

Ethernet Switch (4&8-Port Unmanaged Desktop Switch)

User's Manual



V1.0.1

Foreword

General

This manual introduces the installation, functions and operations of the 4&8 port unmanaged 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 signal words 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, reductions in performance, or unpredictable results.
 TIPS	Provides methods to help you solve a problem or save time.
 NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.1	Content Improvement.	October 2024
V1.0.0	First release.	October 2024

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 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 to $+55^{\circ}\text{C}$ ($+14^{\circ}\text{F}$ to $+131^{\circ}\text{F}$).
- 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

Foreword.....	I
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.....	5
3.1 Preparation.....	5
3.2 Desktop Mount.....	5
3.3 Wall Mount.....	5
4 Wiring.....	6
4.1 Connecting GND Cable.....	6
4.2 Connecting Power Cord.....	6
4.3 Connecting Ethernet Port.....	6
4.4 Connecting PoE Port.....	7
Appendix 1 Security Recommendation.....	8

1 Overview

1.1 Introduction

The Switch is a layer-2 commercial switch. It has a high-performance switching engine and a large buffer memory to ensure smooth video stream transmission. With a full-metal and fanless design, the Switch features great heat dissipation capability on the 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 can provide a variety of working modes for different scenarios.

The Switch is applicable for use in a variety of scenarios, such as in the home and office, on server farms, and in small malls.

1.2 Features

- $4/8 \times 100/1000$ Mbps Ethernet port.
- Uplink ports include electrical port.
- All PoE ports support IEEE802.3af and IEEE802.3at.
- 250 m long-distance PoE transmission, which can be enabled by DIP switch. (Available on certain models.)



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.

- Fanless.
- Supports desktop mount and wall mount.

2 Port and Indicator

2.1 Front Panel

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

Front panel (4 PoE ports)

Figure 2-1 Front panel (4 PoE ports)

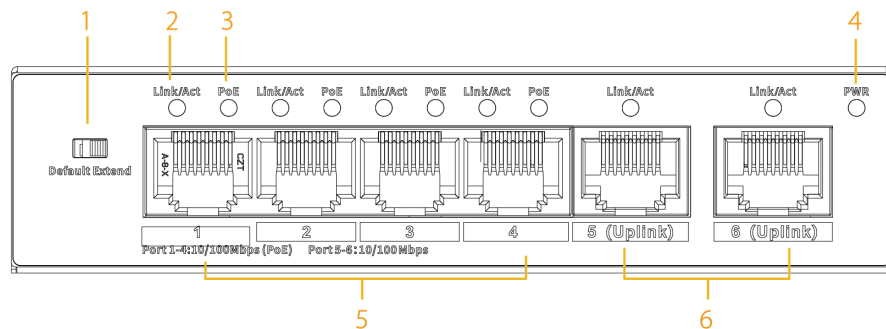


Table 2-1 Port description

No.	Description
1	Extend Mode: Extends the maximum transmission distance to 250 m, but reduces average transmission speed to 10 Mbps.  The actual transmission distance might vary due to power consumption of connected devices or the cable type and status.
2	Single-port connection or data transmission status indicator (Link/Act). ● On: Connected to the device. ● Off: Not connected to device. ● Flashes: Data transmission is in progress.
3	PoE port status indicator. ● On: Powered by PoE. ● Off: Not powered by PoE.
4	Power indicator. ● On: Power on. ● Off: Power off.
5	10/100 Mbps self-adaptive Ethernet ports.
6	10/100 Mbps self-adaptive uplink ports.

Front panel (8 PoE ports)

Figure 2-2 Front panel (8 PoE ports)

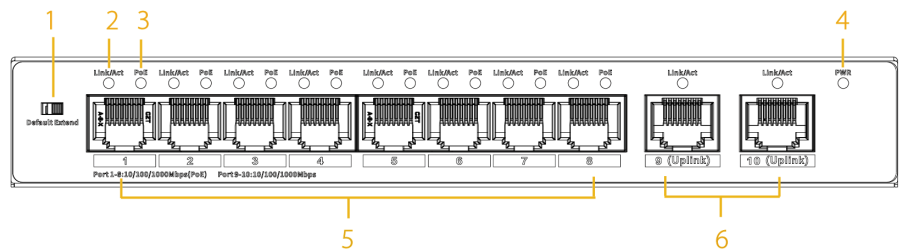


Table 2-2 Port description

No.	Description
1	Extend Mode: Extends the maximum transmission distance to 250 m, but reduces average transmission speed to 10 Mbps.  The actual transmission distance might vary due to power consumption of connected devices or the cable type and status.
2	Single-port connection or data transmission status indicator (Link/Act). ● On: Connected to the device. ● Off: Not connected to device. ● Flashes: Data transmission is in progress.
3	PoE port status indicator. ● On: Powered by PoE. ● Off: Not powered by PoE.
4	Power indicator. ● On: Power on. ● Off: Power off.
5	10/100/1000 Mbps self-adaptive Ethernet ports.
6	10/100/1000 Mbps self-adaptive uplink ports.

2.2 Rear Panel

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

Rear panel (4 PoE ports)

Figure 2-3 Rear panel (4 PoE ports)



Table 2-3 Port description

No.	Description
1	Ground terminal.  Available for certain models.
2	Power port, supports 48-57 VDC.

