4/8-Port 10/100 Mbps Unmanaged Hardened PoE Switch with 1 Gigabit RJ-45 Port and 1 Gigabit SFP

User's Manual

V1.0.1

Foreword

General

This user's manual (hereinafter referred to be "the manual") introduces the features and structure of 4/8-Port 10/100 Mbps Unmanaged Hardened PoE Switch with 1 Gigabit RJ-45 Port and 1 Gigabit SFP.

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.
NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.1	Updated foreword	November 2020
V1.0.0	First release.	November 2020

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 regions. For detailed information, see 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, please refer to our 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 occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

The manual helps you to use our product properly. To avoid danger and property damage, read the manual carefully before using the product, and we highly recommend you to keep it well for future reference.

Operating Requirements

- Do not expose the device directly to the sunlight, and keep it away from heat.
- Do not install the device in the damp environment, and avoid dust and soot.
- Make sure the device is in horizontal installation, and install the device on solid and flat surface to avoid falling down.
- Avoid liquid spattering on the device. Do not place object full of liquid on the device to avoid liquid flowing into the device.
- Install the device in the well-ventilated environment. Do not block the air vent of the device.
- Use the device at rated input and output voltage.
- Do not dissemble the device without professional instruction.
- Transport, use, and store the device in allowed ranges of humidity and temperature.
- Disconnect the power supply first to avoid personal injury when removing the cable.
- Voltage stabilizer and lightening arrester are optional according to site power supply and surrounding environment.

Power Supply Requirements

- Use the battery properly to avoid fire, explosion, and other dangers.
- Replace the battery with battery of the same type.
- Use locally recommended power cord in the limit of rated specifications.
- Use the standard power adapter. We will assume no responsibility for any problems caused by nonstandard power adapter.
- The power supply shall meet the SELV requirement. Use the power supply that conforms to Limited Power Source, according to IEC60950-1. Refer to the device label.
- Adopt GND protection for I-type device.
- The coupler is the disconnecting apparatus. Keep it at the angle for easy to operate.
- Be sure to ground the device (connect with copper wire whose cross section is not less than 2.5 mm² and resistance to ground is less than or equal to 4Ω).

Battery Caution

- Do not ingest battery to avoid chemical burn hazard.
- This product contains a coin cell battery. If the coin cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
- Keep new and used batteries away from children.
- If the battery compartment does not close securely, stop using the product and keep it away from children.
- If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.
- Risk of explosion if the battery is replaced by an incorrect type.
- Do not throw or immerse into water, heat to more than 100℃（212℉）, repair or disassemble, leave in an extremely low air pressure environment or extremely high-temperature

environment, crush, puncture, cut or incinerate.

- Dispose of the battery as required by local ordinances or regulations.

Table of Contents

1 Product Overview

1.1 Introduction

4/8-Port 10/100 Mbps Unmanaged Hardened PoE Switch with 1 Gigabit RJ-45 Port and 1 Gigabit SFP is a type of layer two commercial switch. It provides 4 or 8 10/100 Mbps Ethernet ports, 1 10/100/1000 Mbps self-adaptive RJ-45 port, and 1 1000 Mbps SFP fiber port.

1.2 Features

General Features

- Layer two hardened PoE switch.
- Supports IEEE802.3, IEEE802.3u, IEEE802.3ab/z and IEEE802.3X standards.
- MAC auto learning, aging, MAC address capacity 8K.
- Supports MDI/MDIX self-adaptation.
- RJ-45 port supports 10/100 Mbps self-adaptation, supports IEEE802.3af and IEEE803.3at power supply standards.
- Adopts metal enclosure.
- Industrial wide working temperature design.
- Supports 48V DC–57V DC power supply and dual power backup.

Individual Features

- 4-Port 10/100 Mbps Unmanaged Hardened PoE Switch: Port 1 supports Hi-PoE 60W power supply.
- 8-Port 10/100 Mbps Unmanaged Hardened PoE Switch: Port 1 and port 2 support BT 90W power supply.
- Supports two transmission modes, including Extend Mode On and Extend Mode Off. Extend Mode Off is a standard Ethernet mode with 100 Mbps transmission bandwidth, and supports a maximum transmission distance of 100 m with six different types of cables. Extend Mode On is a long-distance transmission mode with a transmission bandwidth of 10 Mbps, and supports a maximum transmission distance of 250 m with six different types of cables.

1.3 Typical Application

The typical networking scene is shown as follows.

