Ethernet Switch (16/24-port Unmanaged Desktop Switch)

Quick Start Guide

V1.0.0

Foreword

General

This manual mainly introduces the hardware, installation, and wiring steps of the 16/24-port unmanaged desktop switch (hereinafter referred to as "the device").

Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

Signal Words	Meaning
DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
TIPS	Provides methods to help you solve a problem or save you time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	March 2023

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, 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.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- 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

- 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.
- 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.
- Operating temperature range: -20 ℃ to +60 ℃ (-4 °F to +140 °F).

Maintenance Requirements

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

Table of Contents

1 Overview

1.1 Introduction

The device is a layer-2 commercial switch. It provides a high-performance switching engine and large buffer memory to ensure smooth video stream transmission. With a full-metal design, the device has great heat dissipation capabilities on its shell surface, and is able to work in environments that range from –20 °C to +60 °C (–4 °F to +140 °F). With the Mode button, it provides a variety of working modes for different scenarios.

The device is applicable for use in different scenarios, including homes, offices, small malls and on server farms.

1.2 Features

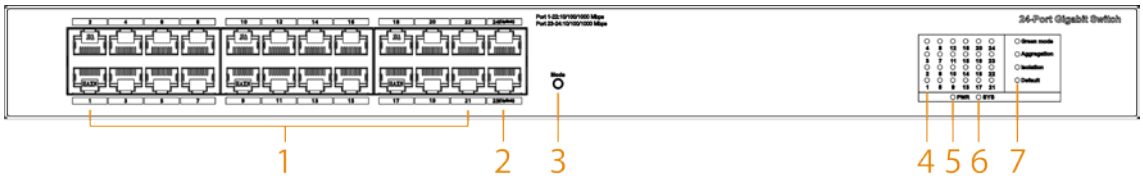
- 16/24 × 10/100 Mbps or 10/100/1000 Mbps Ethernet ports.
- Port isolation is supported by select models, which can be enabled by the Mode button.
- Aggregation uplink is supported by select models, which can be enabled by the Mode button.
- EEE function is supported by select models, which can be enabled by the Mode button.
- Desktop mount and rack mount.

2 Port and Indicator

2.1 Front Panel

The following figure is for reference only, and might differ from the actual product.

Figure 2-1 Front panel



Following are all the ports and indicators on the front panel of the 16/24-port unmanaged desktop switch. The actual device might only have some of these ports and indicators.

Table 2-1 Description of front panel

No.	Description
1	10/100 Mbps or 10/100/1000 Mbps self-adaptive Ethernet ports.
2	Uplink port, including 10/100/1000 Mbps self-adaptive Ethernet port.
3	Working mode button. You can switch from the following four modes through the button. ● Default: This mode is enabled by default. ● Isolation: When this mode is enabled, the downlink ports are independent, the flow is not interoperable, and the downlink port and uplink port can communicate with each other. ● Aggregation: When this mode is enabled, the uplink ports are aggregated into one group, which improves port rate and provides redundancy backup. ● Green mode: When this mode is enabled, the EEE function is enabled. The device can automatically shut down the idle circuit, reduce the power consumption and save energy. This is only available on select models.
4	Single-port connection status indicator (Link/Act). ● On: Connected to device. ● Off: Not connected to device.
5	Power indicator. ● On: Power on. ● Off: Power off.
6	System status (SYS). ● Flashing quickly: The device is booting up. ● Flashing slowly: The device is working properly.

No.	Description
7	Working mode indicator. Available on select models. ● Solid green: This working mode is enabled, including Default, Isolation, Aggregation, and green mode. ● Off: This working mode is not enabled.

2.2 Rear Panel

The following figure is for reference only, and might differ from the actual product.

Figure 2-2 Rear panel

Table 2-2 Rear panel description

No.	Description
1	Power port, supports 100–240 VAC.
2	Ground terminal.

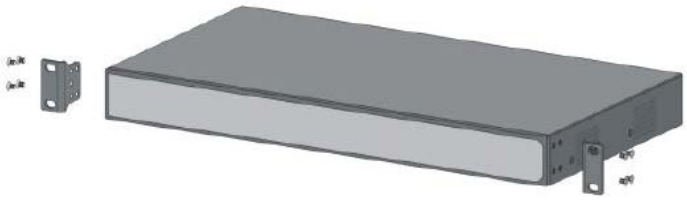
3 Installation

The device supports rack mount.

Procedure

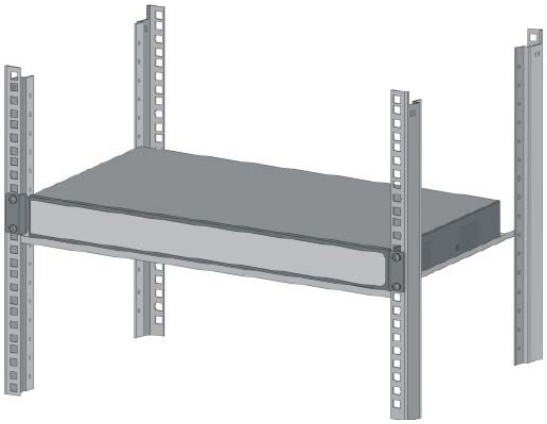
Step 1 Attach the mounting bracket to the device side panel (one on each side) and secure it with the screws provided with the rack.

