

PoE Extender (4-port Unmanaged Hardened Extender)

Quick Start Guide



Foreword

General

This manual mainly introduces the hardware, installation, and wiring steps of the 4-port unmanaged hardened extender (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, 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
V1.0.2	Corrected description of the front panel	November 2021
V1.0.1	Corrected description of the front panel.	August 2021
V1.0.0	First release.	August 2021

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, comply with the guidelines when using it, and keep the manual safe for future reference.

Operating Requirements



- Make sure that the power supply of the device works properly before use.
- Do not pull out the power cable of the device while it is powered on.
- Only use the device within the rated power range.
- Transport, use and store the device under allowed humidity and temperature conditions.
- Prevent liquids from splashing or dripping on the device. Make sure that there are no objects filled with liquid on top of the device to avoid liquids flowing into it.
- Do not disassemble the device.
- When removing the cable, power off the device first to avoid personal injury.
- Operating temperature range: $-30\text{ }^{\circ}\text{C}$ to $+65\text{ }^{\circ}\text{C}$ ($-22\text{ }^{\circ}\text{F}$ to $+149\text{ }^{\circ}\text{F}$).
- This is a class A product. In a domestic environment this might cause radio interference in which case the user may be required to take adequate measures.

Installation Requirements



WARNING

- Connect the device to the adapter before power on.
- Strictly abide by local electrical safety standards, and make sure that the voltage in the area is steady and conforms to the power requirements of the device.
- Do not connect the device to more than one power supply. Otherwise, the device might become damaged.



- Observe all safety procedures and wear required protective equipment provided for your use while working at heights.
- Do not expose the device to direct sunlight or heat sources.
- Do not install the device in humid, dusty or smoky places.
- Install the device in a well-ventilated place, and do not block the ventilator of the device.
- Make sure the device is in horizontal installation, and install the device on solid and flat surface to avoid falling down.
- Use the power adapter or case power supply provided by the device manufacturer.
- Voltage stabilizer and lightning protection device are optional according to power supply and surrounding environment.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Note that the power supply requirements are subject to the device label.
- Be sure to ground the device (cross section of copper wire: $> 2.5\text{ mm}^2$; resistance to ground: $\leq 4\ \Omega$).
- 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.
- Connect class I electrical appliances to a power socket with protective earthing.
- Do not block the ventilator of the device with objects, such as newspapers, table clothes or curtains.
- Do not put open flames, such as a lit candle, on the device.
- When installing the device, make sure the power plug and appliance coupler are easy to reach to cut off the power.

Maintenance Requirements



- Mark key components on the maintenance circuit diagram with warning signs.
- When replacing the battery, make sure that the same type is used. Improper battery use might result in explosion.

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 Side Panel 3
- 3 Installation 4
- 4 Wiring 5
 - 4.1 Connecting GND 5
 - 4.2 Connecting Ethernet Port 5
 - 4.3 Connecting PoE Ethernet Port 6
- Appendix 1 Cybersecurity Recommendations 7

1 Overview

1.1 Introduction

The Device is a hardened PoE extender. It works together with conventional PoE devices to extend their maximum base transmission distance to 350 meters. It contains a high-performance switching engine and large buffer memory to ensure fewer delays in transmission and high reliability. With its full-metal and fanless design, the Device has great heat dissipation capabilities on its shell surface, offers low power consumption, and works in environments that range from $-30\text{ }^{\circ}\text{C}$ to $+65\text{ }^{\circ}\text{C}$ ($-22\text{ }^{\circ}\text{F}$ to $+149\text{ }^{\circ}\text{F}$). It features overcurrent, overvoltage and EMC (Electro Magnetic Compatibility) protection, effectively resisting the interference of static electricity, lightning strikes and pulses, which ensures the reliable operation of the system. With its DIP design, it provides a variety of work modes that suit different scenes, such as corridors, server farm, small mall and offices.

