

12-port Managed Desktop Gigabit Switch with 8-port PoE

Quick Start Guide








Foreword

General

This manual introduces the functions and operations of 12-port managed desktop Gigabit switch with 8-port PoE (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 2021

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, 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 disassemble the device without professional instruction.
- Transport, use, and store the device in allowed ranges of humidity and temperature.
- When removing the cable, power off the device first to avoid personal injury.
- Voltage stabilizer and lightning protection device are optional according to 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 must conform to the requirements of ES1 in IEC 62368-1 standard and no higher than PS2. Note that 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: $\leq 4 \Omega$).
- The coupler is the disconnecting apparatus. Keep it at the angle for easy operation.

Table of Contents

- Foreword I
- Important Safeguards and Warnings..... III
- 1 Overview 1
 - 1.1 Introduction 1
 - 1.2 Features 1
- 2 Device Structure..... 2
 - 2.1 Front Panel..... 2
 - 2.2 Rear Panel..... 2
- 3 Installation 3
 - 3.1 Installing Device..... 3
 - 3.2 Wiring 3
 - 3.2.1 Connecting GND..... 3
 - 3.2.2 Connecting Power Cord..... 4
 - 3.2.3 Connecting Ethernet Port..... 4
 - 3.2.4 Connecting SFP Port..... 5
- 4 Device Login..... 6
- Appendix 1 Cybersecurity Recommendations 7

1 Overview

1.1 Introduction

The device is a layer-2 commercial switch. It provides high-performance switching engine and large buffer memory to ensure smooth video stream transmission. With a full-metal and fanless design, the device features great heat dissipation capability on the shell surface, and is able to work in the environment from $-10\text{ }^{\circ}\text{C}$ to $+55\text{ }^{\circ}\text{C}$. With Telnet, WEB management, SNMP (Simple Network Management Protocol) and other functions, the device can be remotely managed. The device can directly connect to iLinksView.

The device is applicable for use in different scenarios, including home, office, server farm, and small mall.

1.2 Features

- 8 × gigabit PoE ports; 2 × gigabit uplink Ethernet ports; 2 × gigabit SFP fiber ports
- Supports IEEE802.3af and IEEE802.3at. The red ports support Hi-PoE and IEEE802.3bt
- 250 m long-distance PoE transmission (10 Mbps)
- PoE watchdog
- Supports STP, RSTP, and MSTP
- IEEE802.1Q-based VLAN configuration
- Manual link aggregation and static LACP
- Desktop mount and wall mount

2 Device Structure

2.1 Front Panel

Figure 2-1 Front panel

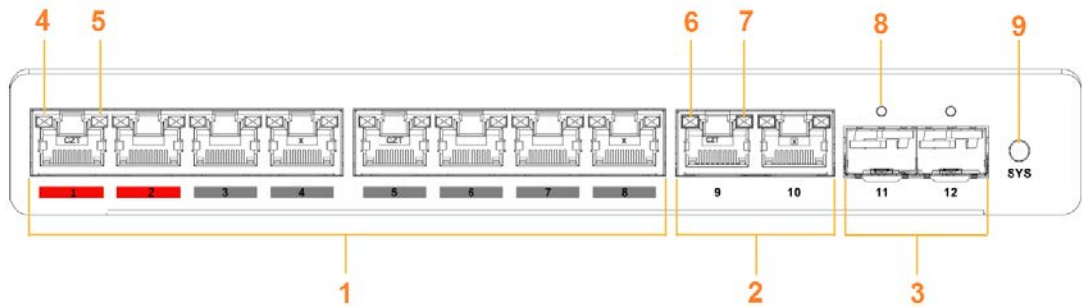


Table 2-1 Front panel description

No.	Description
1	8 × 10/100/1000 Mbps self-adaptive PoE power supply ports.
2	2 × 10/100/1000 Mbps self-adaptive uplink ports.
3	2 × 1000 Mbps self-adaptive SFP fiber ports.
4	Ethernet port status indicator light.
5	PoE power supply status indicator light.
6	When the data is passing the switch, the indicator light flashes.
7	When linking up, the indicator light is always on.
8	Fiber port status indicator light.
9	System status indicator light.