Rear panel (8 PoE ports)

Figure 2-4 Rear panel (8 PoE ports)

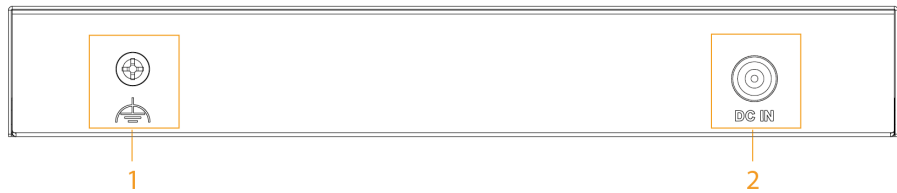


Table 2-4 Port description

No.	Description
1	Ground terminal.  Available for certain models.
2	Power port, supports 48-57 VDC.

3 Installation

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 Wall Mount

Procedure

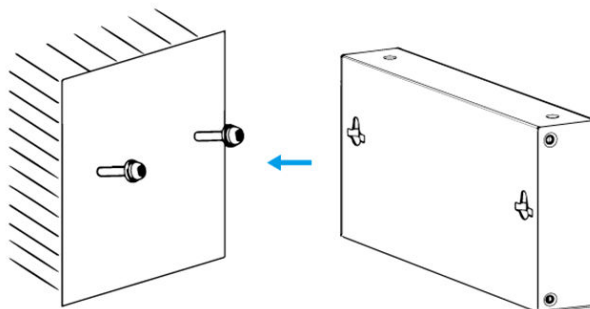
- Step 1 Drill two M4 screws into the wall. The distance between the screws needs to match that of the wall-mount holes of the Switch.



- Screws do not come with the package. Purchase them as needed.
- Make sure that the distance between the screws is the same as the distance between the wall-mount holes (the distance of the 4-port unmanaged desktop switch is 74.7 mm (2.94 inches) and the distance of the 8-port unmanaged desktop switch is 104.2 mm (4.1 inches)).
- Leave a space of at least 4 mm between the wall and the head of the screws.

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

Figure 3-1 Wall mount



4 Wiring

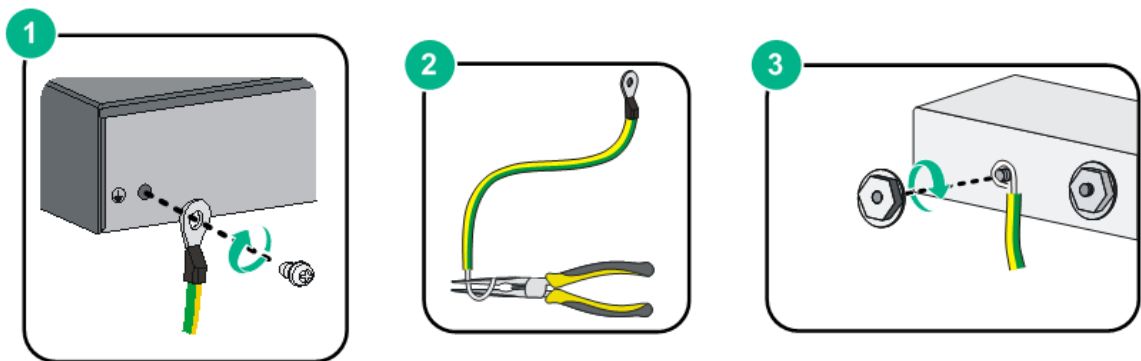
4.1 Connecting GND Cable

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

Background Information

Make sure that the Switch is reliably grounded before connecting the power cord.

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

The 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, allowing you to use a cross-over cable or straight-through cable to connect the terminal device to the network device.

Figure 4-2 Ethernet port pin number

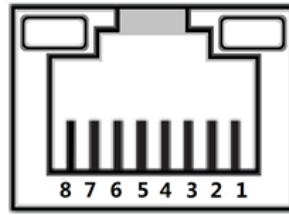
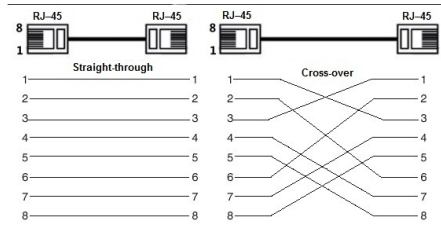


Figure 4-3 Pin description



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

4.4 Connecting PoE 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.

Appendix 1 Security Recommendation

Account Management

1. Use complex 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: 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 repeating characters, such as 111, aaa, etc.

2. Change passwords periodically

It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

3. Allocate accounts and permissions appropriately

Appropriately add users based on service and management requirements and assign minimum permission sets to users.

4. Enable account logout function

The account logout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.

5. Set and update password reset information in a timely manner

The device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. Enable HTTPS

It is recommended that you enable HTTPS to access web services through secure channels.

2. Encrypted transmission of audio and video

If your audio and video data contents are very important or sensitive, it is recommended to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.

3. Turn off non-essential services and use safe mode

If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

If necessary, it is highly recommended to choose safe modes, including but not limited to the following services:

- SNMP: Choose SNMP v3, and set up strong encryption and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up complex passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up complex passwords.

4. Change HTTP and other default service ports

It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. **Enable Allow list**

It is recommended that you turn on the allow list function, and only allow IP in the allow list to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allow list.

2. **MAC address binding**

It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.

3. **Build a secure network environment**

In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
- According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
- Establish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**

It is recommended to check online users regularly to identify illegal users.

2. **Check device log**

By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.

3. **Configure network log**

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

Software Security

1. **Update firmware in time**

According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.

2. **Update client software in time**

It is recommended to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control

and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).