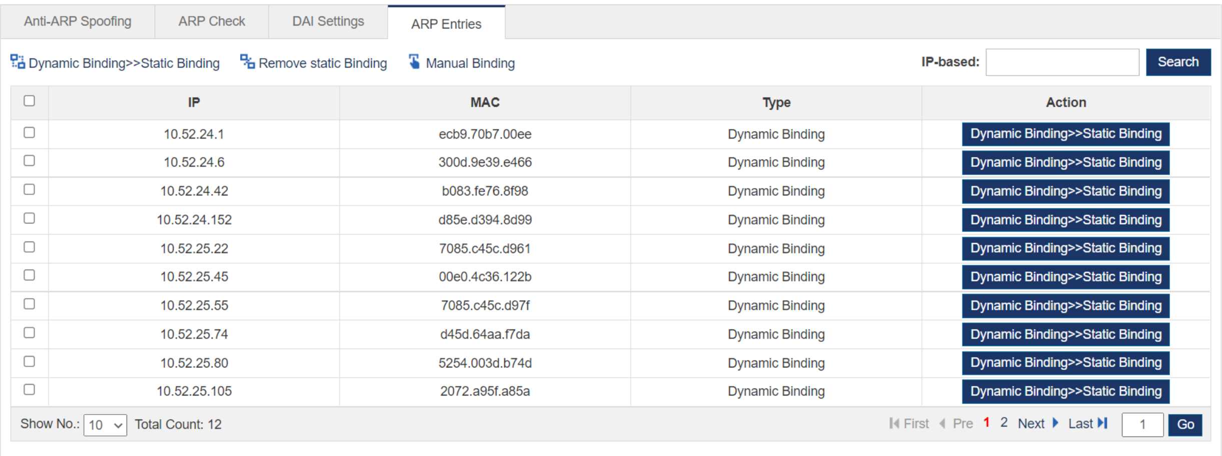
The panel displays DAI trusted ports and the ports can be edited. To cancel modification of a port, click **Display Trusted Port** to display current DAI trusted ports on the panel.

Caution

The ARP check function cannot be enabled on DHCP snooping trusted ports.

(2) ARP Entries

Figure 1-29 ARP Entries



Anti-ARP Spoofing | ARP Check | DAI Settings | ARP Entries

Dynamic Binding>>Static Binding | Remove static Binding | Manual Binding | IP-based: | Search

□	IP	MAC	Type	Action
□	10.52.24.1	ecb9.70b7.00ee	Dynamic Binding	Dynamic Binding>>Static Binding
□	10.52.24.6	300d.9e39.e466	Dynamic Binding	Dynamic Binding>>Static Binding
□	10.52.24.42	b083.fe76.8f98	Dynamic Binding	Dynamic Binding>>Static Binding
□	10.52.24.152	d85e.d394.8d99	Dynamic Binding	Dynamic Binding>>Static Binding
□	10.52.25.22	7085.c45c.d961	Dynamic Binding	Dynamic Binding>>Static Binding
□	10.52.25.45	00e0.4c36.122b	Dynamic Binding	Dynamic Binding>>Static Binding
□	10.52.25.55	7085.c45c.d97f	Dynamic Binding	Dynamic Binding>>Static Binding
□	10.52.25.74	d45d.64aa.f7da	Dynamic Binding	Dynamic Binding>>Static Binding
□	10.52.25.80	5254.003d.b74d	Dynamic Binding	Dynamic Binding>>Static Binding
□	10.52.25.105	2072.a95f.a85a	Dynamic Binding	Dynamic Binding>>Static Binding

Show No.: 10 Total Count: 12 First Pre 1 2 Next Last 1 Go

- Dynamic binding >> static binding
  - Select multiple dynamic binding entries in the ARP entry list and click **Dynamic Binding >> StaticBinding**.
  - In the ARP entry list, click **Dynamic Binding >> Static Binding** in the **Action** column for an ARP entry.The message "Configuration succeeded." is displayed.
- Removing a Static Bindings
  - Select multiple static binding entries in the ARP entry list and click **Remove Static Binding** to batchremove static bindings.
  - In the ARP entry list, click **Remove Static Binding** in the **Action** column for a static binding entry. Themessage "Configuration succeeded." is displayed.
- Manual binding

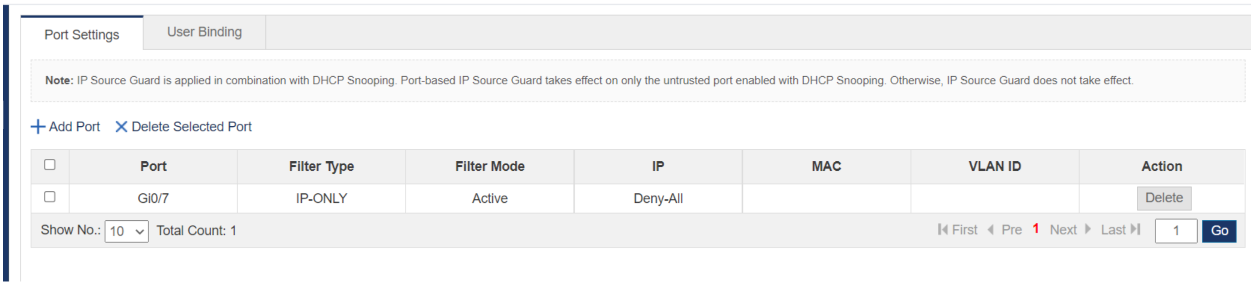
  You must enter an IP address and a MAC address to add a static binding entry. Click **Save**. The message"Configuration Succeeded." is displayed. The added static binding entry is displayed in the port filter list.

3. IP Source Guard

The **IP Source Guard** page allows you to configure ports and bind users.

(1) Port Settings

Figure 1-30 Port Settings



Port Settings | User Binding

Note: IP Source Guard is applied in combination with DHCP Snooping. Port-based IP Source Guard takes effect on only the untrusted port enabled with DHCP Snooping. Otherwise, IP Source Guard does not take effect.

+ Add Port | ✕ Delete Selected Port

□	Port	Filter Type	Filter Mode	IP	MAC	VLAN ID	Action
□	Gi0/7	IP-ONLY	Active	Deny-All			Delete

Show No.: 10 Total Count: 1 First Pre 1 Next Last 1 Go

- Adding a Port Enabled with IP Source Guard

  Click **Add Port** and select a filter type and a port to add a port enabled with IP source guard. Click **Save**. The message "Configuration Succeeded." is displayed. The added port is displayed in the list of ports enabled with IP source guard.
- Editing a Port Enabled with IP Source Guard

In the list of ports enabled with IP source guard, click **Edit** in the **Action** column for a port. Port information is displayed. Edit the information and click **Save**. The message "Configuration succeeded" is displayed.

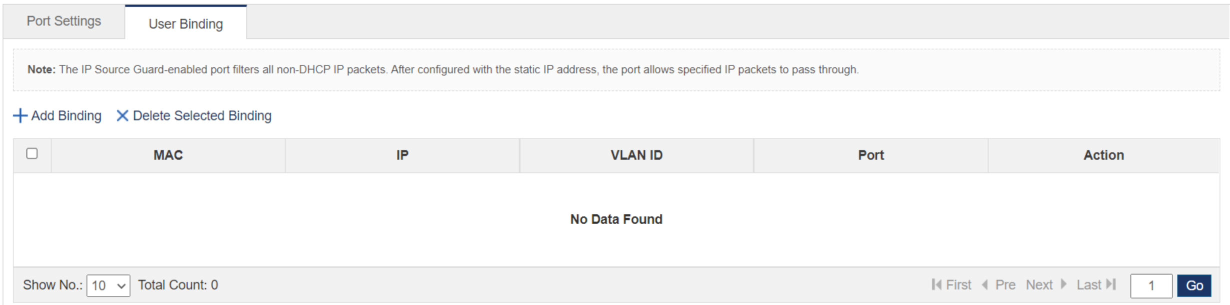
- Deleting a Port Enabled with IP Source Guard

o Select multiple records in the list of ports enabled with IP source guard and click **Delete Selected Port** to batch delete records.

o In the list of ports enabled with IP source guard, click **Delete** in the **Action** column for a port. The message "Are you sure you want to delete the item?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the port is displayed.

(2) User Binding

Figure 1-31 User Binding



Note: The IP Source Guard-enabled port filters all non-DHCP IP packets. After configured with the static IP address, the port allows specified IP packets to pass through.

□	MAC	IP	VLAN ID	Port	Action
			No Data Found		

- Adding a User Binding

You must enter a MAC address, an IP address, and a VLAN ID to add a user binding. Click **Save**. The message "Configuration Succeeded." is displayed. The added binding is displayed in the user binding list.

- Editing a User Binding

In the user binding list, click **Edit** in the **Action** column for a user binding. Binding information is displayed. Editthe information and click **Save**. The message "Configuration succeeded" is deleted.

- Deleting a User Binding

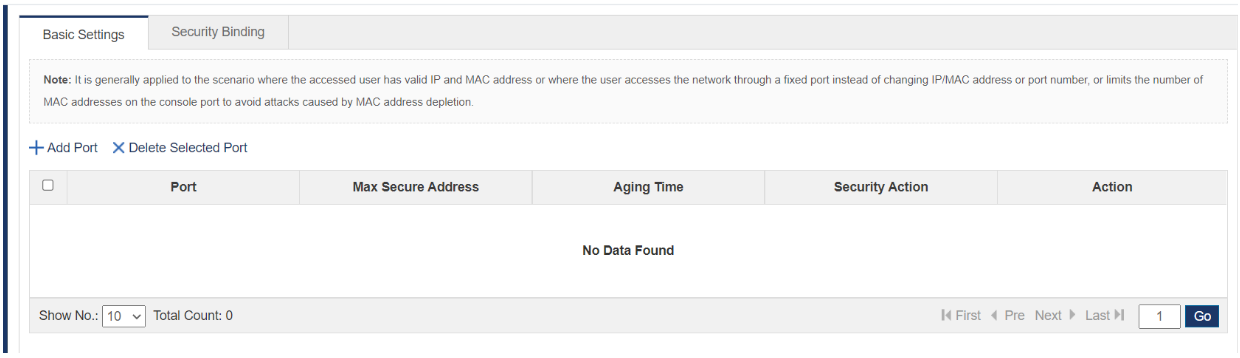
o Select multiple records in the user binding list and click **Delete Selected Binding** to batch delete records.

o In the user binding list, click **Delete** in the **Action** column for a port. The message "Are you sure you want to delete the binding?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the binding is displayed.

