

Ethernet Switch (8-Port Gigabit Managed Switch)

Quick Start Guide



Foreword-nopoe

General

This manual mainly introduces the hardware, installation, and wiring steps of the 8-port Gigabit managed switch (hereinafter referred to as "the device"). Read carefully before using the device, and keep the manual safe for future reference.

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.	September 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



WARNING

- 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 mm² 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.
- This is a class A product. In a domestic environment this may cause radio interference in which case you may be required to take adequate measures.
- Do not block the ventilator of the device with objects, such as a newspaper, table cloth or curtain.
- Do not place an open flame on the device, such as a lit candle.

Maintenance Requirements



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

Table of Contents

- Foreword-nopoe.....I
- Important Safeguards and Warnings..... III
- 1 Overview 1
 - 1.1 Introduction 1
 - 1.2 Features..... 1
- 2 Structure 2
 - 2.1 Front Panel..... 2
 - 2.2 Rear Panel..... 2
- 3 Installation4
 - 3.1 Preparations.....4
 - 3.2 Desktop Mount 4
 - 3.3 Wall Mount..... 4
 - 3.4 Wiring 5
 - 3.4.1 Ethernet Port..... 5
 - 3.4.2 Console Port 5
 - 3.4.3 SFP Port..... 6
 - 3.4.4 GND..... 7
- 4 Quick Operations..... 8
- Appendix 1 Cybersecurity Recommendations..... 9

1 Overview

1.1 Introduction

Equipped with a high performance switching engine, the switch performs optimally. It has low transmission delay, large buffer and is highly reliable. It also has a strong switching capability and optimizes transmission performance when accessing Ultra HD videos. 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 ($+14^{\circ}\text{F}$ to $+131^{\circ}\text{F}$). With protection against overvoltage, EMC and overcurrent from power input terminals, the switch effectively resists interference from static electricity, lightning, and pulses. It also has powerful network management functions, supporting various types of web and network management software based on SNMP.

The switch is applicable to different scenarios including houses, offices and small malls.

1.2 Features

- Layer 2 network management switch.
- Network redundancy: STP/RSTP.
- Static link aggregation and LACP.
- Devices discovery based on LLDP.
- QoS (IEEE802.1p/1Q) to increase determinism.
- IGMP Snooping.
- Fanless design.
- EMC high protection design.
- Desktop and wall-mounted installation.

2 Structure

2.1 Front Panel

Figure 2-1 Front panel

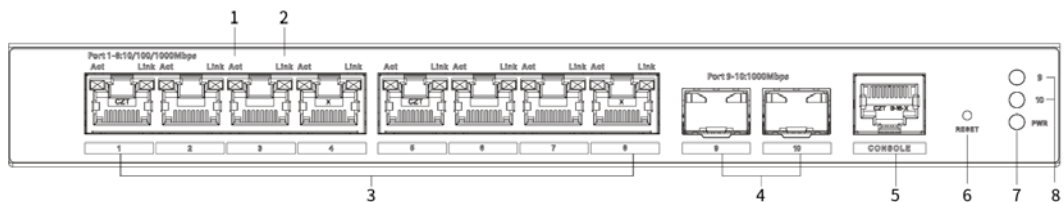


Table 2-1 Front panel description

No.	Name	Description
1	Downlink port Act indicator	Displays the Act status of the downlink port. - Flashes: Data receiving and sending. - Off: No data receiving and sending.
2	Downlink port Link indicator	Displays the Link status of the downlink port. - Solid on: Connected to devices. - Off: Not connected to devices.
3	RJ-45 port	Ethernet port, supports 10/100/1000 Mbps self-adaptive.
4	Gigabit uplink optical port	2 optical ports, support 1000 Mbps.
5	Console port	Device debugging port.
6	Reset button	Press and hold the button for over 5 s until all the indicators are on, and then release the button to recover to the default settings.
7	Power indicator	Displays the current power status of the device.
8	Uplink port indicator	Displays the current status of the Uplink port.

2.2 Rear Panel

Figure 2-2 Rear panel

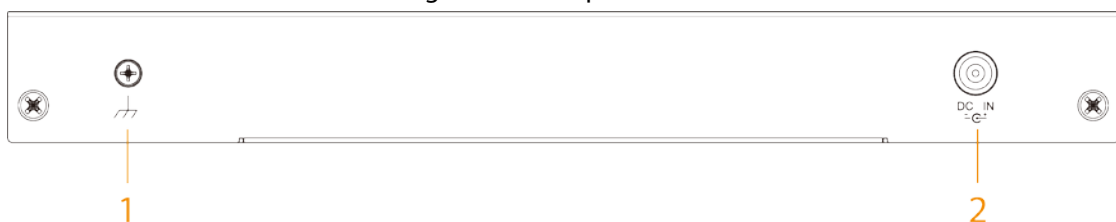


Table 2-2 Rear panel description

No.	Name	Description
1	Ground terminal	GND.
2	Power input port	Supports 12 VDC.