Figure 3-1 Install bracket



Step 2 Attach the device to the rack with screws.

Figure 3-2 Install bracket



4 Wiring

4.1 Connecting GND

Background Information

Normal GND connection of the device is the important guarantee for device lightning protection and anti-interference. The steps for connecting the GND are as follows:

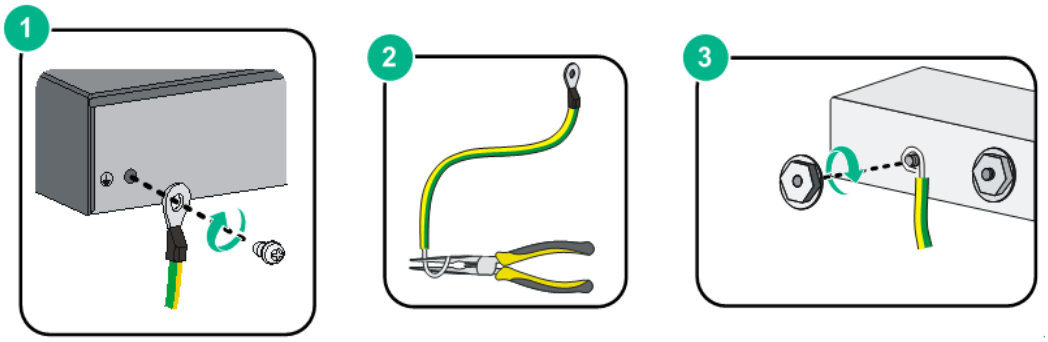
Procedure

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

Background Information

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

Procedure

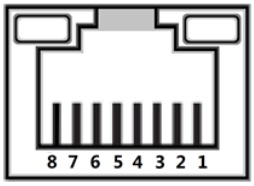
Step 1 Connect one end of the power cord into the power jack of the device.

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

4.3 Connecting Ethernet Port

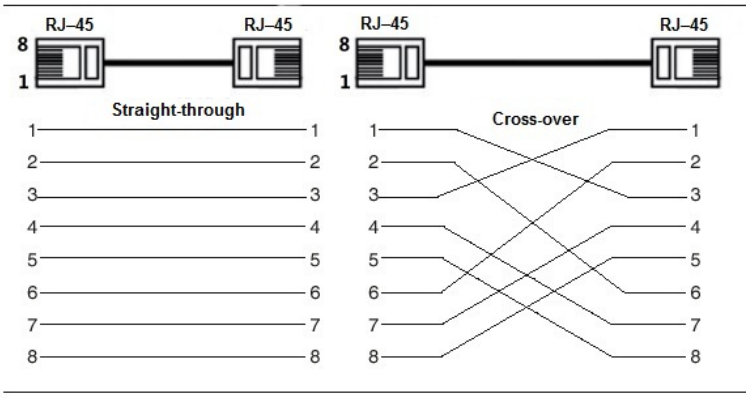
Ethernet port adopts standard RJ-45 port. With self-adaptation function, it can be automatically configured to full duplex/half-duplex operation mode. It supports MDI/MDI-X self-recognition of the cable, therefore, you can use cross-over cable or straight-through cable to connect terminal device to network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

Figure 4-2 Ethernet port pin number



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).

Figure 4-3 Connect cable



4.4 Connecting SFP Ethernet Port

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 port.
- Do not directly insert the SFP optical module with the optical fiber inserted into the slot. Unplug the optical fiber before installing it.

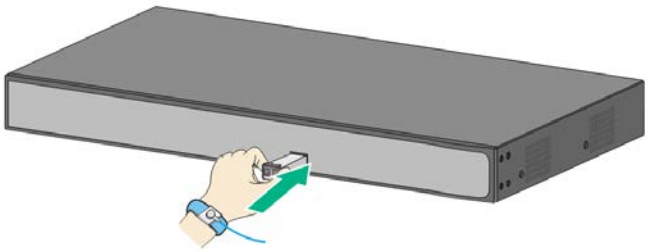
Procedure

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.

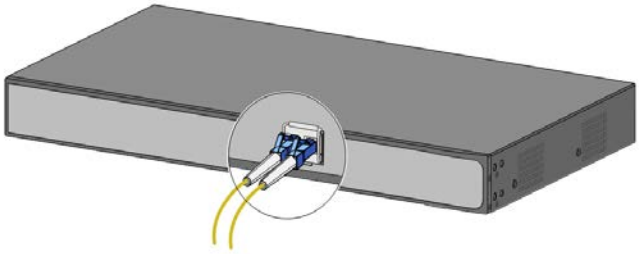
Figure 4-4 Install SFP module



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



Appendix 1 Cybersecurity Recommendations

Mandatory actions to be taken for basic device network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters.
   - Include at least two types of characters; character types include 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 123, abc, etc.
   - Do not use overlapped characters, such as 111, aaa, etc.

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date 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.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. **Physical Protection**

   We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between 1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing

the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

   If necessary, it is highly recommended that you use safe 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.

10. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

    Due to the limited storage capacity of the device, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

13. **Construct a Safe Network Environment**

    In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - 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.