Figure 1-1 Typical networking scene of 4-Port Switch

Figure 1-2 Typical networking scene of 8-Port Switch

2 Device Structure

2.1 4-Port Unmanaged Hardened PoE Switch

2.1.1 Front Panel

Figure 2-1 Front panel

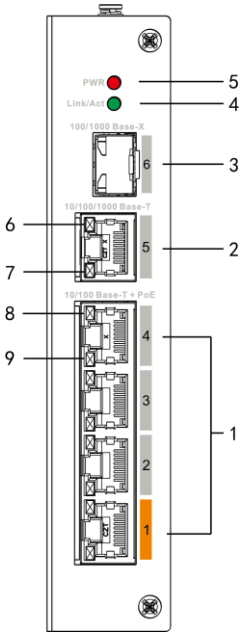


Table 2-1 The description of front panel

No.	Name	Description
1	10/100 Base-T	4 × 10/100 Mbps self-adaptive PoE power supply ports.
2	10/100/1000 Base-T	10/100/1000 Mbps self-adaptive RJ-45 port.
3	100/1000 Base-X	100/1000 Mbps self-adaptive SFP fiber port.
4	Link/Act	Fiber port status indicator light.
5	PWR	Power indicator light, and it is also the PoE power supply status indicator light.
6	Link indicator light	When linking up, the indicator light is solid on.
7	Act indicator light	When the data passing the switch, the indicator light flashes.
8	PoE indicator light	PoE power supply status indicator light.
9	Link/Act indicator light	Ethernet port status indicator light.

2.1.2 Upper Cover

Figure 2-2 Upper cover

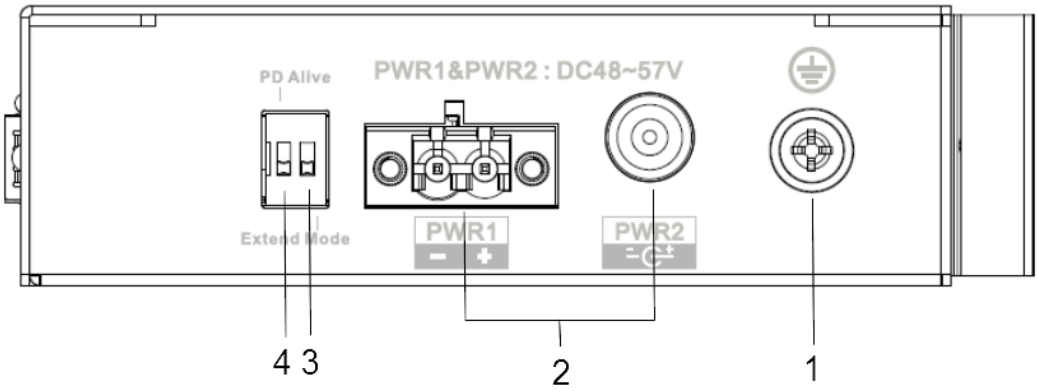


Table 2-2 The description of upper cover

No.	Name	Description
1	Ground terminal	GND.
2	PWR2/PWR1	Power ports, dual power backup access. Supports 48V DC–57V DC power input.
3	Extend Mode	● **ON**: Long-distance transmission mode with 10 Mbps transmission bandwidth, and supports a maximum transmission distance of 250 m with six different types of cables. ● **OFF**: Standard Ethernet mode with 100 Mbps transmission bandwidth, and supports a maximum transmission distance of 100 m with six different types of cables.
4	PD Alive	When PD Alive is dialed to **ON**, the switch perceives that there is no flow output of the camera and determines that the camera crashes. The camera is restarted through PoE power-off to solve the problem.

2.1.3 PoE Power Supply

- One 100 Mbps RJ-45 port supports IEEE802.3af, IEEE802.3at standards and Hi-PoE 60W power supply.
- Three 100 Mbps RJ-45 ports support IEEE802.3af, IEEE802.3at standard power supply.

2.2 8-Port Unmanaged Hardened PoE Switch

2.2.1 Front Panel

Figure 2-3 Front panel

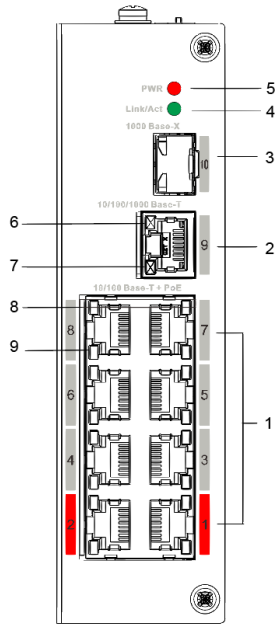


Table 2-3 The description of front panel

No.	Name	Description
1	10/100 Base-T	8 × 10/100 Mbps self-adaptive PoE power supply ports.
2	10/100/1000 Base-T	10/100/1000 Mbps self-adaptive RJ-45 port.
3	1000 Base-X	1000 Mbps SFP fiber port.
4	Link/Act	Fiber port status indicator
5	PWR	Power indicator light, and it is also the PoE power supply status indicator light.
6	Link indicator light	When linking up, the indicator light is solid on.
7	Act indicator light	When the data passing the switch, the indicator light flashes.
8	PoE indicator light	PoE power supply status indicator light.
9	Link/Act indicator light	Ethernet port status indicator.