2.2 Rear Panel

Figure 2-2 Rear panel



Table 2-2 Rear panel description

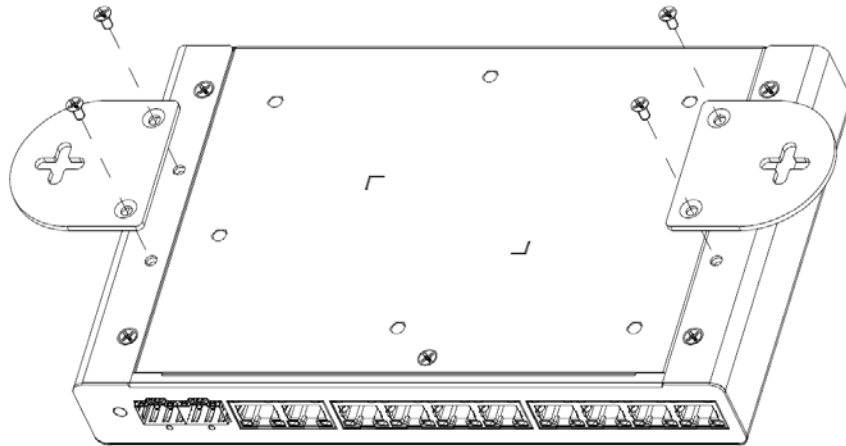
No.	Name	Description
1	GND	Ground terminal.
2	Reset	Reset the whole system.
3	Power port	Supports 48–57V DC.

3 Installation

3.1 Installing Device

The device supports standard rack mount.
Install the rack mount kit on both sides of the switch.

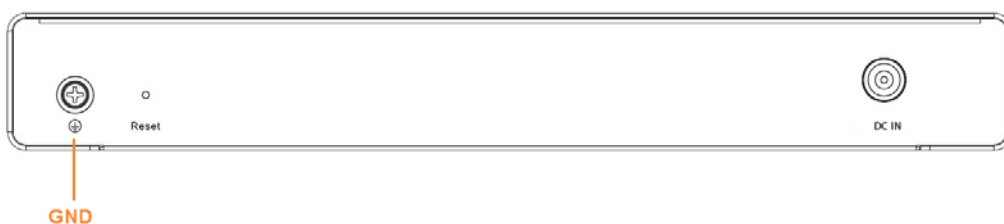
Figure 3-1 Rack mount



3.2 Wiring

3.2.1 Connecting GND

Figure 3-2 GND terminal



Normal GND connection 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 power off the device before disconnecting the GND cable.

There is a GND screw on the device cover board for the GND cable, which is called enclosure GND. Connect one end of the GND cable with the cold-pressed terminal, and fix it on the enclosure GND with the GND screw. The other end of the GND cable should be reliably connected to the ground.



The sectional area of the GND cable shall be more than 2.5 mm², and the GND resistance shall be less than 4 Ω.

3.2.2 Connecting Power Cord

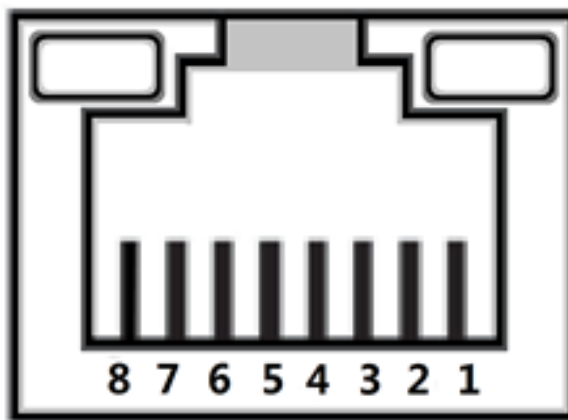
Before connecting the power cord, make sure that the device is reliably grounded.

Step 1 Connect one end of the power cord into the power jack of the device accurately.

Step 2 Connect the other end of the power cord to the external power socket.

