V1.0.0

WEB Management PoE Switch

Quick Start Guide

Foreword

This manual introduces the installation, functions and operations of the Web managed switch (hereinafter referred to as "the switch"). Read carefully before using the device, and keep the manual safe for future reference.

Revision Record

V1.0.0
Revision Content: First release.
Release Time: May 2025.

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as ID and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the device, hazard prevention, and prevention of property damage. Read carefully before using the device, and comply with the guidelines when using it.

Transportation Requirements

⚠

Transport the device under allowed humidity and temperature conditions.

Storage Requirements

⚠

Store the device under allowed humidity and temperature conditions.

Installation Requirements

⚠ WARNING

- Do not connect the power adapter to the device while the adapter is powered on.
- Strictly comply with the local electrical safety code and standards. Make sure that the ambient voltage is stable and meets the power supply requirements of the device.
- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.

⚠

- Do not place the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.
- Put the device in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the device label.
- Do not connect the device to two or more kinds of power supplies, to avoid damage to the device.
- The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.
- The device must be grounded by a copper wire with a cross-sectional area of 2.5 mm^{2}and a ground resistance no more than 4 Ω.
- Voltage stabilizer and lightning surge protector are optional depending on the actual power supply on site and the ambient environment.
- To ensure heat dissipation, the gap between the device and the surrounding area should not be less than 10 cm on the sides and 10 cm on top of the device.
- When installing the device, make sure that the power plug and appliance coupler can be easily reached to cut off power.

Operation Requirements

⚠ WARNING

- Do not disassemble the device without professional instruction.
- Operate the device within the rated range of power input and output.
- Make sure that the power supply is correct before use.
- Make sure the device is powered off before disassembling wires to avoid personal injury.
- Do not unplug the power cord on the side of the device while the adapter is powered on.

⚠

- Use the device under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the device, and make sure that there is no object filled with liquid on the device to prevent liquid from flowing into it.
- Operating temperature: –10 °C to +55 °C (+14 °F to +131 °F).
- This is a class A product. In a domestic environment this may cause radio interference in which case you may be required to take adequate measures.
- Do not block the ventilator of the device with objects, such as a newspaper, table cloth or curtain.
- Do not place an open flame on the device, such as a lit candle.

Maintenance Requirements

⚠ WARNING

- Power off the device before maintenance.
- Mark key components on the maintenance circuit diagram with warning signs.

Contents

1 Overview

1.1 Introduction

Web managed switch is a layer-2 commercial switch. With its long-distance PoE function, it can supply power to devices up to 250 meters away. The 4-port switch has PoE orange port functions with the PoE power supply as high as 60 W, the 8-port and 16/24-port switch has PoE red port functions with the PoE power supply as high as 90 W. With a full-metal design, the switch has great heat dissipation capabilities on its shell surface, and is able to work in environments that range from –10 °C to +55 °C (+14 °F to +131 °F).

In addition, the network topology diagram function can be used to quickly locate the problem. The switch is applicable for uses in different scenarios, including homes, factories and offices.

1.2 Features

- 10/100 Mbps or 10/100/1000 Mbps PoE Ethernet ports, uplink ports support gigabit optical ports or Ethernet ports.
- The gray ports conform with IEEE802.3af and IEEE802.3at standards, the orange ports conform with Hi-PoE standard and the red ports conform with IEEE802.3bt standards.
- Supports network topology visualization.
- Supports 250 m long-distance power supply.

  In Extend Mode, the transmission distance of the PoE port is up to 250 meters but the transmission rate drops to 10 Mbps. The actual transmission distance might vary due to power consumption of connected devices or the cable type and status.
- Features mobile management by app.
- Supports LLDP (Link Layer Discovery Protocol).
- Supports DHCP (Dynamic Host Configuration Protocol) Client.
- Supports VLAN configuration based on IEEE802.1Q.
- STP/RSTP is supported on select models.
- Manual link aggregation and LACP link aggregation are supported on selected models.
- Desktop mount and rack mount for 16/24-port. Desktop mount and wall mount for 4/8-port.

2 Port and Indicator

2.1 Front Panel

2.1.1 Front Panel (4/8-port)

The following figure uses an 8-port 100 Mbps Web managed switch as an example, and might differ from the actual product.

