6-Port 10/100 Mbps Unmanaged Desktop Switch with 4 PoE Ports

User's Manual

V1.0.1

Foreword

General

This user's manual introduces the features and structure of 6-Port 10/100 Mbps unmanaged desktop switch with 4 PoE ports.

General Instruction

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 the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.1	Updated the long distance description.	August 2023
V1.0.0	First release.	September 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 lightning 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.
- Be sure to ground the device (cross section of copper wire: > 2.5 mm^2, resistance to ground: ≤ 4 Ω).

Table of Contents

1 Product Overview

1.1 Introduction

6-Port 10/100 Mbps Unmanaged Desktop Switch with 4 PoE Ports is a type of two-layer commercial switch, which supports long distance Ethernet power supply. It provides 4 × 10/100 Mbps Ethernet ports and 2 × 10/100 Mbps uplink ports. The product is equipped with two types of transmission modes (Extend Mode On/Extend Mode Off).

1.2 Features

General Features

- Layer two commercial switch.
- Supports IEEE802.3, IEEE802.3u and IEEE802.3X standards.
- MAC auto study and aging, MAC address capacity is 2K.
- Supports MDI/MDIX self-adaptation.
- RJ45 port supports 10/100 Mbps self-adaptation, supports IEEE802.3af and IEEE802.3at power supply standards.
- Adopts metal enclosure.
- Supports 48-57 VDC power supply.
- Supports wall-mount installation.
- Supports the anti-theft lock hole.

Individual Features

- Port 1 supports Hi-PoE 60W power supply.
- Supports two types of transmission modes, which are Extend Mode On and Extend Mode Off. When Extend Mode is on, data can be transmitted up to 250 m in CAT6 cable with a bandwidth of 10 Mbps. When Extend Mode is off, data can be transmitted up to 100 m in CAT6 cable with a bandwidth of 100 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.

1.3 Typical Application

Figure 1-1 Typical networking

2 Device Structure

2.1 Front Panel

Figure 2-1 Front panel

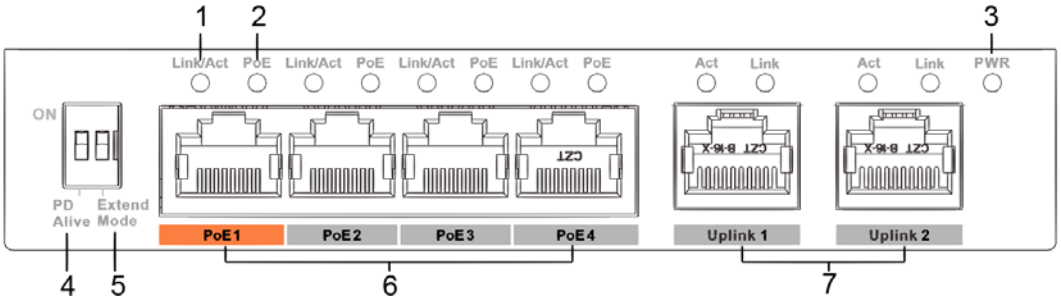

Table 2-1 Front panel description

No.	Name	Description
1	Link/Act	Single port Link status indicator light.
2	PoE	Single port PoE status indicator light.
3	PWR	Power indicator light.
4	PD Alive	When PD Alive (PoE Watchdog) is on, the device can automatically detect camera crashes (no camera activity is detected), and power off and restart the camera through PoE.
5	Extend Mode	• ON: Data can be transmitted up to 250 m in CAT6 cable with a bandwidth of 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. • OFF: Data can be transmitted up to 100 m in CAT6 cable with a bandwidth of 100 Mbps.
6	10/100 Base-T	4 × 10/100 Mbps self-adaptive PoE power supply ports.
7		2 × 10/100 Mbps self-adaptive uplink ports.

2.2 Rear Panel

Figure 2-2 Rear panel

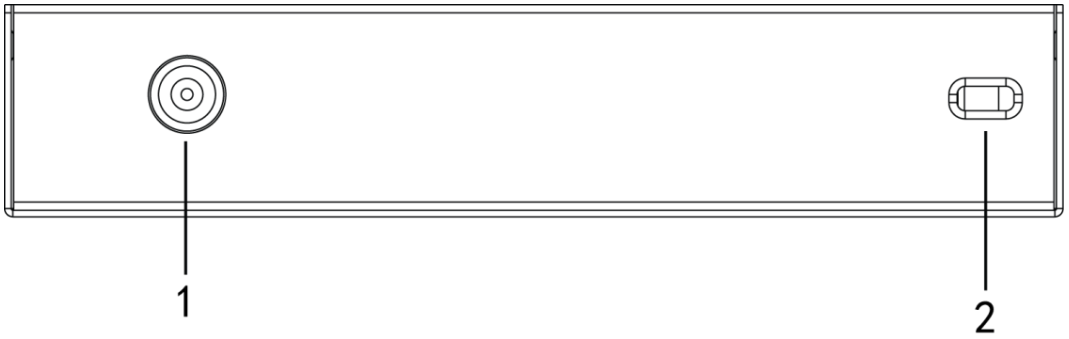

Table 2-2 Rear panel description

No.	Name	Description
1	Power port	Supports 48-57 VDC.
2	Lock hole	Lock the switch.

2.3 Side Panel

Figure 2-3 Side panel

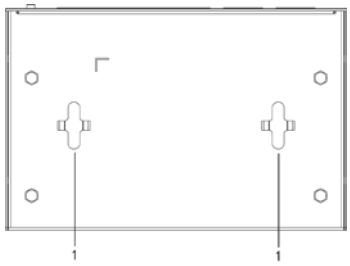

Table 2-3 Side panel description

No.	Name	Description
1	Wall-mount hole	Supports the wall-mount installation.

2.4 PoE Power Supply

- One 100 Mbps RJ45 port supports IEEE802.3af, IEEE802.3at standards and Hi-PoE 60 W power supply.
- Three 100 Mbps RJ45 ports support IEEE802.3af and IEEE802.3at standard power supply.

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:

2. **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.

3. **Change Passwords Regularly**

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

4. **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.

5. **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.

6. **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.

7. **Enable HTTPS**

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

8. **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.

9. **Assign Accounts and Privileges Reasonably**

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

10. **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.

11. **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.

12. **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.

13. **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.

14. **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.