

16/24-port Unmanaged Desktop Switch

Quick Start Guide



Foreword

General

This manual introduces the installation, functions and operations of the 16/24-port unmanaged desktop switch (hereinafter referred to as "the Switch"). Read carefully before using the device, and keep the manual safe for future reference.

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
V1.0.1	Updated long distance description.	August 2023
V1.0.0	First release.	April 2022

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related jurisdictions. For detailed information, refer to the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. 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 the company names in the manual are the properties

of their respective owners.

- Please visit our website, contact the supplier or customer service if there is any problem occurring when 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



- 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 mm² 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.
- Operating temperature: -10°C (14°F) to $+55^{\circ}\text{C}$ (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



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

Table of Contents

- ForewordI
- Important Safeguards and Warnings..... III
- 1 Overview 1
 - 1.1 Introduction 1
 - 1.2 Features..... 1
- 2 Port and Indicator 2
 - 2.1 Front Panel..... 2
 - 2.2 Rear Panel..... 3
- 3 Installation 4
- 4 Wiring 5
 - 4.1 Connecting GND..... 5
 - 4.2 Connecting Power Cord..... 5
 - 4.3 Connecting Ethernet Port..... 5
 - 4.4 Connecting PoE Ethernet Port 6
- Appendix 1 Cybersecurity Recommendations 7

1 Overview

1.1 Introduction

The Switch 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 Switch has great heat dissipation capabilities on its shell surface, and is able to work in environments that range from -10°C to $+55^{\circ}\text{C}$ ($+14^{\circ}\text{F}$ to $+131^{\circ}\text{F}$). With its DIP design, it provides a variety of work modes that suit different scenarios. The Switch also supports power consumption management, which allows it to adapt to fluctuations in the power consumption of terminal devices. This ensures stable operation. The Switch is applicable for use in different scenarios, including homes, offices, small malls and on server farms.

1.2 Features

- 16/24 × 10/100 Mbps PoE Ethernet port.
- All ports meet the requirements of IEEE802.3af and IEEE802.3at standards. The orange ports conform with Hi-PoE standard.
- Desktop PoE Switch series support 250 m long-distance PoE transmissions, which can be enabled by DIP switch.



In Extend Mode, the transmission distance of the PoE port is up to 250 m 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.

- Desktop PoE Switch series support PoE watchdog for real-time detection of terminal device status.
- Power consumption management.
- Desktop mount and rack mount.

No.	Description
7	DIP switch. - PoE Watchdog: When a terminal device crash is detected, power off and restart the terminal device. - Extend Mode: Extends the maximum transmission distance to 250 m, but reduces average transmission speed to 10 Mbps.  In Extend Mode, the transmission distance of the PoE port is up to 250 m 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. - VIP Port: Enable the QoS mode through the DIP switch to achieve priority transmission of corresponding Ethernet ports. - Port Isolation: The port isolation mode can be enabled through the DIP switch. When this function is enabled, the downlink ports are independent, the flow is not interoperable, and the downlink port and uplink port can communicate with each other.  Only available on select models.

2.2 Rear Panel

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

Figure 2-2 Rear panel

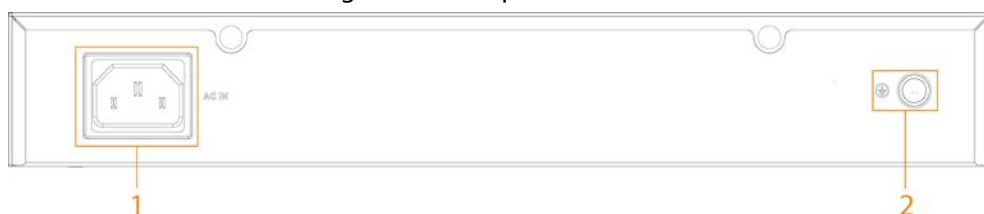


Table 2-2 Description of rear panel

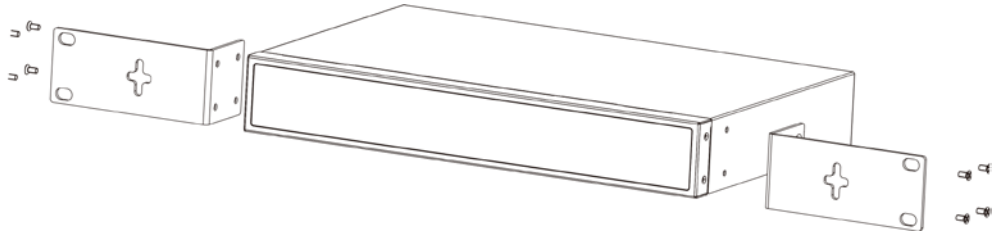
No.	Description
1	Power port, supports 100–240 VAC.
2	Ground terminal.