4. Port Security

(1) Basic Settings

Figure 1-32 Basic Settings



Basic Settings | Security Binding

Note: It is generally applied to the scenario where the accessed user has valid IP and MAC address or where the user accesses the network through a fixed port instead of changing IP/MAC address or port number, or limits the number of MAC addresses on the console port to avoid attacks caused by MAC address depletion.

+ Add Port ✕ Delete Selected Port

□	Port	Max Secure Address	Aging Time	Security Action	Action
			No Data Found		

Show No.: 10 Total Count: 0 First Pre Next Last 1 Go

- Adding a Security Port

The IP address is mandatory. Other parameters are optional. Click **Save** and the message "ConfigurationSucceeded." is displayed. The added port is displayed in the security port list.

- Editing a Security Port

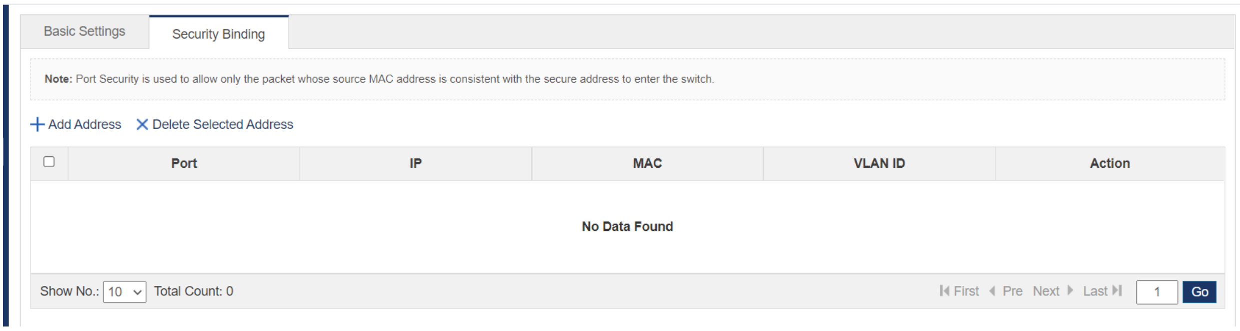
In the security port list, click **Edit** in the **Action** column for a security port. The user binding information is displayed. Edit the information and click **Save**. The message "Configuration succeeded" is displayed.

- Deleting a Security Port

  - Select multiple records in the user binding list and click **Delete Selected Binding** to batch delete records.
  - In the security port list, click **Delete** in the **Action** column for a port. The message "Are you sure you want to delete the security port?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the port is deleted.

(2) Security Binding

Figure 1-33 Security Binding



Basic Settings | Security Binding

Note: Port Security is used to allow only the packet whose source MAC address is consistent with the secure address to enter the switch.

+ Add Address ✕ Delete Selected Address

□	Port	IP	MAC	VLAN ID	Action
			No Data Found		

Show No.: 10 Total Count: 0 First Pre Next Last 1 Go

- Adding a Bound Security Address

The IP address is mandatory. Other parameters are optional. Click **Save.** The message "Configuration Succeeded." is displayed. The added address is displayed in the bound security address list.

- Editing a Bound Security Address

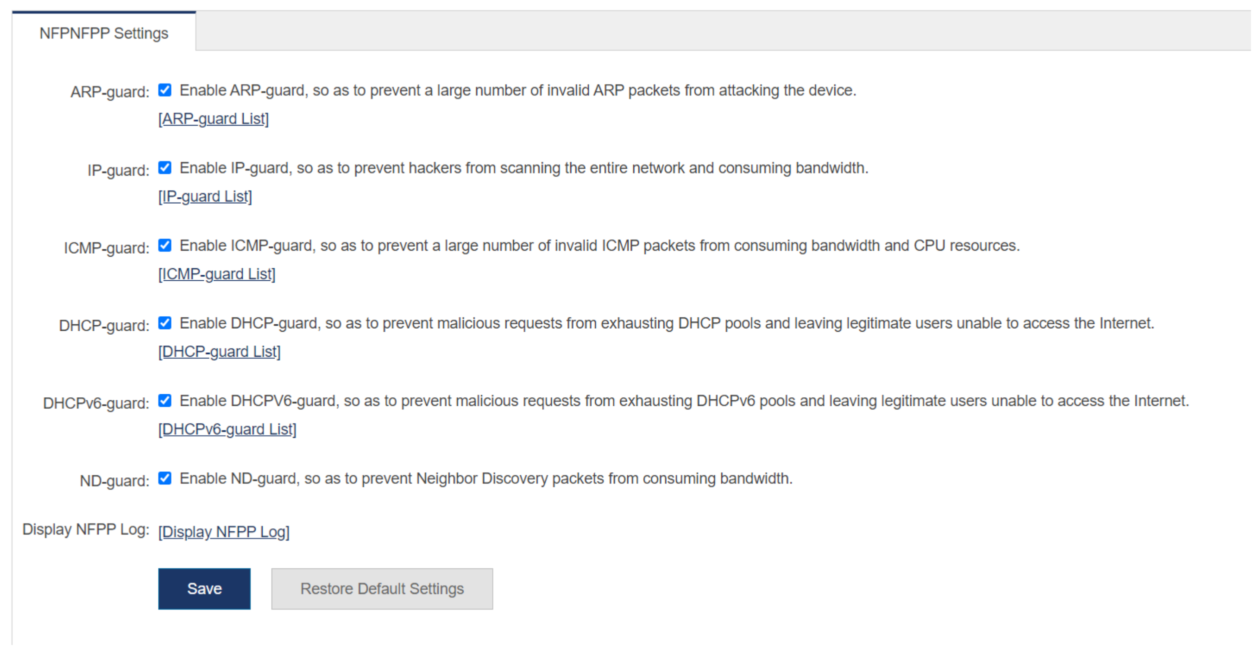
In the bound security address list, click **Edit** in the **Action** column for an address. User binding information is displayed. Edit the information and click **Save**. The message "Configuration succeeded" is displayed.

- Deleting a Bound Security Address

- Select multiple records in the bound security address list and click **Delete Selected Address** to batchdelete records.
- In the bound security address list, click **Delete** in the **Action** column for a bound security address. Themessage "Are you sure you want to delete the bound security address?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the bound security address is deleted.

5. NFPP

Figure 1-34 NFPP



NFPNFPP Settings

ARP-guard: ☑ Enable ARP-guard, so as to prevent a large number of invalid ARP packets from attacking the device.
[ARP-guard List]

IP-guard: ☑ Enable IP-guard, so as to prevent hackers from scanning the entire network and consuming bandwidth.
[IP-guard List]

ICMP-guard: ☑ Enable ICMP-guard, so as to prevent a large number of invalid ICMP packets from consuming bandwidth and CPU resources.
[ICMP-guard List]

DHCP-guard: ☑ Enable DHCP-guard, so as to prevent malicious requests from exhausting DHCP pools and leaving legitimate users unable to access the Internet.
[DHCP-guard List]

DHCPv6-guard: ☑ Enable DHCPV6-guard, so as to prevent malicious requests from exhausting DHCPv6 pools and leaving legitimate users unable to access the Internet.
[DHCPv6-guard List]

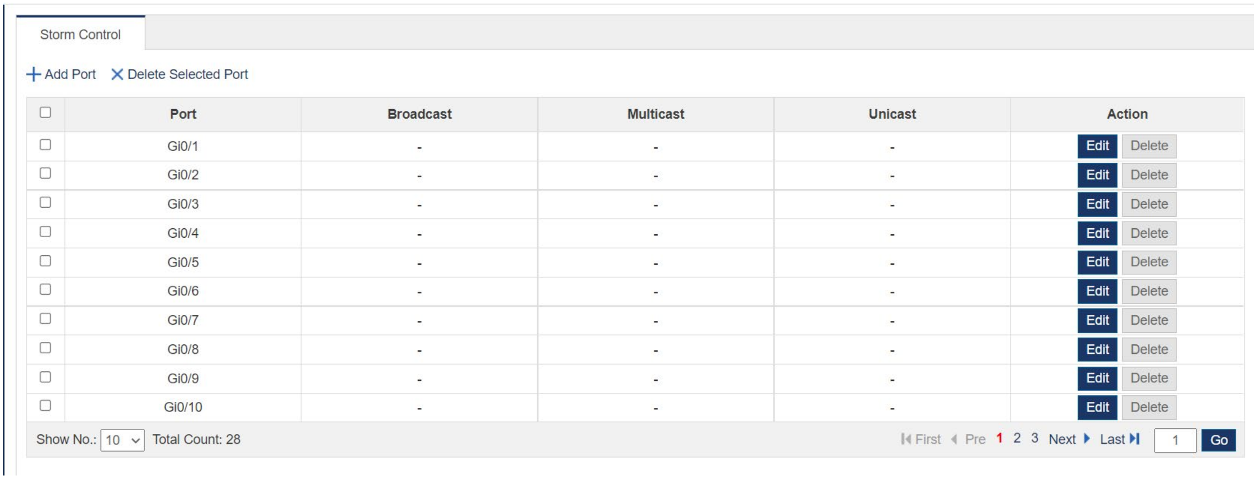
ND-guard: ☑ Enable ND-guard, so as to prevent Neighbor Discovery packets from consuming bandwidth.