Figure 2-1 Front panel (4/8-port)

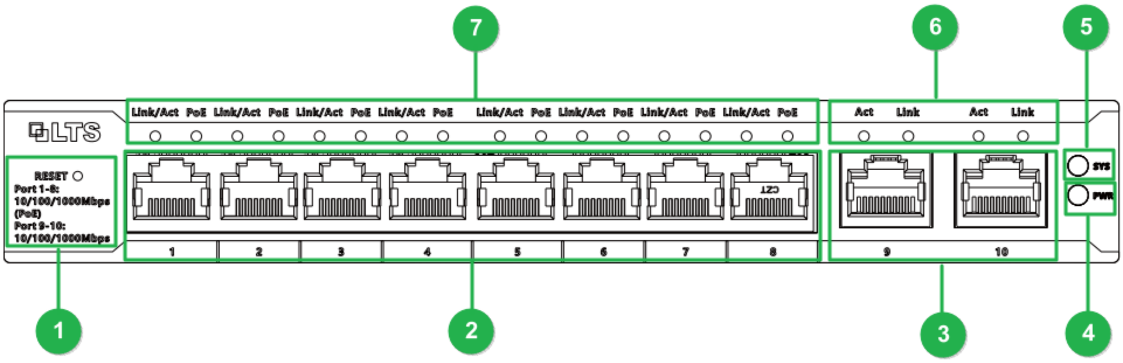

7
6
5
LTS
Link/Act PoE Link/Act PoE Link/Act PoE Link/Act PoE Link/Act PoE Link/Act PoE Link/Act PoE Link/Act PoE
Act Link Act Link
SYS
PWR
RESET
Port 1-8: 10/100/1000Mbps (PoE)
Port 9-10: 10/100/1000Mbps
1 2 3 4 5 6 7 8 9 10
1
2
3
4

Table 2-1 Description of front panel (4/8-port)

No.	Name	Description
1	Reset button	Press and hold it for more than 5 seconds, and release after the panel status indicators all turn on to restore the switch to default settings.
2	PoE ports	4/8 × 10/100 Mbps or 10/100/1000 Mbps self-adaptive PoE Ethernet ports.
3	Uplink ports	10/100/1000 Mbps self-adaptive Ethernet ports. ● The number of the uplink ports might differ from different models. Please refer to the actual product. ● Some models support 1000 Mbps optical ports. Please refer to the actual product.
4	Power indicator	● On: Power on. ● Off: Power off.
5	System status indicator (SYS)	Flashes: The system works normally.
6	Uplink port status indicators	Link indicator. ● On: Connected to device. ● Off: Not connected to device.

No.	Name	Description
		Activity indicator. ● Flashing: Transmitting data. ● Off: Not transmitting data.
7	PoE port status indicators	PoE port status indicator. ● On: Powered by PoE. ● Off: Not powered by PoE.
	Link/Act indicator	Link/Act indicator. ● On: Connected to device. ● Off: Not connected to device. ● Flashing: Transmitting data.

2.1.2 Front Panel (16/24-port)

The following figure uses a 16-port 100 Mbps Web managed switch as an example, and might differ from the actual product.

Figure 2-2 Front panel (16/24-port)

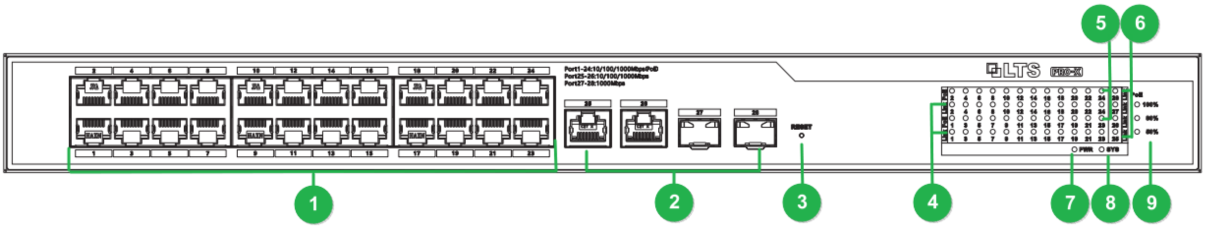


Table 2-2 Description of front panel (16/24-port)

