Ethernet Switch (16/24-port Unmanaged Desktop PoE Switch)

Quick Start Guide

V1.0.0

Foreword

This manual introduces the installation, functions and operations of the 16/24-port unmanaged desktop PoE 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.

Identification	Description
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
V1.0.0	First release.	August 2023

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

- 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 mm^2 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 range: -10 ℃ to + 55 ℃ (+ 14 ℉ to + 131 ℉).

Maintenance and repair requirements

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

Table of Contents

1 Overview

1.1 Introduction

16/24-port 100/1000 Mbps unmanaged PoE switch is a two-layer commercial switch. Equipped with a high performance switching engine and large buffer memory, it features low transmission delay and high reliability. With its full metal and fanless design, the device has great heat dissipation and low power consumption, working in environments ranging from -10 °C to +55 °C (+14 °F to +131 °F). With the DIP switch, it supports PoE watchdog, long-distance PoE, VIP port and port isolation, and provides a variety of working modes for different scenarios.

This series of products are suitable for small-scale monitoring networks such as office desktops, schools, hotels, supermarkets, hospitals.

1.2 Features

- Two-layer commercial switch, with working temperature of -10 °C to + 55 °C (+14 °F to +131 °F).
- Supports IEEE 802.3, IEEE 802.3u, IEEE 802.3x, IEEE 802.3az, IEEE 802.3ab, IEEE 802.3z standard.
- Ports 1–2 support IEEE 802.3bt standard, with a maximum power supply of 90 W.
- MAC address automatic learning and aging.
- All RJ-45 ports are automatically adapted to the MDI/MDIX mode.
- Full-metal design.
- Built-in power supply, standard power cord, supports 100–240 VAC, 50/60 Hz power supply.
- Supports desktop and rack mount.
- PoE watchdog.
- Supports 250 m long-distance PoE power supply, which can be controlled by the 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.
- Supports the VIP port QoS mode.
- Port isolation.

2 Structure

2.1 Front Panel

The following figure uses a 24-port 100 Mbps switch for an example, and is for reference only. Please refer to the actual products.

Figure 2-1 Front panel

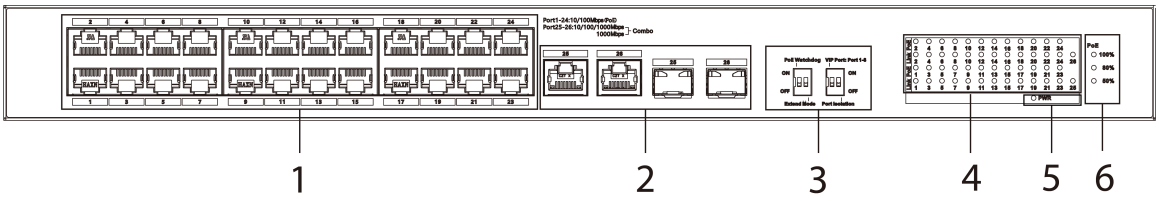


Table 2-1 Description of front panel

No.	Name	Description
1	PoE RJ-45 port	10/100 Mbps or 10/100/1000 Mbps self-adaptive Ethernet port. Ports 1–2 support IEEE 802.3af/at/bt standards, and other ports support IEEE 802.3af/at standards.
2	Uplink Port	• 100 Mbps: 2 × combo uplink ports (the electrical port supports 10/100/1000 Mbps, and the optical port supports 1000 Mbps). • 1000 Mbps: 2 × 10/100/1000 Mbps self-adaptive RJ-45 ports and 2 × 1000 Mbps SFP optical ports.
3	Dial switch	• PoE watchdog: Enable the PoE watchdog through the DIP switch. When detecting IPC crash, the IPC powers off and restarts. • Extend mode: Enable the long-distance transmission through the DIP switch. The transmission distance of the PoE port is up to 250 m but the transmission rate drops 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: Port 1–8. Enable the QoS mode through the DIP switch to enable priority transmission of 1 to 8 electrical ports. • Port isolation: Enable the port isolation through the DIP switch. After it is enabled, the downlink ports are independent, and the traffic is not interconnected, while the downlink ports and uplink ports can communicate with each other.
4	Port indicator/PoE indicator	The port status indicator and PoE status indicator.
5	Power indicator	Power indicator.