Display NFPP Log: [Display NFPP Log]

You can enable or disable each attack guard function and click **Save**. The message “Configuration succeeded”is displayed. To restore default settings, click **Restore Default Settings**.

6. Storm Control

Figure 1-35 Storm Control



□	Port	Broadcast	Multicast	Unicast	Action
□	Gi0/1	-	-	-	Edit Delete
□	Gi0/2	-	-	-	Edit Delete
□	Gi0/3	-	-	-	Edit Delete
□	Gi0/4	-	-	-	Edit Delete
□	Gi0/5	-	-	-	Edit Delete
□	Gi0/6	-	-	-	Edit Delete
□	Gi0/7	-	-	-	Edit Delete
□	Gi0/8	-	-	-	Edit Delete
□	Gi0/9	-	-	-	Edit Delete
□	Gi0/10	-	-	-	Edit Delete

Show No.: 10 Total Count: 28

- Adding a Port Enabled with Storm Control

You must enter one of the broadcast address, unicast address, and multicast address to add a port enabled withstorm control port. Click **Save**. The message "Configuration Succeeded." is displayed. The added port is displayed in the list of ports enabled with storm control.

- Editing a Port Enabled with Storm Control

In the list of ports enabled with storm control, click **Edit** in the **Action** column for a port. Information about the port enabled with storm control is displayed. Edit the information and click **Save**. The message "Configuration succeeded" is displayed.

- Deleting a Port Enabled with Storm Control

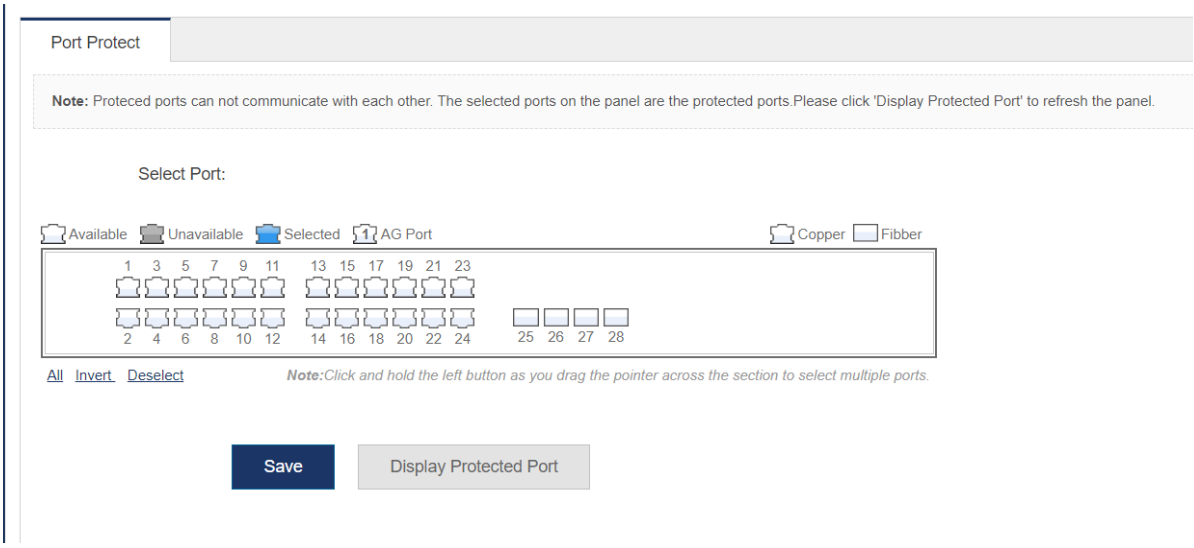
o Select multiple records in the list of ports enabled with storm control and click **Delete Selected Port** tobatch delete records.

o In the list of ports enabled with storm control, click **Delete** in the Action column for a port. The message"Are you sure you want to delete the storm control port?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the port enabled with storm control is deleted.

1.3.5 Advanced

1. Port Protection

Figure 1-36 Port Protect



Note: Proteced ports can not communicate with each other. The selected ports on the panel are the protected ports.Please click 'Display Protected Port' to refresh the panel.

Note:Click and hold the left button as you drag the pointer across the section to select multiple ports.

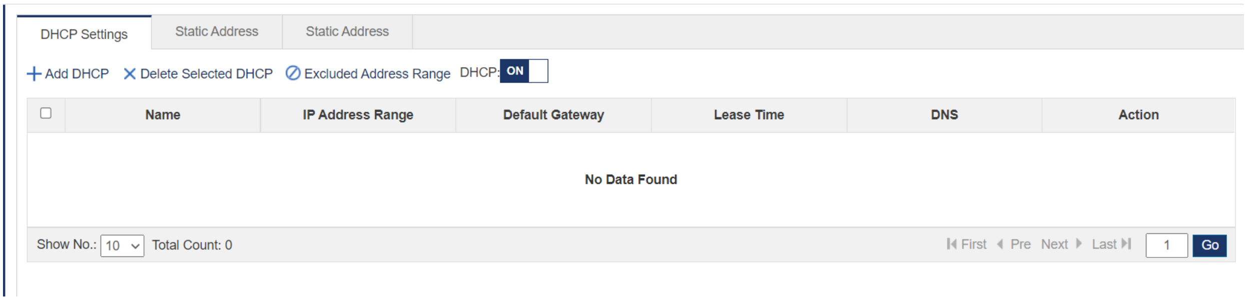
Select a port on the panel to be configured as a protected port. Click **Save**. The message "Configuration Succeeded." is displayed.

2. DHCP Server

The **DHCP Server** page allows you to configure DHCP and allocate static addresses and displays the client list.

(1) DHCP Settings

Figure 1-37 DHCP Settings


DHCP Settings | Static Address | Static Address

+ Add DHCP ✕ Delete Selected DHCP ⊘ Excluded Address Range DHCP: ON

□	Name	IP Address Range	Default Gateway	Lease Time	DNS	Action
			No Data Found			

Show No.: 10 Total Count: 0 First Pre Next Last 1 Go

- Adding a DHCP Address Pool

Enter an address pool name, an IP address range, a mask, a default gateway address, and the lease time. Click **Save**. The message "Configuration succeeded." is displayed. The added address pool is displayed in the DHCPaddress pool list.

- Editing a DHCP Address Pool

In the DHCP address pool list, click **Edit** in the **Action** column for an address pool. DHCP information is displayed. Edit the information and click **Save**. The message "Configuration succeeded" is displayed.

- Deleting a DHCP Address Pool

o Select multiple records in the DHCP address pool list and click **Delete Selected DHCP** to batch deleterecords.

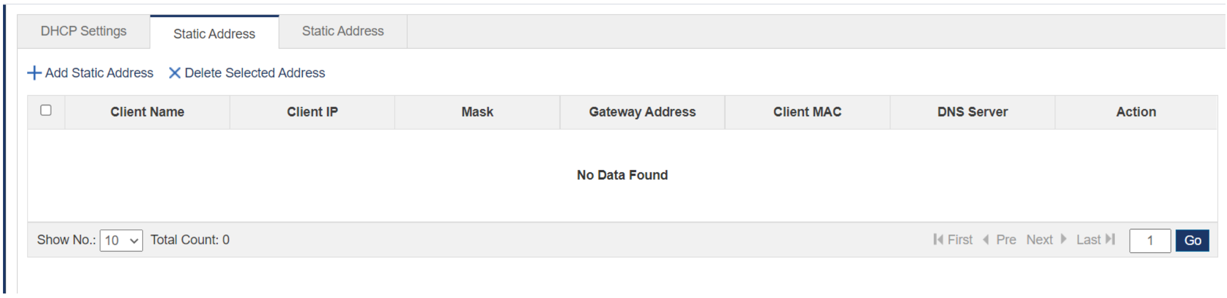
o In the DHCP address pool list, click **Delete** in the Action column for an address pool. The message "Areyou sure you want to delete the address pool?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the DHCP address pool is deleted.

- Enabling DHCP

Click the **DHCP** button to enable the DHCP service.

(2) Static Address

Figure 1-38 Static Address


DHCP Settings | Static Address | Static Address

+ Add Static Address ✕ Delete Selected Address

□	Client Name	Client IP	Mask	Gateway Address	Client MAC	DNS Server	Action
				No Data Found			

Show No.: 10 Total Count: 0 First Pre Next Last 1 Go

- Adding a Static Address

The client's name, client IP address, and client MAC address are mandatory. Other parameters are optional. Click **Save**. The message "Configuration succeeded." is displayed. The added address is displayed in the static address list.

- Editing a Static Address

In the static address list, click **Edit** in the **Action** column for an address. Static address information is displayed.Edit the information and click **Save**. The message "Configuration succeeded" is displayed.

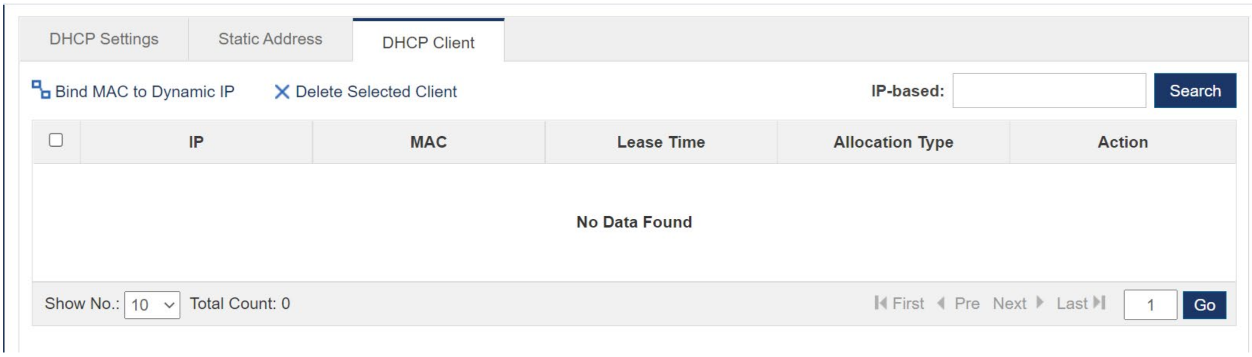
- Delete Static Address

o Select multiple records in the static address list and click **Delete Selected Address** to batch deleterecords.

