Ethernet Switch (Unmanaged Desktop Switch)

Quick Start Guide

V1.0.0

Foreword

General

This manual mainly introduces the hardware, installation, and wiring steps of the 5/8/16/24-port unmanaged desktop switch (hereinafter referred to as "the Device").

Safety Instructions

The following signal words 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 2021

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. 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

This section introduces content covering the proper handling of the Device, hazard prevention, and prevention of property damage. Read carefully before using the Device, comply with the guidelines when using it, and keep the manual safe for future reference.

Operating Requirements

- Make sure that the power supply of the device works properly before use.
- Do not pull out the power cable of the device while it is powered on.
- Only use the device within the rated power range.
- Transport, use and store the device under allowed humidity and temperature conditions.
- Prevent liquids from splashing or dripping on the device. Make sure that there are no objects filled with liquid on top of the device to avoid liquids flowing into it.
- Do not disassemble the device.
- Operating temperature range: –10 °C (14 °F) to +55 °C (131 °F).
- This is a class A product. In a domestic environment this might cause radio interference in which case the user may be required to take adequate measures.

Installation Requirements

- Connect the device to the adapter before power on.
- Strictly abide by local electrical safety standards, and make sure that the voltage in the area is steady and conforms to the power requirements of the device.
- Do not connect the device to more than one power supply. Otherwise, the device might become damaged.

- Observe all safety procedures and wear required protective equipment provided for your use while working at heights.
- Do not expose the device to direct sunlight or heat sources.
- Do not install the device in humid, dusty or smoky places.
- Install the device in a well-ventilated place, and do not block the ventilator of the device.
- Use the power adapter or case power supply provided by the device manufacturer.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Note that the power supply requirements are subject to the device label.
- Be sure to ground the device (cross section of copper wire: > 2.5 mm^2; resistance to ground: ≤ 4 Ω).
- 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.
- Connect class I electrical appliances to a power socket with protective earthing.
- Do not block the ventilator of the device with objects, such as newspapers, table clothes or curtains.
- Do not put open flames, such as a lit candle, on the device.

- When installing the device, make sure the power plug and appliance coupler are easy to reach to cut off the power.

Maintenance 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

The Device is a layer-2 commercial switch. It has a high-performance switching engine and a 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 environments that range from–10 ℃ (14 °F) to +55 ℃ (131 °F). The Device is an unmanaged switch, so it does not need to be configured through web interface, which simplifies installation.
The Device is applicable for use in in a variety of scenarios, such as in the home and office, on server farms, and in small malls.

1.2 Features

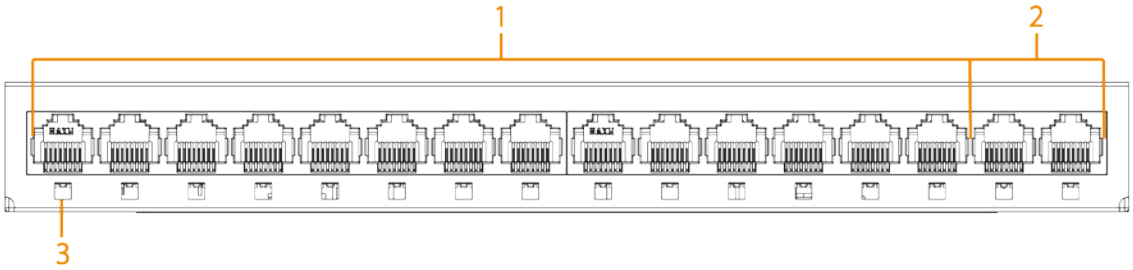
- 5/8/16/24 × 100/1000 Mbps Ethernet ports.
- All ports meet the requirements of IEEE802.3, IEEE802.3u, IEEE802.3x, IEEE802.3ab and IEEE802.3z standards.
- Supports non-blocking cable speed forwarding on all ports.
- Supports IEEE 802.3x (full duplex flow control) and back pressure flow control (half duplex).
- Full metal enclosure with a fully-sealed, dustproof and fanless design.
- Desktop mount and wall mount.

2 Port and Indicator

2.1 Front Panel

The following figure is for reference only, and might differ from the actual product.

Figure 2-1 Front panel



Following are all the ports and indicators on the front panel of the 16-port unmanaged desktop switch. Your actual device might only have some of them.

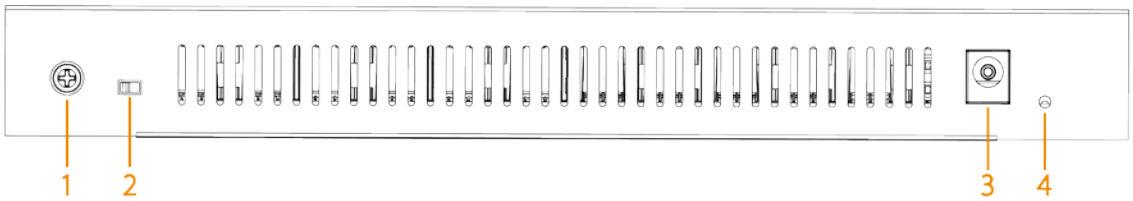
Table 2-1 Description of front panel

No.	Description
1	10/100 Mbps or 10/100/1000 Mbps self-adaptive Ethernet ports.
2	10/100 Mbps or 10/100/1000 Mbps self-adaptive uplink ports.
3	Single-port connection or data transmission status indicator (Link/Act). ● On: Connected to device. ● Off: Not connected to device. ● Flashes: Data transmission is in progress.

2.2 Rear Panel

The following figure is for reference only, and might differ from the actual product.