No.	Name	Description
6	PoE output power indicator	PoE output power indicator.

Table 2-2 Description of thr indicator status

Indicator	Indicator color	Status	Description
PWR	Green	Solid on	Power on.
		Off	Power off.
PoE indicator	Green	Solid on	Powered by PoE.
		Off	Not powered by PoE.
Port indicator	Green	Link indicator off	The port is not linked.
		Link indicator solid on	Port links up.
		Link indicator flashes	Port data transmission in progress.
PoE output power indicator	Green	Only green solid on	PoE total output power ≦ 50%.
	Green, yellow	Green and yellow solid on	50% < PoE total output power ≦ 80%.
	Green, yellow, red	Green, yellow and red solid on	80% < PoE total output power.

2.2 Rear Panel

The following figure is for reference only. Rear panel diagrams differ depending on different models. Refer to actual products for details.

Figure 2-2 Rear Panel

Table 2-3 Rear panel description

No.	Name	Description
1	Power port	Supports 100–240 VAC.

No.	Name	Description
2	Grounding terminal	Ground.  • Normal GND of the device is the important guarantee for device lightning protection and anti-interference. You should connect the GND cable before powering on the device, and then power off the device before disconnecting the GND cable. • The sectional area of the GND cable must be more than 2.5 mm^2, and the GND resistance must be less than 4 Ω.

3 Installation and Connection

3.1 Installation

3.1.1 Desktop Mount

The Switch supports desktop mount. You can directly place it on a solid and flat desktop, and reserve enough ventilation space for the switch to dissipate heat.

3.1.2 Rack Mount

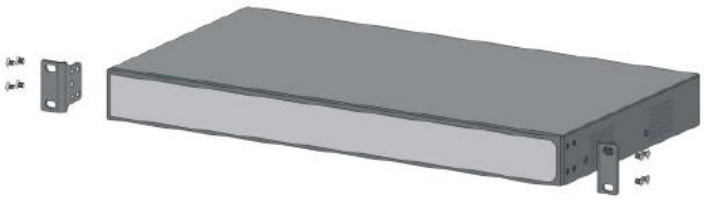
Background Information

Switches can be installed in EIA standard 11-inch size racks.

Procedure

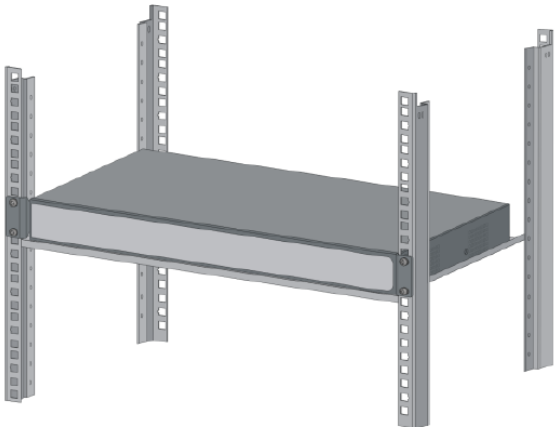
Step 1 Attach the mounting brackets to the switch (one on each side), and then fix them with the provided screws.

Figure 3-1 Attach the mounting brackets



Step 2 Fix the switch onto the rack.

Figure 3-2 Fix the switch onto the rack



3.2 Powering on

Connect one end of the power adapter to the power port on the rear panel of the switch, and insert the other end into the socket. Turn on the power switch on the rear panel, check whether the

power indicator (PWR) of the switch is on. If the power indicator (PWR) is on, it indicates that the power connection is successful.

3.3 Connecting Network Cable

Connect one end of the network cable to the IPC that supports PoE, and the other end to any RJ-45 port of the switch. The maximum distance between the switch and IPC is about 100 meters (If Extend Mode is enabled, the maximum distance is 250 meters). After connected, the IPC powers on and the corresponding switch port starts to work normally.

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.

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:

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.