- In the static address list, click **Delete** in the **Action** column for a static address. The message "Are yousure you want to delete the static address?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the static address is deleted.

(3) Client Display

Figure 1-39 Client Display



□	IP	MAC	Lease Time	Allocation Type	Action
No Data Found					

- Querying an IP address

Enter an IP address in the search box and click **Search** to query the IP address.

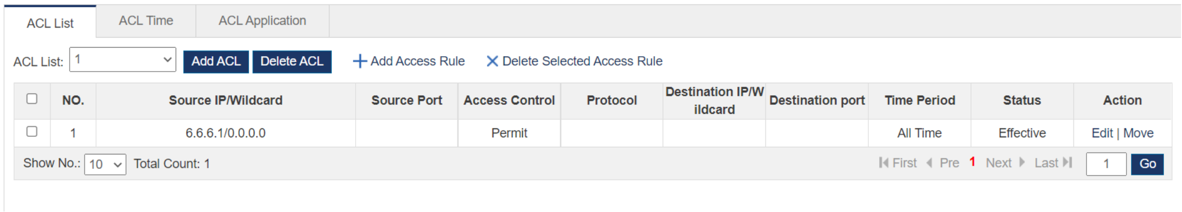
- Binding a MAC Address to a Dynamic IP Address

Select multiple records in the client list and click **Bind MAC to Dynamic IP** to bind the IP address to the MACaddress.

3. ACL

(1) ACL List

Figure 1-40 ACL List



□	NO.	Source IP/Wildcard	Source Port	Access Control	Protocol	Destination IP/Wildcard	Destination port	Time Period	Status	Action
□	1	6.6.6.1/0.0.0.0		Permit				All Time	Effective	Edit | Move

- Adding an ACL

Click **Add ACL** and configure the ACL to be added. You must enter an ACL. Click **Save**. The message“Configuration succeeded.” is displayed. The added ACL is displayed in the ACL list.

- Deleting an ACL

In the ACL list, select the ACL to be deleted and click **Delete ACL**. The message "Delete succeeded." isdisplayed.

- Adding an ACL Rule

Select an ACL type, a protocol, and a time, and configure an IP address to add an ACL rule. Click **Save**.The message “Configuration succeeded.” is displayed. The added ACL rule is displayed in the ACL rule list.

- Editing an ACL Rule

In the ACL rule list, click **Edit** in the **Action** column for a rule. ACL rule information is displayed. Edit theinformation and click **Save**. The message “Configuration succeeded” is displayed.

- Deleting an ACL Rule

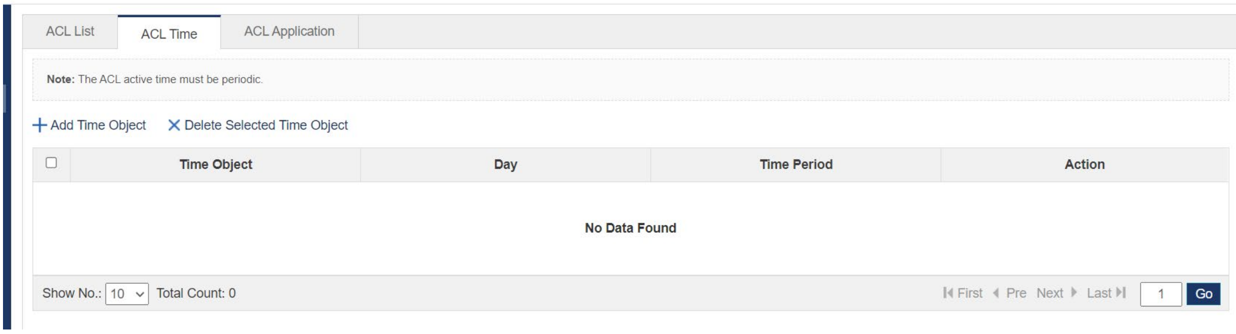
- Select multiple records in the ACL rule list and click **Delete Selected Access Rule** to batch deleterecords.
- In the ACL rule list, click **Delete** in the **Action** column for a rule. The message "Are you sure you want todelete the rule?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the rule is deleted.

- Moving an ACL Rule

Enter the ID of an ACL rule to be moved and click **Move**. The message "Configuration succeeded." is displayed.

(2) ACL Time

Figure 1-41 ACL Time



Note: The ACL active time must be periodic.

□	Time Object	Day	Time Period	Action
		No Data Found		

- Adding ACL Time

Enter the time object name and select a time to add an ACL time. Click **Save**. The message "Configurationsucceeded." is displayed. The added ACL time is displayed in the ACL time list.

- Editing ACL Time

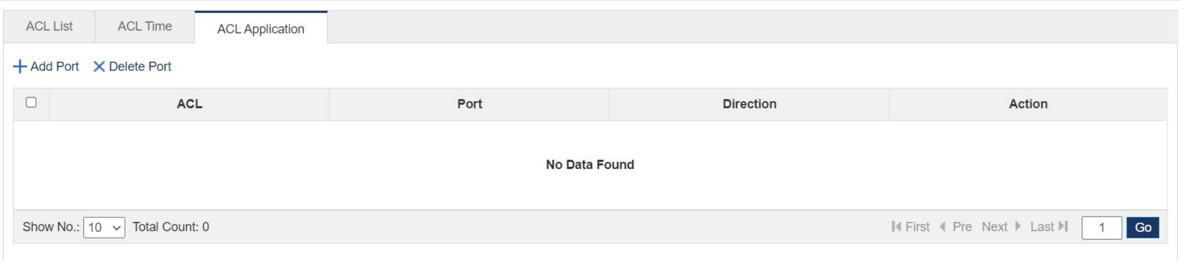
In the ACL time list, click **Edit** in the **Action** column for an ACL time. ACL time information is displayed. Edit theinformation and click **Save**. The message "Configuration succeeded" is displayed.

- Deleting ACL Time

Select multiple records in the ACL time list and click **Delete Selected Time Object** to batch delete records.

(3) ACL Application

Figure 1-42 ACL Application



□	ACL	Port	Direction	Action
		No Data Found		

- Adding an Applied ACL

Select an ACL list, a filter direction and a port and click **Save**. The message "Configuration succeeded." isdisplayed. The added ACL applied to a port is displayed in the applied ACL list.

- Editing an Applied ACL

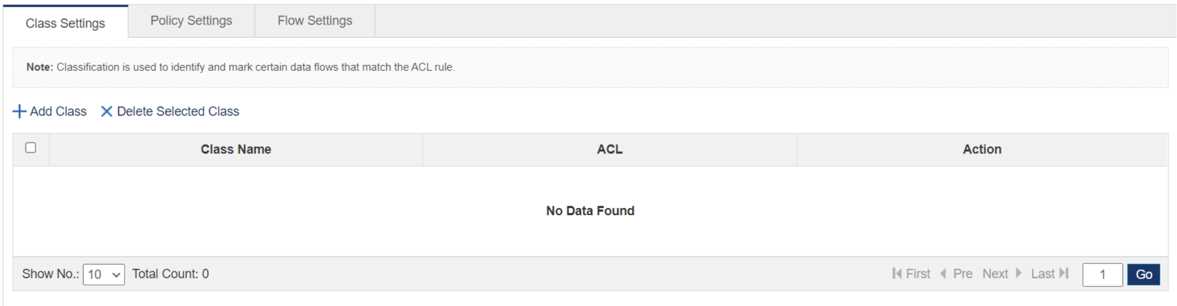
In the applied ACL list, click **Edit** in the **Action** column. Applied ACL information is displayed. Edit the informationand click **Save**. The message "Configuration succeeded" is displayed.

- Deleting an Applied ACL
  - Select multiple records in the applied ACL list and click **Delete Port** to batch delete records.
  - In the applied ACL list, click **Delete** in the **Action** column for an applied ACL. The message "Are yousure you want to delete the item?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the applied ACL is deleted.

4. QOS

(1) Classification Settings

Figure 1-43 Class Settings



Note: Classification is used to identify and mark certain data flows that match the ACL rule.

□	Class Name	ACL	Action
		No Data Found	

Show No.: 10 Total Count: 0 1

- Adding a class

The class name is mandatory. Select an ACL and click **Save**. The message “Configuration succeeded.” isdisplayed. The added class is displayed in the class list.

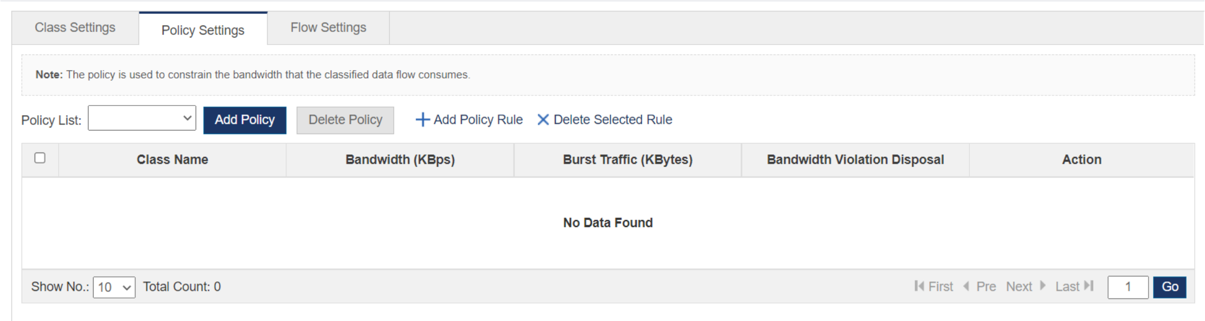
- Editing a Class

In the class list, click **Edit** in the **Action** column. Class information is displayed. Edit the information and click **Save**. The message “Configuration succeeded” is displayed.