No.	Name	Description
1	PoE ports	16/24 × 10/100 Mbps or 10/100/1000 Mbps self-adaptive Ethernet ports.
2	Uplink ports	10/100/1000 Mbps self-adaptive Ethernet ports and 1000 Mbps optical ports. The uplink ports are combo ports on select models.
3	Reset button	Press and hold it for more than 5 seconds, and release after the panel status indicators all turn on to restore the switch to default settings.
4	Link/Act indicator	● On: Connected to device. ● Off: Not connected to device. ● Flashing: Transmitting data.
5	PoE port status indicators	● On: Powered by PoE. ● Off: Not powered by PoE.
6	Uplink port status (Link) indicators	● On: Connected to device. ● Off: Not connected to device.

No.	Name	Description
7	Power indicator	● On: Power on. ● Off: Power off.
8	System status indicator (SYS)	Flashes: The system works normally.
9	PoE output power indicator	● Only solid green: PoE output power ≤ 50%. ● Solid green and yellow: 50% < PoE output power ≤ 80%. ● Solid green, yellow and red: 80% < PoE output power.

2.2 Rear Panel

2.2.1 Rear Panel (4/8-port)

The figures might differ from different models. Please refer to the actual product.

Figure 2-3 Rear panel (4/8 port)

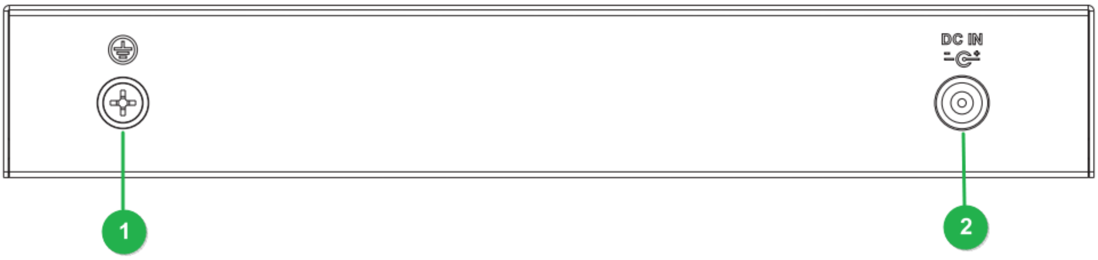


Table 2-3 Description of rear panel (4/8 port)

No.	Name	Description
1	Ground terminal	Connecting GND. ● Normal GND connection of the Switch guarantees device lightning protection and anti-interference. You must connect the GND cable before powering on the Switch and power off the Switch before disconnecting the GND cable. ● The sectional area of the GND cable must be more than 2.5 mm^2, and the GND resistance must to be less than 4 Ω.
2	Power port	Supports 53 VDC or 54 VDC.

2.2.2 Rear Panel (16/24-port)

The figures might differ from different models. Please refer to the actual product.

Figure 2-4 Rear panel (16/24 port)

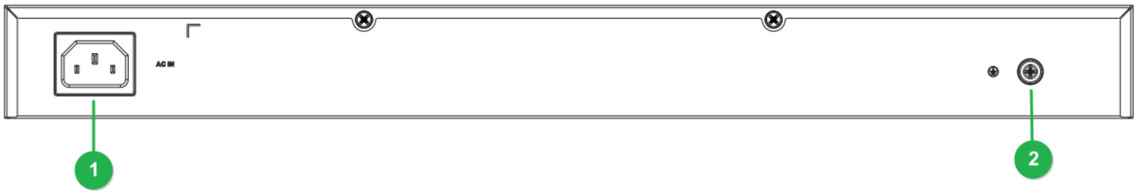


Table 2-4 Description of rear panel (16/24 port)

No.	Name	Description
1	Power port	Supports 100–240 VAC.
2	Ground terminal	Connecting GND. ● Normal GND connection of the Switch guarantees device lightning protection and anti-interference. You must connect the GND cable before powering on the Switch and power off the Switch before disconnecting the GND cable. ● The sectional area of the GND cable must be more than 2.5 mm^2, and the GND resistance must to be less than 4 Ω.