Figure 2-2 Rear panel



Following are all the ports and indicators on the rear panel of the 16-port unmanaged desktop switch. Your actual device might only have some of them.

Table 2-2 Description of rear panel

No.	Description
1	Ground terminal. Available on select models.
2	DIP Switch. ● ON: Ports 1 through 14 cannot communicate with each other, but can communicate with uplink ports of 15 and 16. ● OFF: All ports can communicate with each other. Available on select models.
3	Power port.
4	Power indicator. ● On: Power on. ● Off: Power off.

3 Installation

3.1 Preparation

- Select an appropriate installation method.
- Install the Device on a solid and flat surface.
- Leave around 10 cm of open space around the Device for heat dissipation and to ensure good ventilation.

3.2 Desktop Mount

The Device supports desktop mount. You can directly place it on a solid and flat desktop.

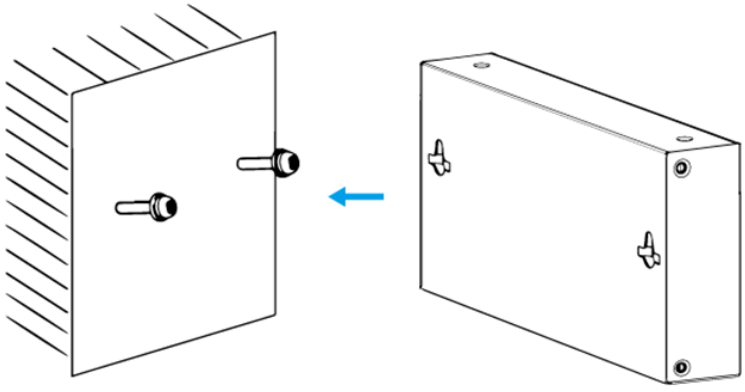
3.3 Wall Mount

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 same as the distance between the wall-mount holes.

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



4 Wiring

4.1 Connecting GND

GND cables do not come with the package of select models. Purchase them as needed.

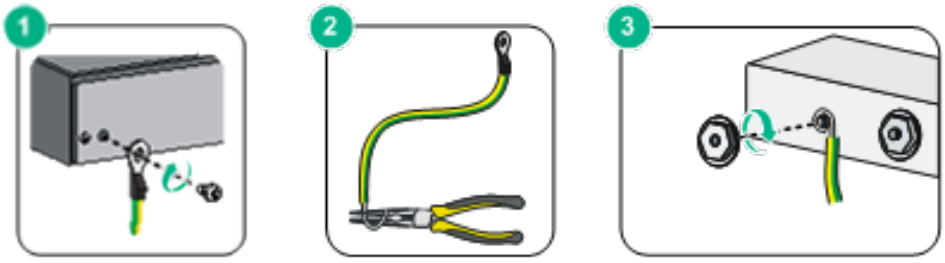
Grounding the Device can protect it against lightning and interference. The steps for connecting the GND are as follows:

Step 1 Remove the ground screw from the Device and pass the ground screw through the round hole of the OT terminal of the ground cable. Turn the ground screw clockwise with a cross screwdriver to fasten the OT terminal of the ground cable.

Step 2 Wind the other end of the ground cable into a circle with the needle-nose pliers.

Step 3 Connect the other end of the ground cable to the ground bar, then turn the hex nut clockwise with a wrench to fasten the other end of the ground cable to the ground terminal.

Figure 4-1 Connect GND



4.2 Connecting Power Cord

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

Step 1 Connect one end of the power cord to the power jack of the Device.

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

4.3 Connecting Ethernet Port

The Ethernet port is a standard RJ-45 port. With its self-adaptation function, it can be automatically configured to full duplex/half-duplex operation mode. It supports MDI/MDI-X self-recognition of the cable, allowing you to use a cross-over cable or straight-through cable to connect the terminal device to the network device.

Figure 4-2 Ethernet port pin number

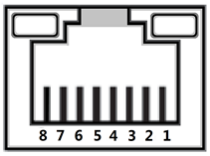
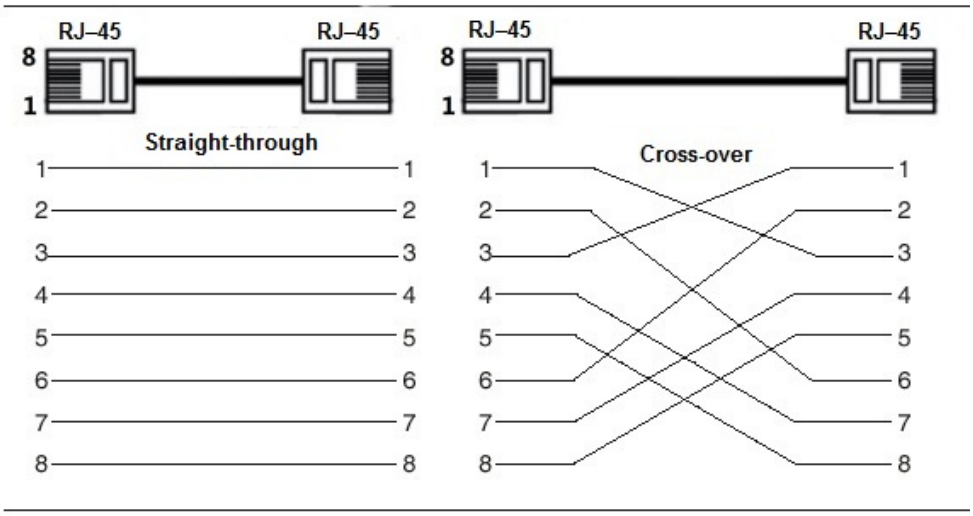


Figure 4-3 Pin description



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

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.