- Deleting a Class
  - Select multiple records in the class list and click **Delete Selected Class** to batch delete records.
  - In the class list, click **Delete** in the **Action** column for a class. The message "Are you sure you want todelete the item?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the class is deleted.

(2) Policy Settings

Figure 1-44 Policy Settings



Note: The policy is used to constrain the bandwidth that the classified data flow consumes.

Policy List:

□	Class Name	Bandwidth (KBps)	Burst Traffic (KBytes)	Bandwidth Violation Disposal	Action
			No Data Found		

Show No.: 10 Total Count: 0 1

- Adding a Policy

The policy name is mandatory. Click **Save**. The message “Configuration succeeded.” is displayed. The added policy is displayed in the policy list.

- Deleting a Policy

In the policy list, click **Delete** in the **Action** column for a policy. The message "Are you sure you want to delete the item?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the policy is deleted.

- Adding a Policy Rule

The bandwidth and burst traffic are mandatory. Other parameters are optional. Click **Save**. The message “Configuration succeeded.” is displayed. The added policy rule is displayed in the policy rule list.

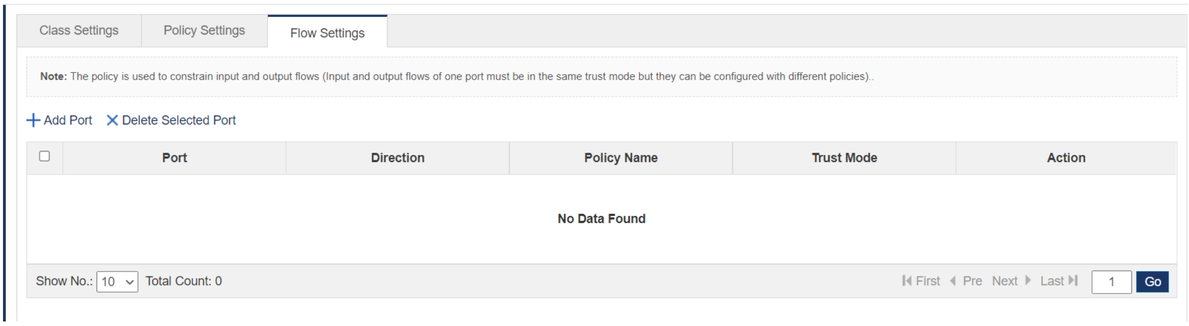
- Editing a Policy Rule

In the policy rule list, click **Edit** in the **Action** column for a policy rule. Policy rule information is displayed. Edit the information and click **Save**. The message “Configuration succeeded” is displayed.

- Deleting a Policy Rule
  - Select multiple records in the policy rule list and click **Delete Selected Rule** to batch delete records.
  - In the policy rule list, click **Delete** in the **Action** column for a rule. The message "Are you sure you wantto delete the item?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the policy rule is deleted.

(3) Flow Settings

Figure 1-45 Flow Settings



Note: The policy is used to constrain input and output flows (Input and output flows of one port must be in the same trust mode but they can be configured with different policies)..

□	Port	Direction	Policy Name	Trust Mode	Action
			No Data Found		

Show No.: 10 Total Count: 0

- Adding a Port to Which a Policy Is Applied

Select a rate-limiting direction, a trusted mode, a policy list, and a port. Click **Save**. The message “Configurationsucceeded.” is displayed. The added port is displayed in the list of ports to which a policy is applied.

- Deleting a Port to Which a Policy Is Applied
  - Select multiple records in the list of ports to which a policy is applied and click **Delete Selected Port** to batch delete records.
  - In the list, click **Delete** in the **Action** column for a rule. The message "Are you sure you want to delete the item?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the portis deleted.

1.3.6 System

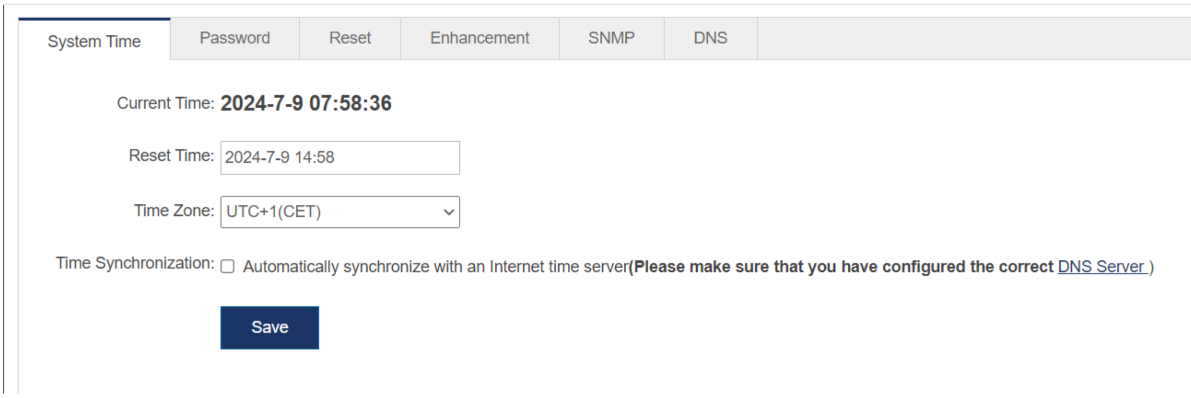
The **System** page allows you to configure system settings, upload the system, configure system logging, CWMP,and network detection, and use the web console.

1. Settings

The **Settings** page includes **System Time**, **Password**, **Reset**, **Enhancement**, **SNMP** and **DNS**.

(1) System Time

Figure 1-46 System Time



Current Time: **2024-7-9 07:58:36**

Reset Time: 2024-7-9 14:58

Time Zone: UTC+1(CET)

Time Synchronization: □ Automatically synchronize with an Internet time server(**Please make sure that you have configured the correct** DNS Server)

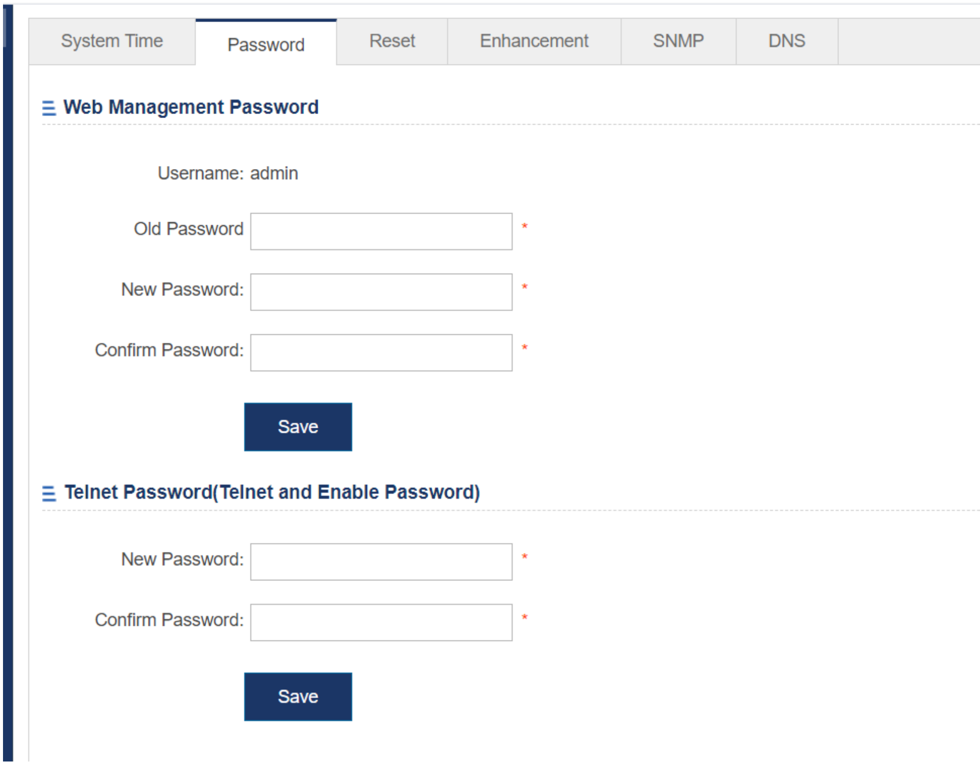
- System Time

The page displays the current system time. You can set the system time manually or click **Automatically synchronize with an Internet time server.**

Select either of the two methods to set the system time. Click **Save**. The message “Configuration succeeded.” is displayed.

(2) Password

Figure 1-47 Password



Web Management Password

Username: admin

Old Password *

New Password: *

Confirm Password: *

Telnet Password(Telnet and Enable Password)

New Password: *

Confirm Password: *

- Changing the Web Management Password

You need to enter the old password and enter a new password twice to change the web management password.If the input old password is incorrect, the message "Incorrect old password" in red font is displayed. You are required to enter the correct old password and click **Save** to complete the password change.

