Gigabit Unmanaged PoE Switch

User’s Manual

V1.0.0

Foreword

General

This manual introduces the features and structure of the gigabit unmanaged switch with PoE ports device (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, 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
V1.0.0	First release.	July 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 jurisdictions. For detailed information, refer to 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, 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 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 occurring when using the device.
- If there is any uncertainty or controversy, we reserve the right of 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.

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.

Table of Contents

1 Product Overview

1.1 Introduction

The gigabit unmanaged PoE switch provides multiple 10/100/1000 Mbps adaptive ports. Using store and forward technologies and combined with dynamic memory allocation to ensure that messages are effectively distributed to each port. Support flow control function to avoid the loss of data packets during transmitting and receiving. Compatible with three network environments of 10 Base-T, 100 Base-TX and 1000 Base-T, and the port speed is automatically matched with 10/100/1000 Mbps. Configure optical ports for long-distance transmission through optical fiber.

The product supports standard PoE power supply; support IEEE802.3af and IEEE802.3at standards; port 1 and port 2 support IEEE802.3bt standard, and are compatible with Hi-PoE. This series of products are designed with high integration, light and easy to use, and are widely used in office and home networks.

1.2 Features

General Features

- Supports IEEE802.3, IEEE802.3u, IEEE802.3x, IEEE802.3az, and IEEE802.3ab standards.
- Flow control method: full-duplex adopts IEEE802.3x standard and half-duplex adopts back-pressure standard.
- Port 1 and port 2 support IEEE802.3bt standard and are compatible with Hi-PoE.
- 2 gigabit uplink optical ports.
- Store and forward technologies.
- The UTP port supports the auto-negotiation function to automatically adjust the transmission mode and transmission rate.
- Supports MAC address self-learning.
- Supports MDI/MDIX self-adaptation.
- Adopts metal enclosure.

Individual Features

- The 20-Port Unmanaged Desktop Gigabit Switch supports 16 × 10/100/1000 Mbps adaptive RJ45 ports; supports built-in power supply.
- The 28-Port Unmanaged Desktop Gigabit Switch supports 24 × 10/100/1000 Mbps adaptive RJ45 ports; supports built-in power supply.

2 Device Structure

2.1 20-Port Unmanaged Desktop Gigabit Switch

Front Panel

Figure 2-1 Front panel

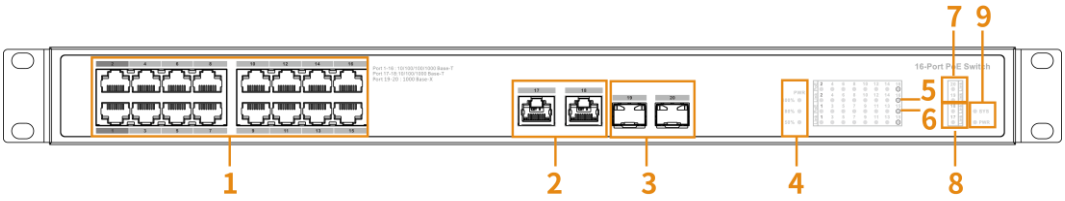


Table 2-1 Description of front panel

No.	Name	Description
1	PoE RJ45 port	• Port 1–Port 2: 2 × 10/100/1000 Mbps adaptive RJ45 ports, support BT-PoE and Hi-PoE power supply, power-on time is within10 s. • Port 3–Port 16: 14 × 10/100/1000 Mbps adaptive RJ45 ports, support PoE power supply.
2	Gigabit uplink Ethernet port	Port 17–Port 18: 2 × 10/100/1000 Mbps adaptive RJ45 ports.
3	Gigabit uplink optical port	Port 19–Port 20: 2 × 1000 Mbps optical ports.
4	Power indicator	Current PoE power consumption display.
5	Ethernet port indicator light	Real-time status display of the Ethernet ports.
6	PoE indicator light	Real-time status display of the PoE ports.
7	Optical port indicator light	Connection status of the optical ports.
8	Ethernet port indicator light	Connection status of the Ethernet ports.
9	Status indicator light	Device status indicator light and power indicator light.

Table 2-2 Description of indicator light

Indicator	Indicator Color	Status	Description
PWR	Green	On	The Device is powered on.
		Off	The Device is powered off.
PoE indicator light	Green	On	PoE power supply is used.
		Off	PoE power supply is not used.
Port	Green	Link indicator off	The port is not linked.

Indicator	Indicator Color	Status	Description
indicator light		Link indicator on	The port is linked.
		Link indicator flashing	The port is receiving or sending data.

Rear Panel

Figure 2-2 Rear panel

Table 2-3 Description of rear panel

No.	Name	Description
1	Power switch	Used for Powering on or off the Device.
2	Power port	Supports 100V–240V AC power input.
3	Ground screw	GND.