3 Installation

3.1 Preparations

- Select a proper installation method according to your actual needs.
- Make sure that the working platform is stable and steady.
- Leave about 10 cm space for heat dissipation to ensure good ventilation.

3.2 Desktop Mount

The switch supports desktop mount. Place it on a steady and stable desktop.

3.3 Wall Mount

Procedure

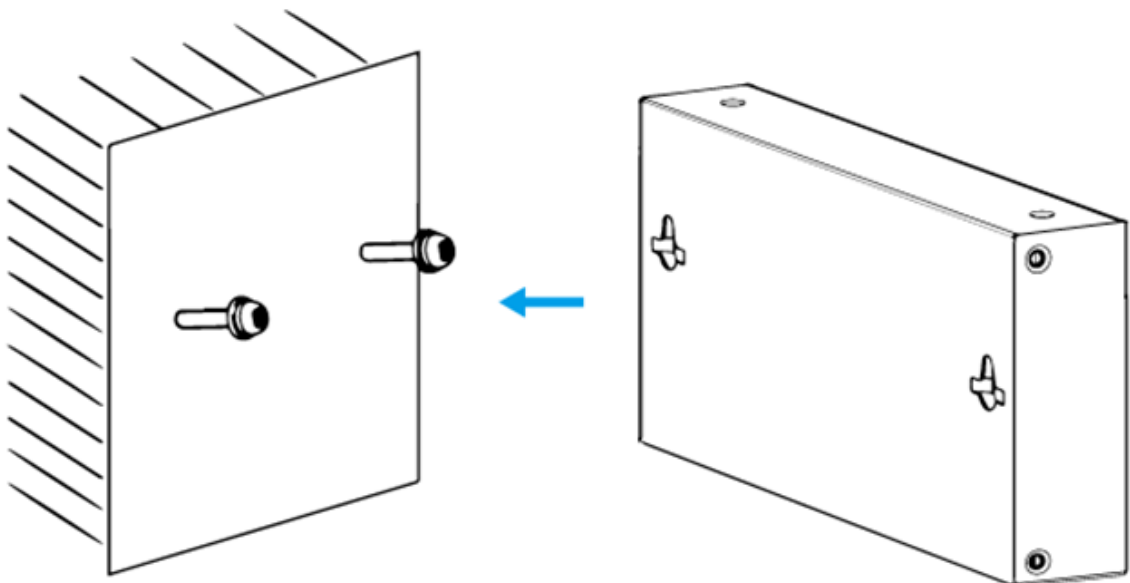
- Step 1 Drill two M4 screws into the wall, leaving a space of 4 mm between the wall and the head of the screw.



- Screws do not come with the package. Purchase them as needed.
- Make sure that the distance between the screws is the distance between the wall-mount holes (120 mm).

- Step 2 Align the wall-mount holes on the back cover of the device with the screws, and hang the device on the screws.