Note

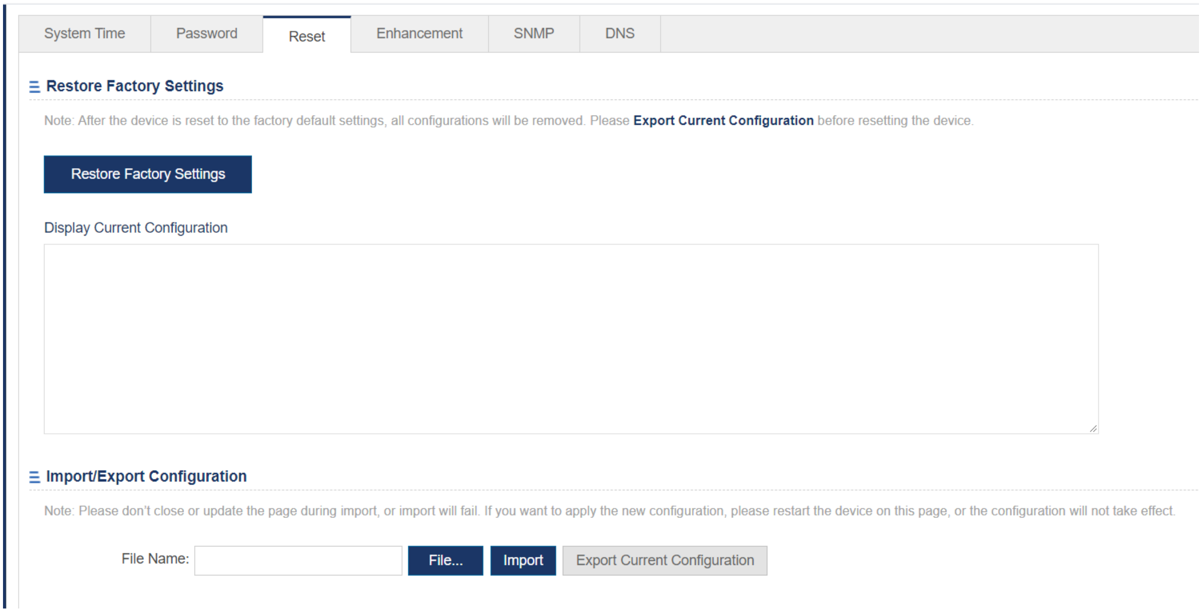
The enable password is changed by default when the password of the Web is changed.

- Changing the Telnet Authentication Password

To change the telnet password, you do not need to enter the old password but need to enter a new passwordtwice. Other operations are the same as those of changing the password of the super administrator.

(3) Reset

Figure 1-48 Reset



Restore Factory Settings

Note: After the device is reset to the factory default settings, all configurations will be removed. Please **Export Current Configuration** before resetting the device.

Import/Export Configuration

Note: Please don't close or update the page during import, or import will fail. If you want to apply the new configuration, please restart the device on this page, or the configuration will not take effect.

- Import/Export Configuration

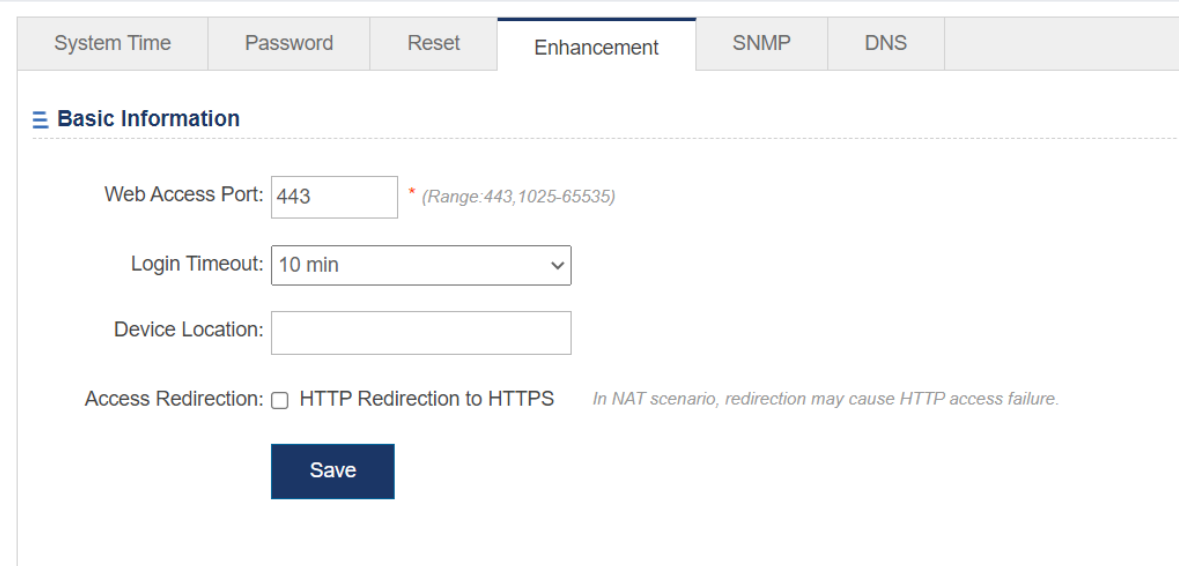
Import the configuration to modify the device configuration and restart the device to make the configuration takeeffect. Export the current configuration for backup.

- Restore Factory Settings

Click **Restore Factory Settings** to clear the configuration and restore factory settings.

(4) Enhancement

Figure 1-49 Enhancement



Web Access Port: 443 * (Range:443,1025-65535)

Login Timeout: 10 min

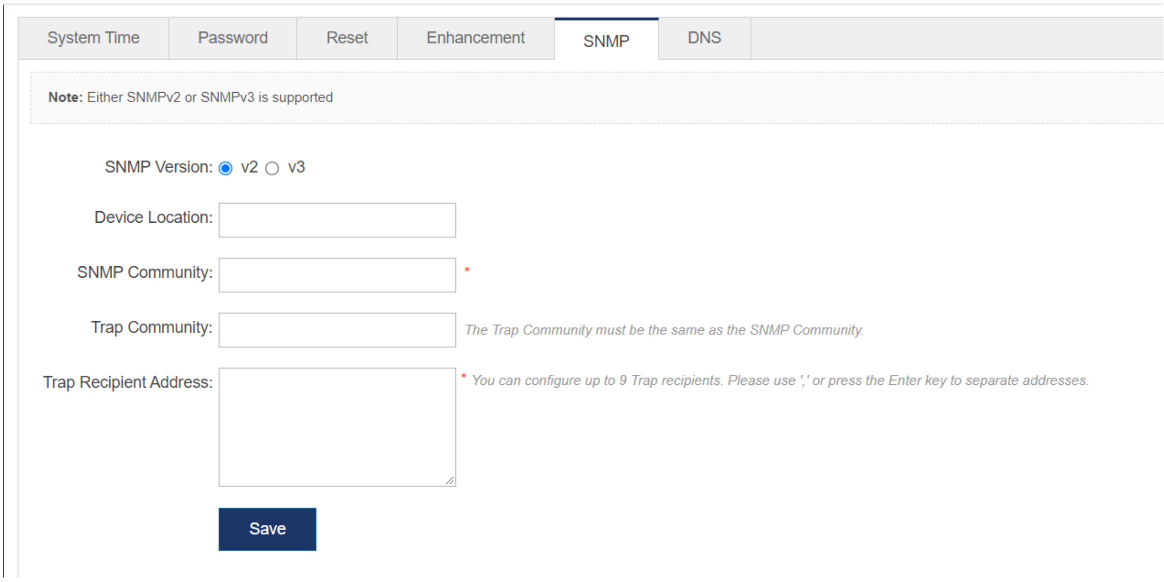
Device Location:

Access Redirection: □ HTTP Redirection to HTTPS In NAT scenario, redirection may cause HTTP access failure.

You must set a web access port. The login timeout and device location are optional. Click **Save**. The message“Configuration succeeded.” is displayed.

(5) SNMP

Figure 1-50 SNMP



Note: Either SNMPv2 or SNMPv3 is supported

SNMP Version: ● v2 ○ v3

Device Location:

SNMP Community: *

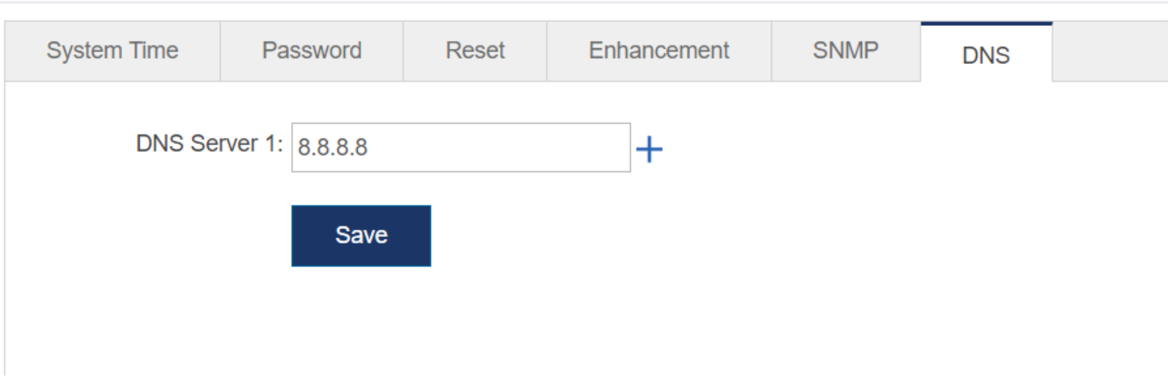
Trap Community: The Trap Community must be the same as the SNMP Community.

Trap Recipient Address: * You can configure up to 9 Trap recipients. Please use ',' or press the Enter key to separate addresses.

Select an SNMP version. The device location, SNMP community, and trap recipient address are mandatory, andother parameters are optional. Click **Save**. The message “Configuration succeeded.” is displayed.

(6) DNS

Figure 1-51 DNS



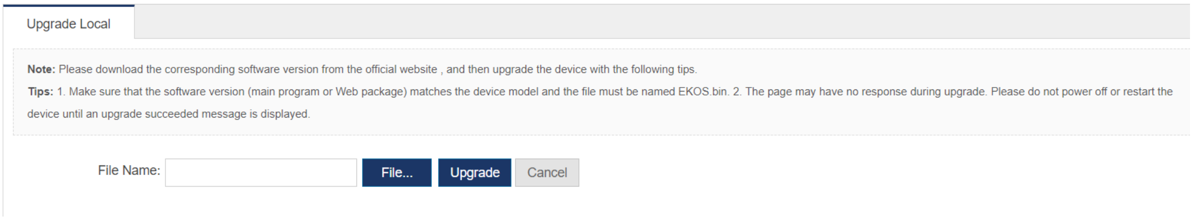
DNS Server 1: 8.8.8.8 +

Enter a DNS server address. Click **Save**. The message “Configuration succeeded.” is displayed.