2.2 28-Port Unmanaged Desktop Gigabit Switch

Front Panel

Figure 2-3 Front panel

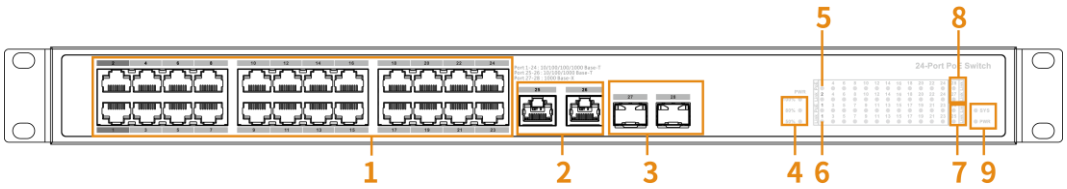


Table 2-4 Description of front panel

No.	Name	Description
1	PoE RJ45 port	• Port 1–Port 2: 2 × 10/100/1000 Mbps adaptive RJ45 ports, support BT-PoE and Hi-PoE power supply, power-on time is within 10 s. • Port 3–Port 24: 22 × 10/100/1000 Mbps adaptive RJ45 ports, support PoE power supply.
2	Gigabit uplink Ethernet port	Port 25–Port 26: 2 × 10/100/1000 Mbps adaptive RJ45 ports.
3	Gigabit uplink optical port	Port 27–Port 28: 2 × 1000 Mbps optical ports.
4	Power indicator	Current PoE power consumption display.
5	Ethernet port indicator light	Real-time status display of the Ethernet ports.

No.	Name	Description
6	PoE indicator light	Real-time status display of the PoE ports.
7	Optical port indicator light	Connection status of the optical ports.
8	Ethernet port indicator light	Connection status of the Ethernet ports.
9	Status indicator light	Device status indicator light and power indicator light.

Table 2-5 Description of indicator light

Indicator	Indicator Color	Status	Description
PWR	Green	On	The Device is powered on.
		Off	The Device is powered off.
PoE indicator light	Green	On	PoE power supply is used.
		Off	PoE power supply is not used.
Port indicator light	Green	Link indicator off	The port is not linked.
		Link indicator on	The port is linked.
		Link indicator flashing	The port is receiving or sending data.

Rear Panel

Figure 2-4 Rear panel

Table 2-6 Description of rear panel

No.	Name	Description
1	Power switch	Used for Powering on or off the Device.
2	Power port	Supports 100V–240V AC power input.
3	Ground screw	GND.

3 Installation and Connection

3.1 Installation

3.1.1 Desktop Installation

You can install the Device on a stable desk and place it near the power supply. Make sure that there is enough ventilation space for heat dissipation.

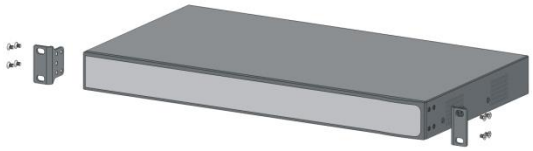
3.1.2 Rack Installation

You can install the Device on the 11-inch rack of EIA standard.

Step 1 Check the grounding of the rack, and make sure that the rack is stable.

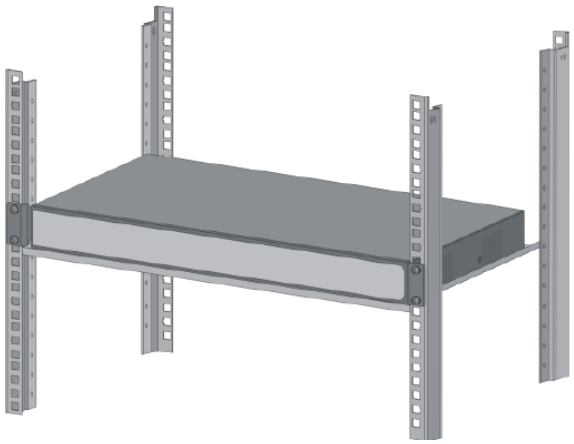
Step 2 Fix the brackets on both sides of the side panel of the Device with screws.

Figure 3-1 Fix bracket



Step 3 Fix the Device on the rack with screws.

Figure 3-2 Fix the Device on the rack



3.2 Powering on the Device

Step 1 Connect one end of the power adapter to the power port on the rear panel of the Device, and then plug the other end into the socket.

Step 2 Check whether the power indicator light (PWR) of the Device is on. If the power indicator light 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 RJ45 port of the Device. The maximum distance between the Device and the IPC is about 100 meters. Once the connection is successful and the device is powered on normally, the corresponding switch port works normally.

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 equipment 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 equipment (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 equipment 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 equipment network security:

1. **Physical Protection**

   We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment 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 equipment (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 equipment 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. **Enable Whitelist**
   We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the whitelist.
8. **MAC Address Binding**
   We recommend you to bind the IP and MAC address of the gateway to the equipment, 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 equipment 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 equipment, 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 equipment 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.

- It is recommended that you enable your device's firewall or blacklist and whitelist feature to reduce the risk that your device might be attacked.