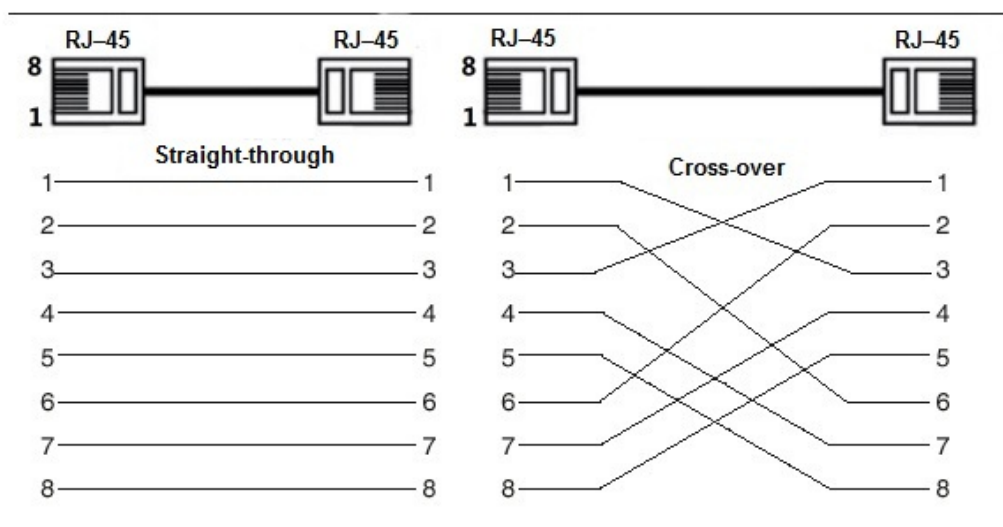
3.2.3 Connecting Ethernet Port

Figure 3-3 Ethernet port pin number



10/100/1000 M Base-T Ethernet port adopts standard RJ-45 port. Equipped with self-adaptation function, it can be automatically configured to full duplex/half-duplex operation mode, and supports MDI/MDI-X self-recognition function of the cable, which means that the switch can use cross-over cable or straight-through cable to connect terminal device to network device.

Figure 3-4 Pin description



The cable connection of RJ-45 connector conforms to the standard 568B (1-orange white, 2-orange, 3-green white, 4-blue, 5-blue white, 6-green, 7-brown white, 8-brown).



When connecting to a non-PoE device, the device needs to be used with an isolated power supply.

3.2.4 Connecting SFP Port

Before installing SFP module, wear antistatic gloves, and then wear antistatic wrist strap. Make sure that the antistatic gloves and the antistatic wrist strap are in good contact.

Step 1 Lift the handle of SFP module upward vertically, and stuck it to the top hook.

Step 2 Hold the SFP module by both sides, and push it gently into the SFP slot till the SFP module is firmly connected to the slot (both the top and bottom spring strip of the SFP module are firmly stuck with the SFP slot).



The signal is transmitted through laser by optical fiber cable. The laser conforms to the requirement of level 1 laser products. To avoid injury of eyes, do not look at the 1000 Base-X optical port directly when the device is powered on.

Figure 3-5 SFP module structure

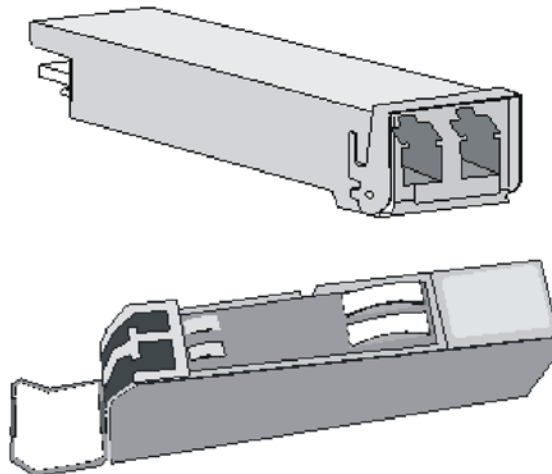
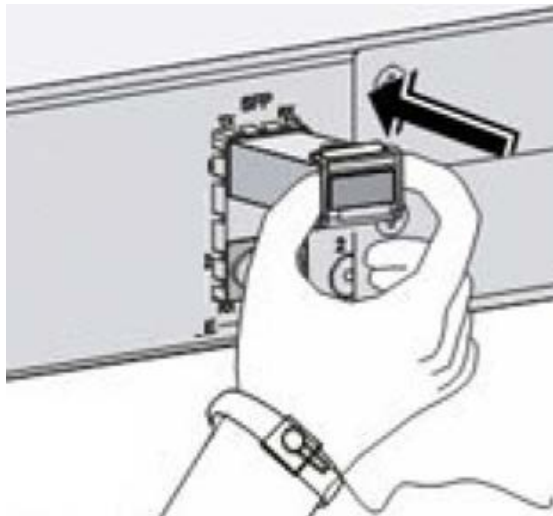


Figure 3-6 SFP module installation



4 Device Login

You can log in to the device through WEB for management and operation.

Step 1 In the browser address bar, enter the IP address of the device (192.168.1.110 by default).

Step 2 Enter the username and password (both are admin by default).

Step 3 Click **Login**.



For first login, you need to change the password according to the interface prompt.

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.