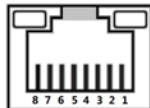
Figure 3-1 Wall mount



3.4 Wiring

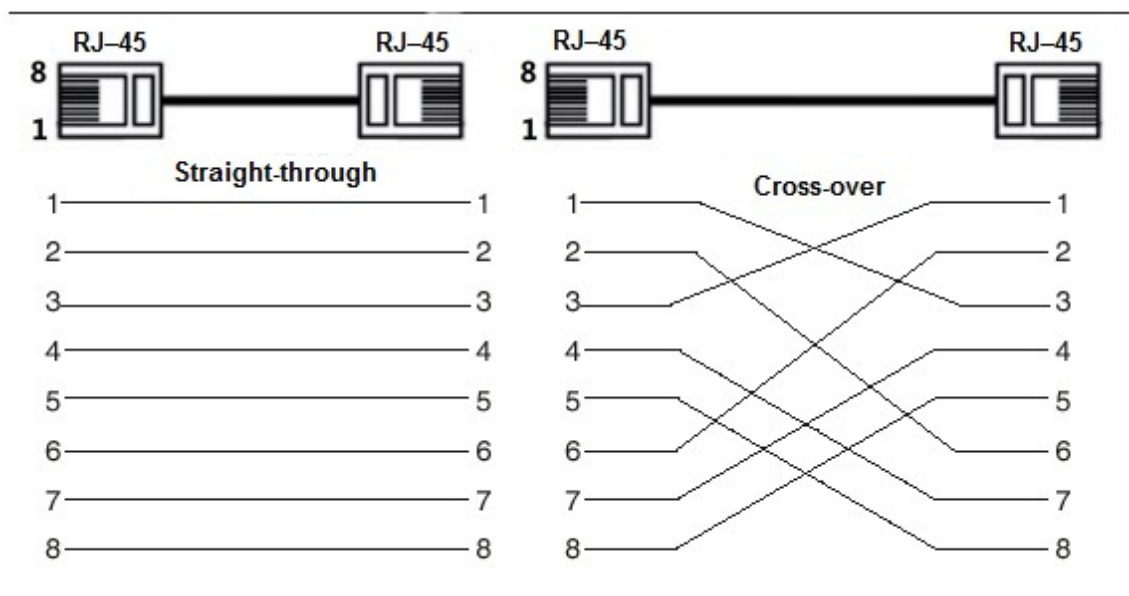
3.4.1 Ethernet Port

Figure 3-2 Ethernet port pin number



10/100/1000 Mbps 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.

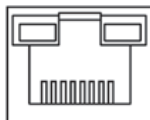
Figure 3-3 Pin description



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).

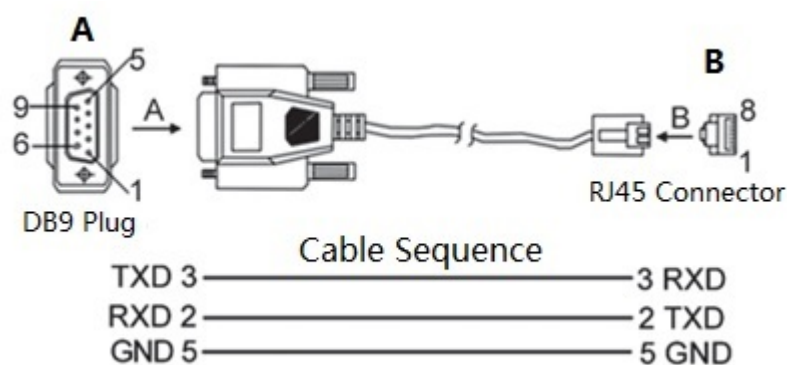
3.4.2 Console Port

Figure 3-4 Console port



The switch console port and computer controlling 9-pin serial port are connected with RJ-45 DB9 cable. You can call the console software of the device by operating the superterminal software of the Windows system for device configuration, maintenance, and management.

Figure 3-5 Cable sequence of RJ45 DB9



One end of RJ-45 DB9 cable is RJ-45 connector, which needs to be inserted into the console port of the device. And the other end is DB9 plug, which needs to be inserted into the computer controlling 9-pin serial port.

Table 3-1 Pin description

DB9 pin	RJ-45 pin	Signal	Description
2	3	RXD	Receiving data
3	2	TXD	Sending data
5	5	GND	GND

3.4.3 SFP Port

Background Information



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.

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.

Figure 3-6 SFP module structure

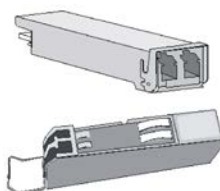
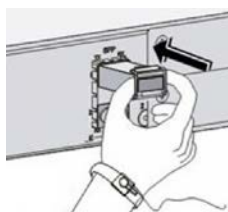


Figure 3-7 SFP module installation



Procedure

- Step 1 Lift the handle of SFP module upward vertically, and then stuck it to the top hook.
- Step 2 Hold the SFP module by both sides, and then 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.

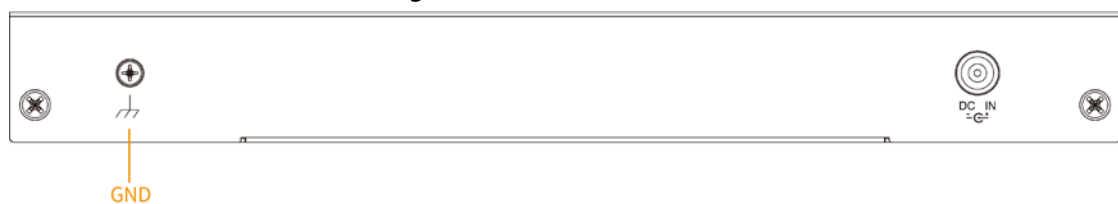
3.4.4 GND

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 then fix it on the enclosure GND with the GND screw. The other end of the GND cable should be reliably connected to the 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 should be more than 2.5 mm^2 , and the GND resistance shall be less than 4Ω .

Figure 3-8 GND terminal



4 Quick Operations

We will introduce VLAN configuration briefly in this section. See the corresponding command line manual for detailed configuration.

You can log in to web page of the device via the following IP address.

Table 4-1 Device factory default

Parameter	Description
IP address	192.168.1.110/255.255.255.0
Username	admin
Password	User Define

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.