2. Upgrade

(1) Local Upgrade

Figure 1-52 Upgrade Local



Note: Please download the corresponding software version from the official website , and then upgrade the device with the following tips.

Tips: 1. Make sure that the software version (main program or Web package) matches the device model and the file must be named EKOS.bin. 2. The page may have no response during upgrade. Please do not power off or restart the device until an upgrade succeeded message is displayed.

File Name:

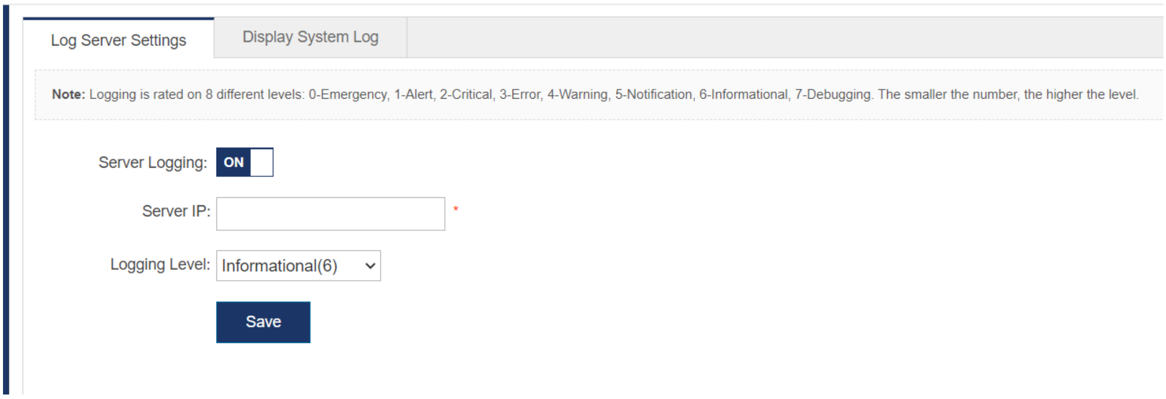
Click **File**, select the locally saved bin file, and then click **Upgrade** to perform local upgrade.

3. System Logging

The **System Logging** page includes **Log Server Settings** and **Display System Log**

(1) Log Server Settings

Figure 1-53 Log Server Settings



Note: Logging is rated on 8 different levels: 0-Emergency, 1-Alert, 2-Critical, 3-Error, 4-Warning, 5-Notification, 6-Informational, 7-Debugging. The smaller the number, the higher the level.

Server Logging: ON

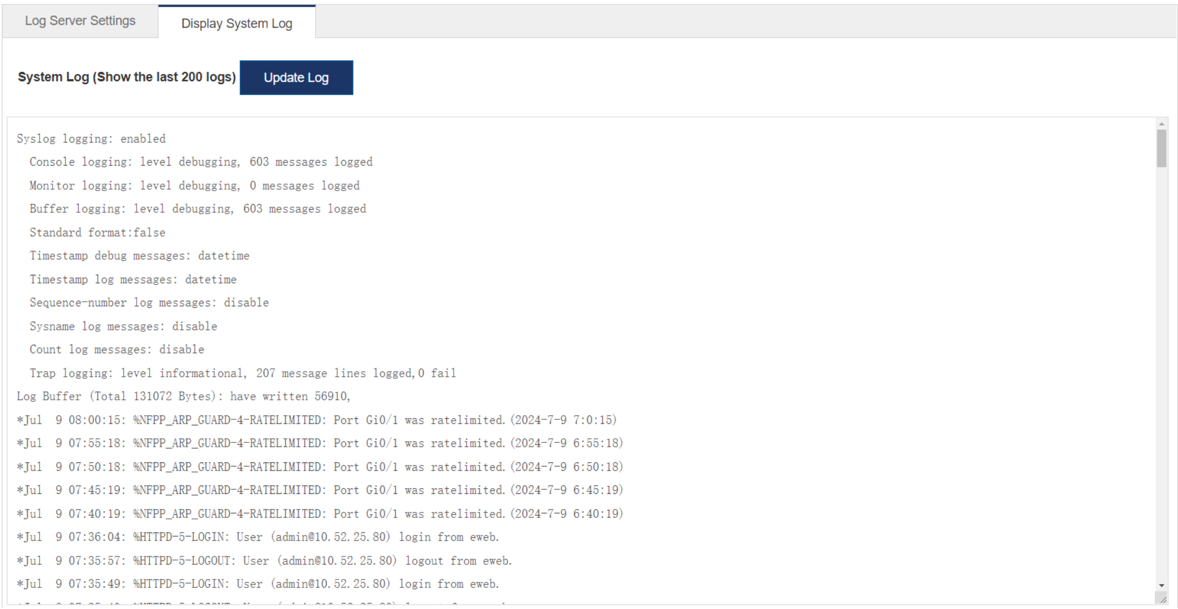
Server IP: *

Logging Level: Informational(6)

Enter a server IP address and select a log severity. Then the device will send system logs to the correspondingserver.

(2) Display System Log

Figure 1-54 Display System Log



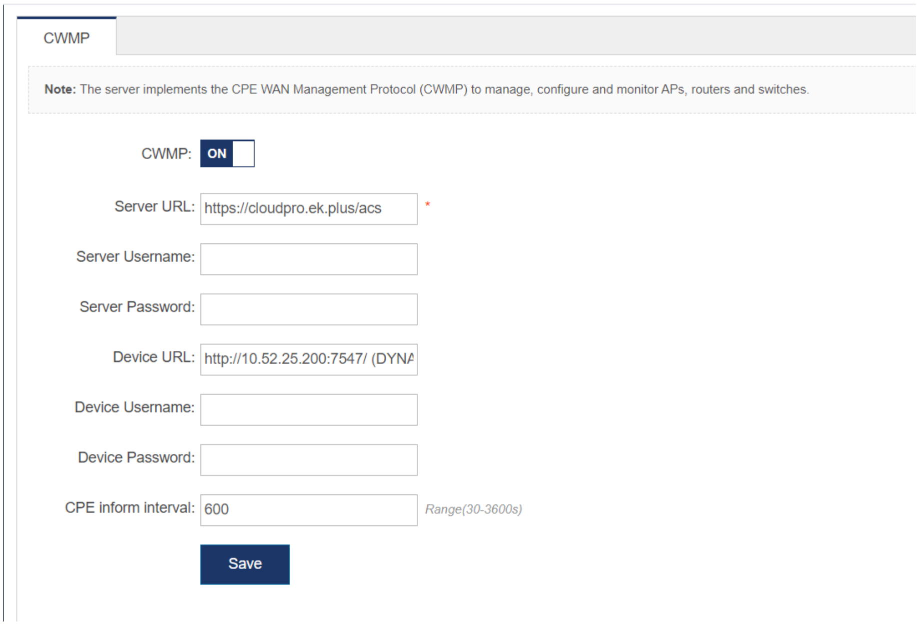
System Log (Show the last 200 logs)

```
Syslog logging: enabled
  Console logging: level debugging, 603 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 603 messages logged
  Standard format:false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: disable
  Sysname log messages: disable
  Count log messages: disable
  Trap logging: level informational, 207 message lines logged,0 fail
Log Buffer (Total 131072 Bytes): have written 56910,
*Jul  9 08:00:15: %NFPP_ARP_GUARD-4-RATELIMITED: Port Gi0/1 was ratelimited.(2024-7-9 7:0:15)
*Jul  9 07:55:18: %NFPP_ARP_GUARD-4-RATELIMITED: Port Gi0/1 was ratelimited.(2024-7-9 6:55:18)
*Jul  9 07:50:18: %NFPP_ARP_GUARD-4-RATELIMITED: Port Gi0/1 was ratelimited.(2024-7-9 6:50:18)
*Jul  9 07:45:19: %NFPP_ARP_GUARD-4-RATELIMITED: Port Gi0/1 was ratelimited.(2024-7-9 6:45:19)
*Jul  9 07:40:19: %NFPP_ARP_GUARD-4-RATELIMITED: Port Gi0/1 was ratelimited.(2024-7-9 6:40:19)
*Jul  9 07:36:04: %HTTPD-5-LOGIN: User (admin@10.52.25.80) login from eweb.
*Jul  9 07:35:57: %HTTPD-5-LOGOUT: User (admin@10.52.25.80) logout from eweb.
*Jul  9 07:35:49: %HTTPD-5-LOGIN: User (admin@10.52.25.80) login from eweb.
```

The text box displays current system logs. Click **Update Log** to update logs.

4. CWMP

The **CWMP** page allows you to view and configure CWMP.



Note: The server implements the CPE WAN Management Protocol (CWMP) to manage, configure and monitor APs, routers and switches.