3 Installation

Different installation methods suit for different models. Please select appropriate methods as needed.

3.1 Preparation

- Select an appropriate installation method as needed.
- Install the Switch on a solid and flat surface.
- Leave around 10 cm of open space around the Switch for heat dissipation and to ensure good ventilation.

3.2 Desktop Mount

The Switch supports desktop mount. You can directly place it on a solid and flat desktop.

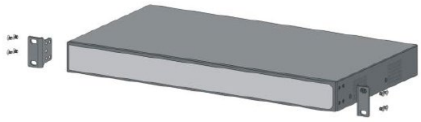
3.3 Rack Mount

The switch supports rack mount.

Procedure

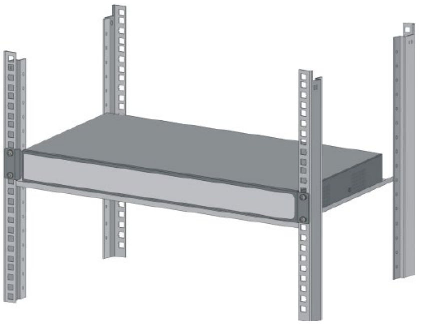
Step 1 Attach the mounting brackets to the switch (one on each side), and fix them with the provided screws.

Figure 3-1 Attach the mounting brackets



Step 2 Fix the switch onto the rack.

Figure 3-2 Fix the switch onto the rack



3.4 Wall Mount

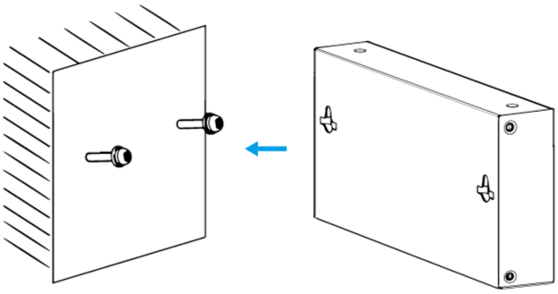
Procedure

Step 1 Drill two M4 screws into the wall, leaving a space of 4 mm between the wall and the head of the screw.

- Screws do not come with the package. Purchase them as needed.
- Make sure that the distance between the screws is the distance between the wall-mount holes (77.8 mm for a 4-port switch and 128.4 mm for an 8-port switch).

Step 2 Align the wall-mount holes on the back cover of the device with the screws, and hang the device on the screws.

Figure 3-3 Wall mount



4 Wiring

4.1 Connecting GND

Normal GND connection of the device is the important guarantee for device lightning protection and anti-interference.

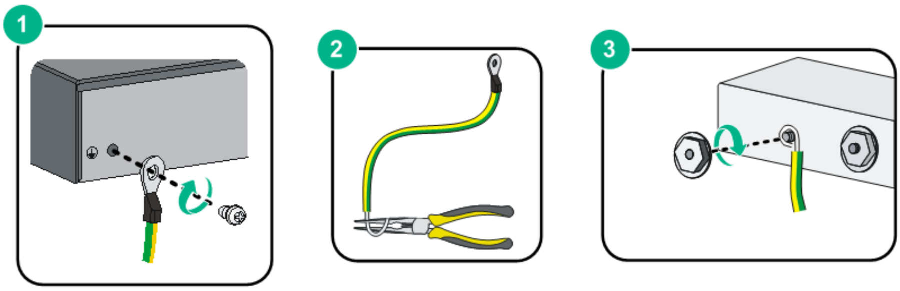
Procedure

Step 1 Remove the ground screw on the device and place it properly. Pass the ground screw through the round hole of the OT terminal of the ground cable. Turn the ground screw clockwise with a cross screwdriver to fasten the OT terminal of the ground cable.

Step 2 Wind the other end of the ground cable into a circle with needle-nose pliers.

Step 3 Connect the other end of the ground cable to the ground bar, turn the hex nut clockwise with a wrench to fasten the other end of the ground cable to the ground terminal.

Figure 4-1 Connect GND



4.2 Connecting Power Cord

Prerequisites

Before connecting the power cord, make sure that the device is reliably grounded.

Procedure

Step 1 Connect one end of the power cord into the power jack of the device accurately.

Step 2 Connect the other end of the power cord to the external power socket.