1.2 Features

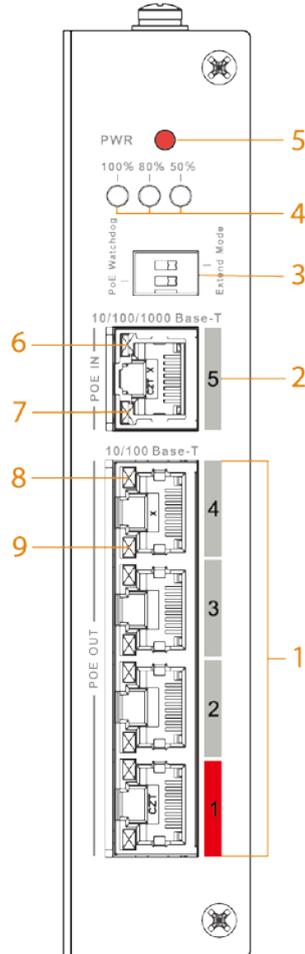
- 4 × 100 Mbps PoE Ethernet ports, 1 × 1000 Mbps PoE Ethernet port.
- All ports meet the requirements of IEEE802.3af and IEEE802.3at standards. The red ports also conform with Hi-PoE and IEEE802.3bt standards.
- 250 m long-distance PoE transmission, which can be enabled by the DIP switch.
- PoE watchdog for real-time detection of terminal device status.
- Lightning Protection: common mode: 4 kV, differential mode: 2 kV.
- Fanless.
- Full-metal.
- Desktop mount and DIN-rail 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 Device. Your actual device might only have a part of them.

Table 2-1 Description of the front panel

No.	Description
1	10/100 Mbps self-adaptive PoE Ethernet ports.
2	10/100/1000 Mbps self-adaptive PoE Ethernet port.
3	DIP switch. <ul style="list-style-type: none"> PoE Watchdog: When a terminal device crash is detected, the Device will 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.

No.	Description
4	<p>PoE output power indicators (with the total power consumption of 60 W).</p> <ul style="list-style-type: none"> ● Solid yellow: Total power \leq 50%. ● Solid green and yellow: $50\% <$ total power \leq 80%. ● Solid green, yellow and red: total power $>$ 80%. <p></p> <p>Normally, the output power consumption of the extender depends on the power supply device.</p>
5	<p>Power indicator.</p> <ul style="list-style-type: none"> ● On: Power on. ● Off: Power off.
6	<p>Single-port connection status indicator (Link).</p> <ul style="list-style-type: none"> ● On: Connected to device. ● Off: Not connected to device.
7	<p>Single-port data transmission status indicator (Act).</p> <ul style="list-style-type: none"> ● Off: No data transmission. ● Flashes: Transmitting data.
8	<p>PoE Ethernet ports status indicator.</p> <ul style="list-style-type: none"> ● On: Powered by PoE. ● Off: Not powered by PoE.
9	<p>Single-port connection or data transmission status indicator (Link/Act).</p> <ul style="list-style-type: none"> ● On: Connected to device. ● Off: Not connected to device. ● Flashes: Transmitting data.

2.2 Side Panel

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

Figure 2-2 Side panel



3 Installation

The Device supports DIN-rail mount. Hang the Device hook on the rail, and press the Device to attach the buckle on the rail.



The width of the DIN-rail supported by the Device is 50 mm.