CWMP:	ON
Server URL:	https://cloudpro.ek.plus/acs *
Server Username:	
Server Password:	
Device URL:	http://10.52.25.200:7547/ (DYNA
Device Username:	
Device Password:	
CPE inform interval:	600 *Range(30-3600s)*

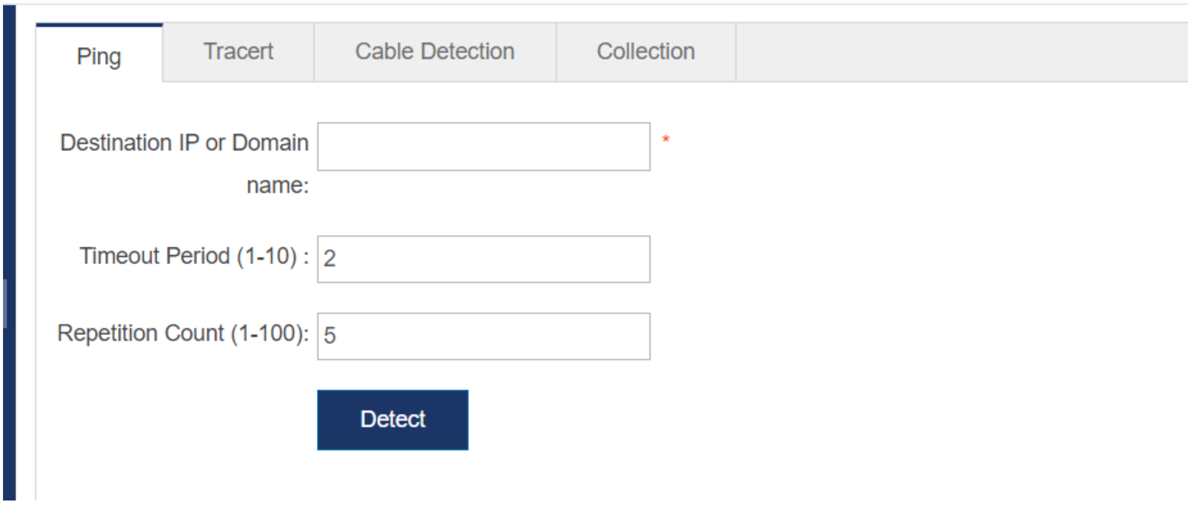
Enable or disable CWMP. You can configure the server URL, server name, server password, device URL, device name, device password, and device connection interval.

5. Detection

The **Detection** page includes **Ping**, **Tracert** and **Cable Detection**.

(1) Ping

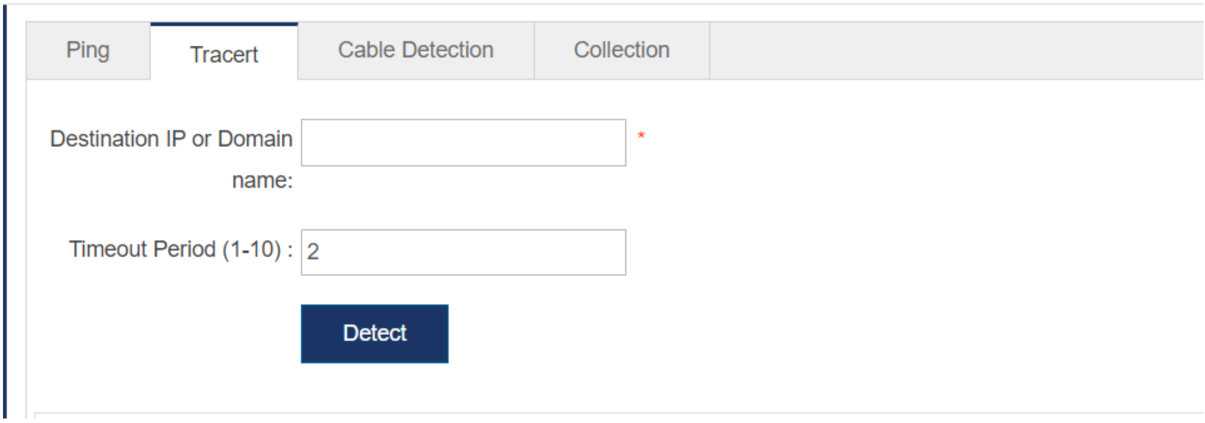
Figure 1-55 Ping



Enter the destination IP and other parameters and click **Detect**. Wait for a few minutes. The text box will displaythe detected results.

(2) Tracert

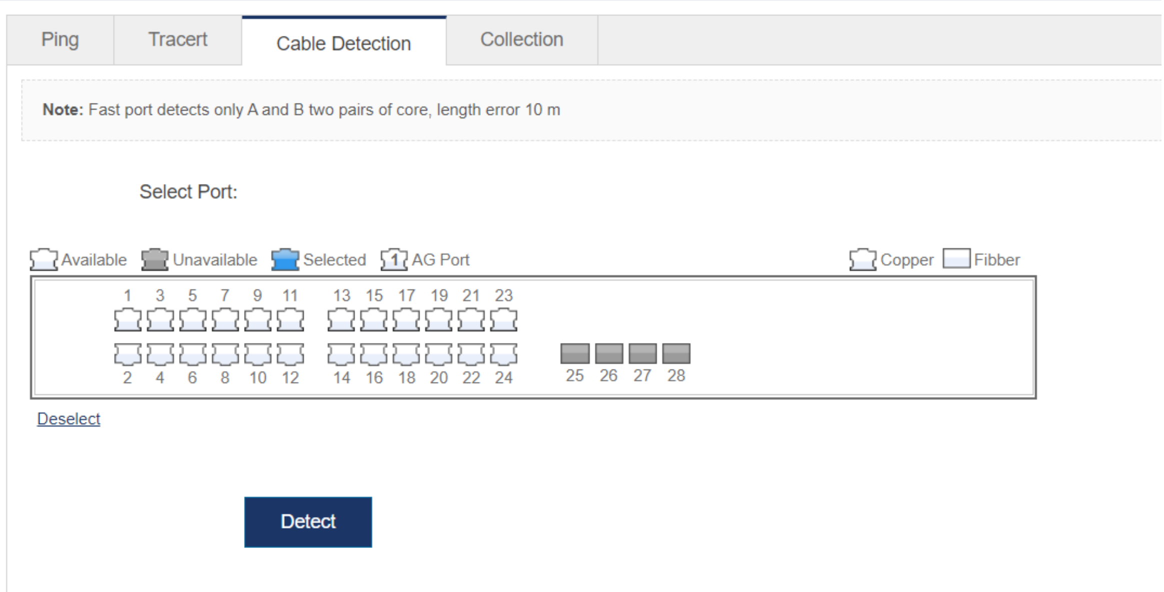
Figure 1-56 Tracert



The steps of tracert test are the same as those of the ping test. Enter the destination IP and other parameters and click **Detect**. Wait for a few minutes. The text box will display the detected results.

(3) Cable Detection

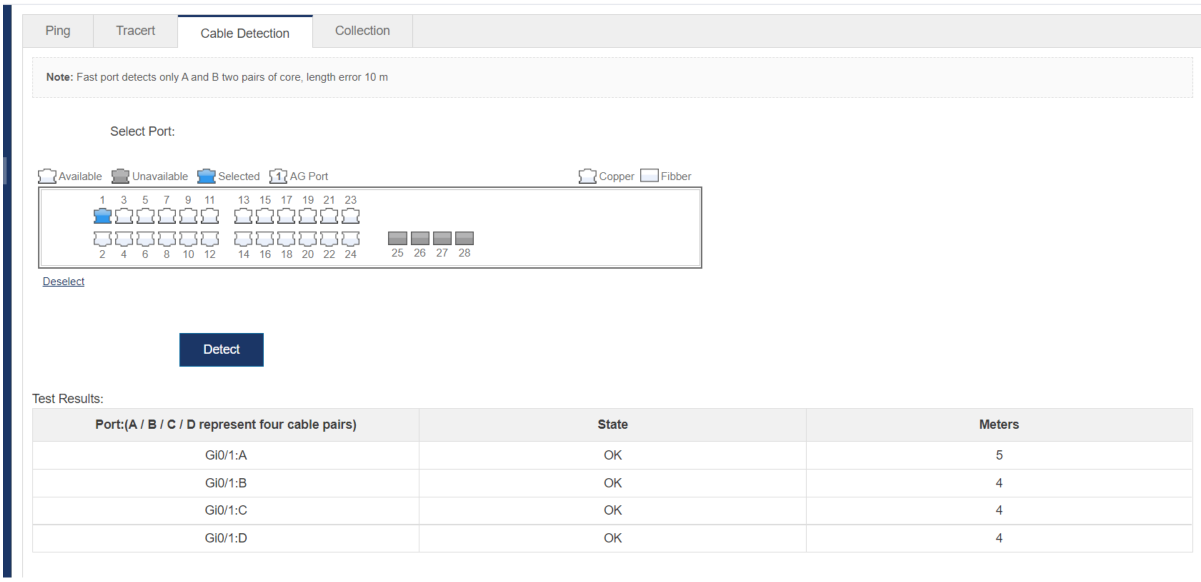
Figure 1-57 Cable Detection



Note: Fast port detects only A and B two pairs of core, length error 10 m

Select a port on the panel and click **Detect**. Wait for a few minutes. Test results will be displayed below **Detect**.

Figure 1-58 Test Results



Note: Fast port detects only A and B two pairs of core, length error 10 m

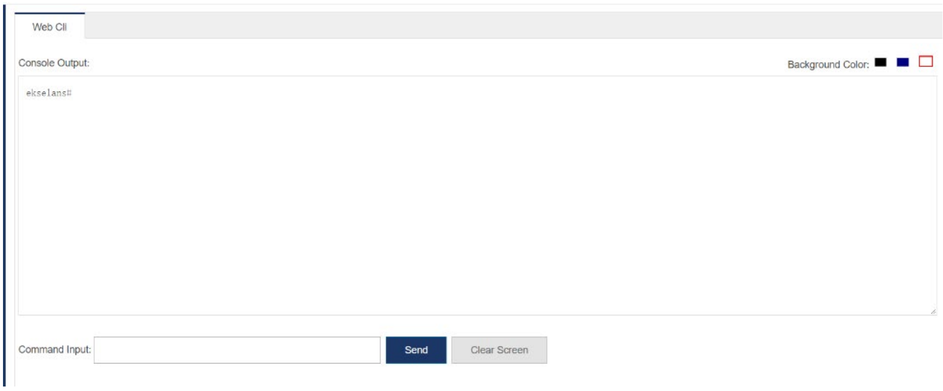
Test Results:

Port:(A / B / C / D represent four cable pairs)	State	Meters
Gi0/1:A	OK	5
Gi0/1:B	OK	4
Gi0/1:C	OK	4
Gi0/1:D	OK	4

6. Web Console

The page stimulates the CLI console. Enter CLI commands in the input box, and press Enter or click **Send** toinput commands. The page supports tab completion and ? command.

Figure 1-59



```
ekselans#
```