4.3 Connecting Ethernet Port

Ethernet port adopts standard RJ-45 port. With self-adaptation function, it can be automatically configured to full duplex/half-duplex operation mode. It supports MDI/MDI-X self-recognition of the cable, therefore, you can use cross-over cable or straight-through cable to connect terminal device to network device.

Figure 4-2 Ethernet port pin number

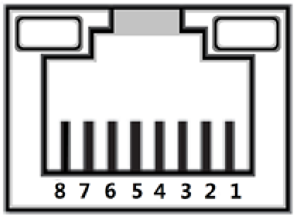
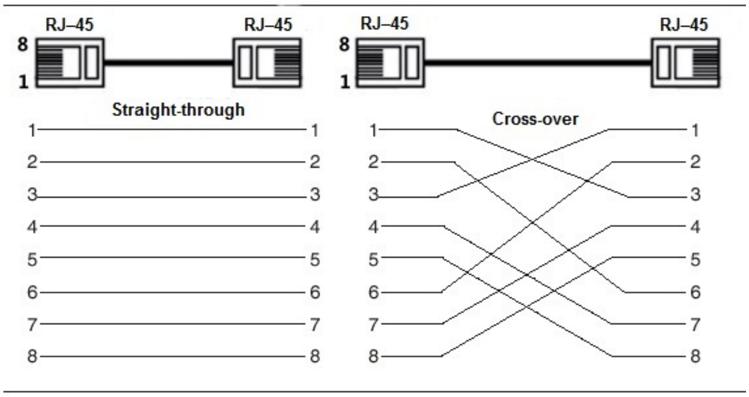


Figure 4-3 Pin description



The cable connection of RJ-45 connector conforms to the standard 568B (1-orange white, 2-orange, 3-green white, 4-blue, 5-blue white, 6-green, 7-brown white, 8-brown).

4.4 Connecting SFP Ethernet Port

Background Information

⚠ **WARNING**

- When installing the SFP optical module, do not touch the gold finger of the SFP optical module.
- Do not remove the dust plug of the SFP optical module before connecting the optical fiber.
- Do not directly insert the SFP optical module into the slot while the optical fiber is inserted in it. Unplug the optical fiber before installing it.

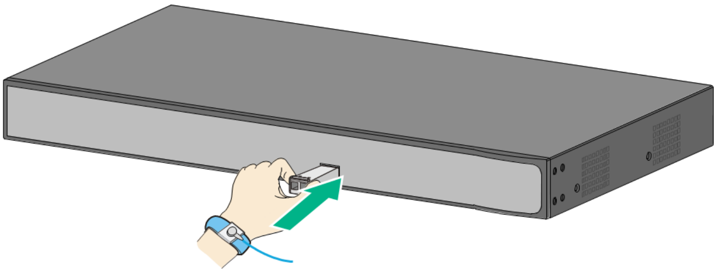
Procedure

Step 1 Wear the antistatic wrist band, and confirm that the antistatic wrist band is in good contact with your skin and the Device is reliably grounded.

Step 2 Turn up the handle of the SFP optical module vertically and hold the optical module on both sides with your hands.

Step 3 Push the optical module gently into the slot in the horizontal direction until the SFP optical module is firmly connected to the slot.

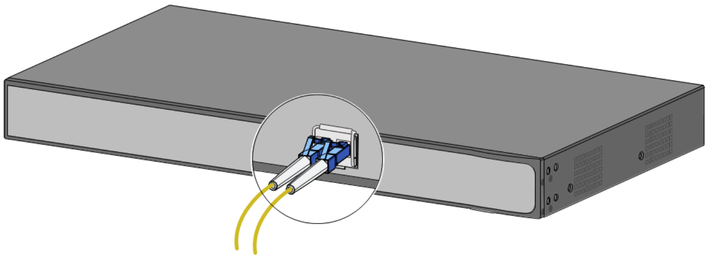
Figure 4-4 Install SFP module



Step 4 Remove the dust cap of the LC connector of the optical fiber and the dust plug of the SFP optical module.

Step 5 Connect the LC connector of the optical fiber to the SFP optical module.