Figure 3-1 DIN rail

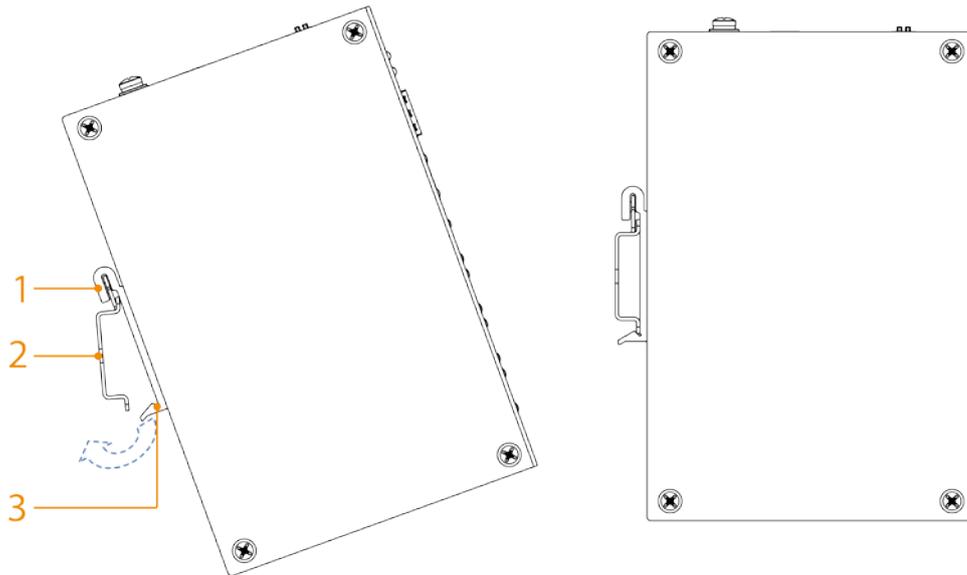


Table 3-1 Component description

No.	Name
1	Hook.
2	Rail.
3	Buckle.

4 Wiring

4.1 Connecting GND

Grounding the Device can protect it against lightning and interference. You should connect the GND cable before powering on the Device and power off the Device before disconnecting the GND cable. There is a GND screw on the side panel of the Device for connecting the GND cable. It is called enclosure GND.

Figure 4-1 GND port



- Step 1** Remove the GND screw from the enclosure GND with a cross screwdriver.
- Step 2** Connect one end of the GND cable to the cold-pressed terminal, and fix it to the enclosure GND with the GND screw.
- Step 3** Connect the other end of the GND cable to the ground.

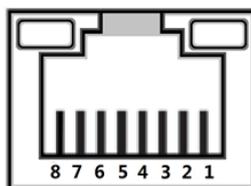


The sectional area of the GND cable must be more than 2.5 mm^2 , and GND resistance must be less than 4Ω .

4.2 Connecting Ethernet Port

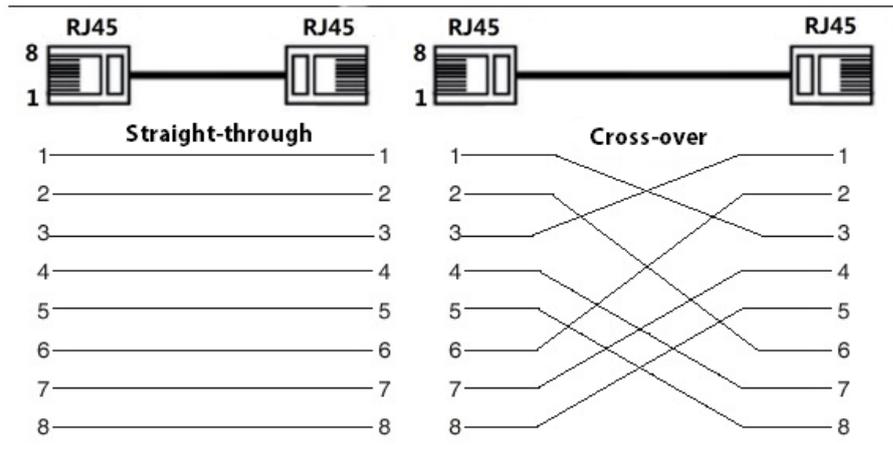
The Ethernet port is a standard RJ-45 port. With its self-adaptation function, it can be automatically configured to full duplex/half-duplex operation mode. It supports MDI/MDI-X self-recognition of the cable, allowing you to use a cross-over cable or straight-through cable to connect the terminal device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

Figure 4-2 Ethernet port pin number



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).

Figure 4-3 Cable connection



4.3 Connecting PoE Ethernet Port

You can directly connect the Device PoE Ethernet 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 Device is 250 m.



The Device must be powered by an LPS-compliant 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.