2.2.2 Upper Cover

Figure 2-4 Upper cover

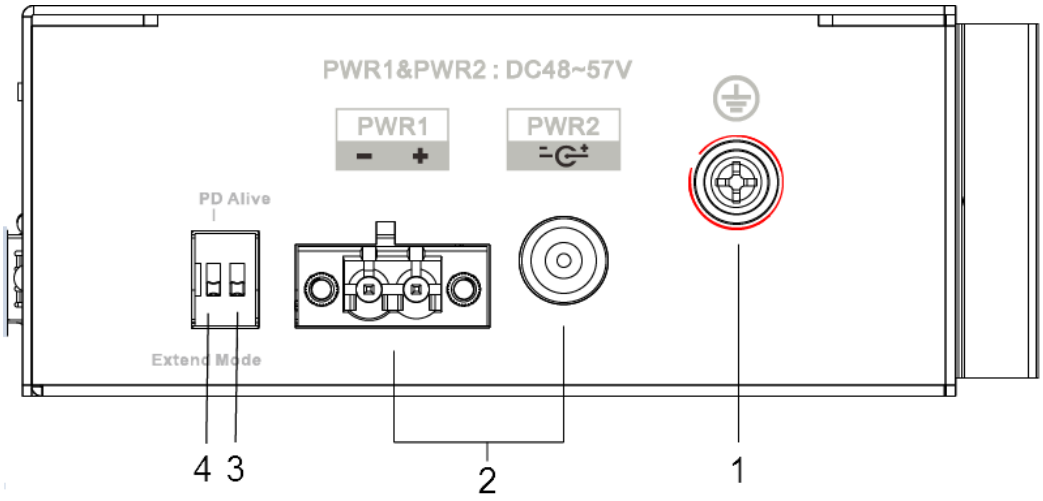


Table 2-4 The description of upper cover

No.	Name	Description
1	Ground terminal	GND.
2	PWR2/PWR1	Power ports, dual power backup access. Supports 48V DC–57V DC power input.
3	Extend Mode	• **ON**: Long-distance transmission mode with 10 Mbps transmission bandwidth, and supports a maximum transmission distance of 250 m with six different types of cables. • **OFF**: Standard Ethernet mode with 100 Mbps transmission bandwidth, and supports a maximum transmission distance of 100 m with six different types of cables.
4	PD Alive	When PD Alive is dialed to **ON**, the switch perceives that there is no flow output of the camera and determines that the camera crashes. The camera is restarted through PoE power off to solve the problem.

2.2.3 PoE Power Supply

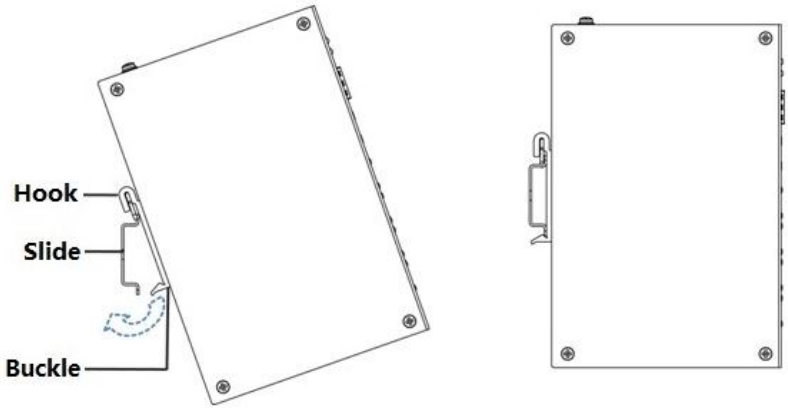
- Two 100 Mbps RJ-45 ports supports IEEE802.3af, IEEE802.3at standards and BT 90W power supply.
- Six 100 Mbps RJ-45 ports support IEEE802.3af, IEEE802.3at standard power supply.

3 Device Installation

PoE switch supports DIN rail mounting. Lay the switch hook on the rail, press the PoE switch to make the buckle get into the slide.

- 4-port PoE switch supports the slide width of 28 mm.
- 8-port PoE switch supports the slide width of 38 mm.

Figure 3-1 Installation



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.