Figure 4-5 Connect optical fiber



4.5 Connecting PoE Ethernet Port

You can directly connect the device PoE Ethernet port to the switch PoE Ethernet port through network cable to achieve synchronized network connection and power supply. With Extend Mode disabled, the maximum distance between the switch and the device is about 100 m.

⚠

When connecting to a non-PoE device, the device needs to be used with an isolated power supply.

5 Initializing the Switch

You can log in to the webpage to initialize the device, or using the X portal application to active the PoE switch.

🕮

- Device initialization is required for first-time use or after the switch has been reset.
- DHCP Client is enabled by default. If no IP address is assigned, the default IP address can be used. (See from the device label, usually 192.168.1.110.)
- Device initialization is available only when the switch and the computer are on the same network segment.
- Plan the network segment properly to connect the switch to the network.
- Different models support different methods of local initialization. For details, see from the technical specifications.

Appendix 1 Cybersecurity Recommendations

Compulsory measures to ensure the basic device network security:

- Timely Update Firmware and Client Software
  - ◇ Keep the device (such as video recorder and IP camera) firmware up-to-date based on standard procedure in the tech-industry to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
  - ◇ Download and use the latest version of client software.
- Use Complex Passwords with Combination of Characters, Numbers and SymbolsPlease refer to the following suggestions to set passwords:
  - ◇ The length should not be less than 8 characters;
  - ◇ Combine at least two types of characters in a password among upper and lower case letters, numbers and symbols;
  - ◇ Do not contain the account name or the account name in reverse order;
  - ◇ Do not use continuous characters, such as abcdefgh and 12345678;
  - ◇ Do not use overlapped characters, such as aaaaaaaa and 11111111.

Constructive suggestions on improving device network security:

- Change Passwords Regularly

  We recommend that you change passwords regularly to reduce the risk of being guessed or cracked.
- Configure and Update Password Reset Information in Time

  Password reset function is supported by the device. Please configure related information for password reset in time, including the end user's email address and password protection questions. Please update the information accordingly in time if it changes. Please do not use simple questions whose answers can be easily obtained when setting password protection questions.
- Enable Account Lock

  The account lock is enabled by default. We recommend you keep it on to ensure the account security. A number of failed login attempts will lead the corresponding account and the source IP address to be locked.
- Physical Protection

  Physical protection is recommended on the device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement strict access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware and unauthorized connection of removable device (for example, USB flash drive and serial port).
- Reset Default HTTP and Other Service Ports

  Changing the default HTTP and other service ports is recommended. We recommend you change them into any set of numbers between 1024–65535 to reduce the risk of exposing ports in use to outsiders.
- Enable HTTPS

  HTTPS is recommended to be enabled so that you can obtain the web service through a secure communication channel.
- Bind IP and MAC Address to Device

To reduce the risk of ARP spoofing, we recommend you bind the IP and MAC address of the gateway to the device.

- Assign Accounts and Privileges Reasonably

  Based on business requirements and management requirements, prudently add user accounts and assign a minimum set of permissions to them.
- Disable Unnecessary Services and Apply Secure Modes

  If not needed, we recommend you turn off some services such as SNMP, SMTP, and UPnP to reduce risks.

  If necessary, we recommend using security modes, including but not limited to the following services:
  - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
  - SMTP: Choose TLS to access mailbox server.
  - FTP: Choose SFTP, and set up strong passwords.
  - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.
- Audio and Video Encrypted Transmission

  To reduce the risk of losing data during transmission, encrypted transmission is recommended for very important and sensitive audio and video data.

  *Reminder: Encrypted transmission might decrease the transmission efficiency.
- Establish a Secure Network Environment

  The following actions are highly recommended to ensure device security and to reduce potential cyber risks:
  - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
  - Partition and isolate the network according to the actual network needs. If there are no communication requirements between two sub networks, we recommend you adopt network isolation through VLAN, network GAP and other technologies.
  - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
  - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.
- Security Auditing
  - Check online users: Check online users regularly to prevent unauthorized login.
  - Check device log: Obtain the IP addresses that were used to log in to the device and their key operations with help of the logs.
- Network Log

  The stored log is not saved in full due to the limited storage capacity. If you need to save the log for a long time, we recommend you enable the network log function to make sure that the critical logs are synchronized to the network log server for tracing.