3 Installation

The Switch supports rack mount.

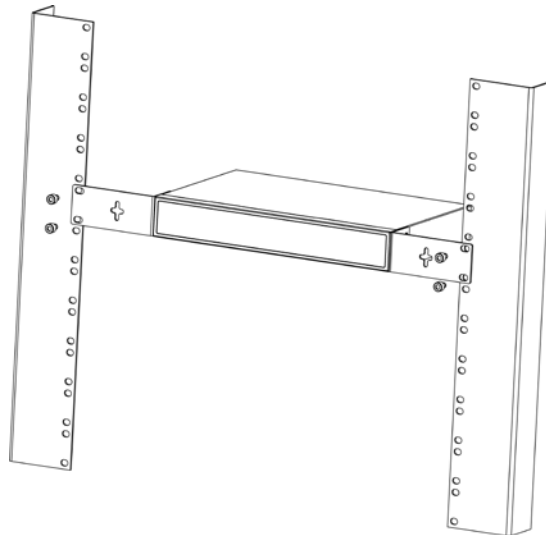
Step 1 Attach the mounting bracket to the Switch side panel (one on each side) and secure it with the screws provided with the rack.

Figure 3-1 Attach the mounting brackets



Step 2 Attach the Switch to the rack with screws.

Figure 3-2 Fix the Switch onto the rack



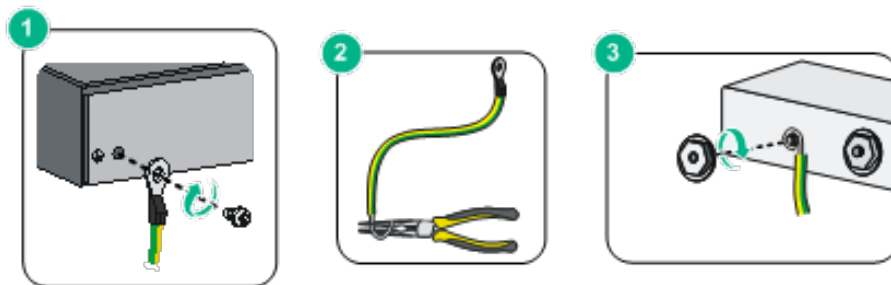
4 Wiring

4.1 Connecting GND

Normal GND connection of the device guarantees device lightning protection and anti-interference.

- Step 1 Remove the ground screw from the device and 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 the needle-nose pliers.
- Step 3 Connect the other end of the ground cable to the ground bar, then 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

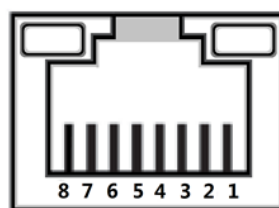
Before connecting the power cord, make sure that the device is securely grounded.

- Step 1 Connect one end of the power cord to 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 is a standard RJ-45 port. With its 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 cables or straight-through cables to connect the terminal device to the network device.

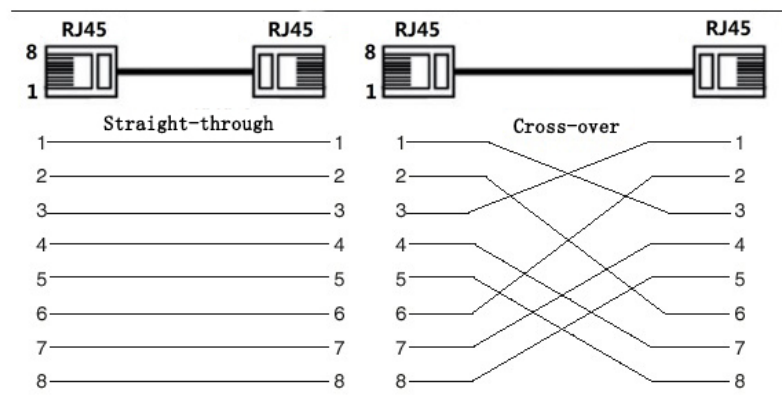
Figure 4-2 Ethernet port pin number



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 PoE Ethernet Port

If the terminal device has a PoE Ethernet port, you can directly connect this port to the switch PoE Ethernet port through the network cable to achieve synchronized network connection and power supply. The maximum distance between the switch and the terminal device is about 100 m.



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

Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

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.