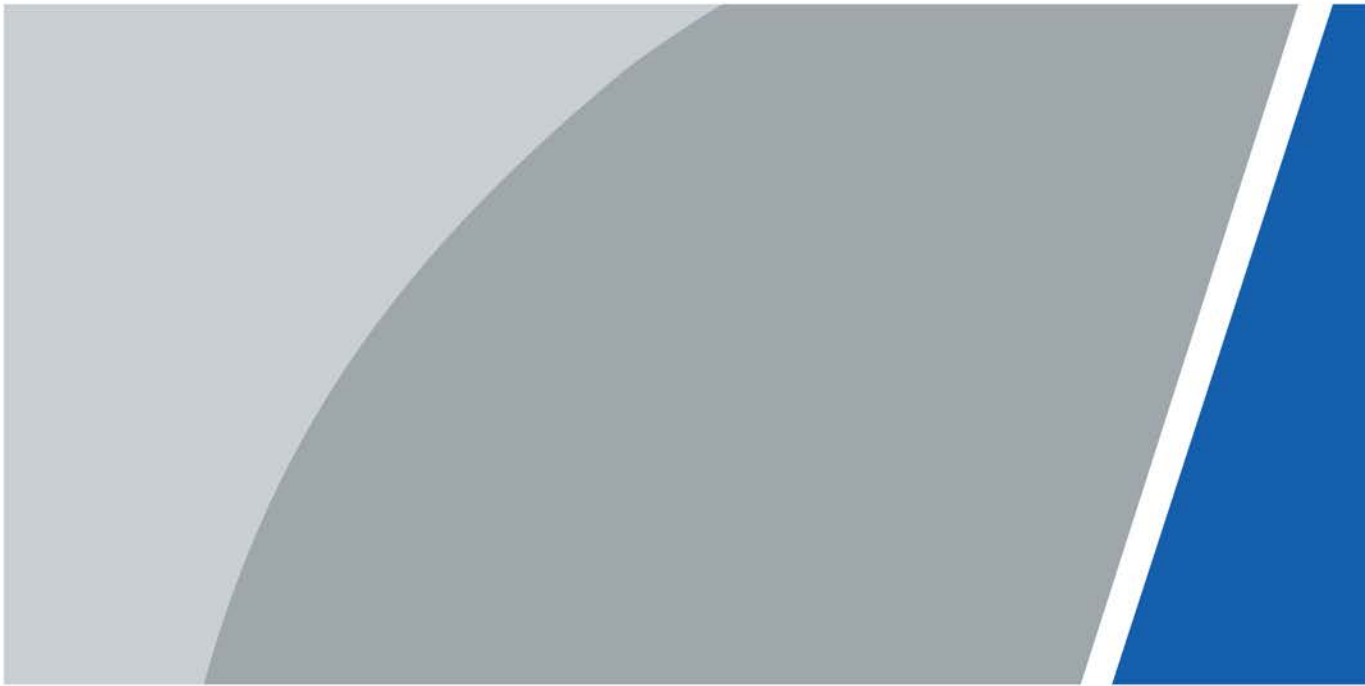# PoE Switch (16/24-port Managed Desktop Switch)

Quick Start Guide

V1.0.1

Foreword

General

This manual mainly introduces the hardware, installation, and wiring steps of the 16/24-port managed desktop switch (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, 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
V1.0.1	Updated the long distance description.	August 2023
V1.0.0	First release.	August 2021

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, 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

⚠ WARNING

- 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.
- Make sure the device is in horizontal installation, and install the device on solid and flat surface to avoid falling down.
- Use the power adapter or case power supply provided by the device manufacturer.
- Voltage stabilizer and lightning protection device are optional according to power supply and surrounding environment.
- 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.
- When replacing the battery, make sure that the same type is used. Improper battery use might result in explosion.

Table of Contents

1 Overview

1.1 Introduction

The Device is a layer-2 commercial switch. It provides a high-performance switching engine and large buffer memory to ensure smooth video stream transmission. With a full-metal design, the Device has great heat dissipation capabilities on its shell surface, and is able to work in environments that range from –10 ℃ (14 ℉) to +55 ℃ (+131 ℉). With its DIP design, it provides a variety of work modes that suit different scenarios. The Device also supports power consumption management, which allows it to adapt to fluctuations in the power consumption of terminal devices. This ensures stable operation. With web management, SNMP and other functions, the Device can be remotely managed. It can directly connect to iLinksView.

The Device is applicable for use in different scenarios, including homes, offices, small malls and on server farms.

1.2 Features

- 16/24 × 100 Mbps PoE Ethernet ports, uplink ports support gigabit optical ports or Ethernet ports.
- All ports meet the requirements of IEEE802.3af and IEEE802.3at standards. The red ports also conform with Hi-PoE and IEEE802.3bt standards, and the orange ports conform with Hi-PoE standard.
- 250 m long-distance PoE transmissions, which can be configured on the web.

  📖

  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.
- PoE watchdog for real-time detection of terminal device status, which can be configured on the web.
- Supports STP, RSTP, and MSTP.
- IEEE802.1Q-based VLAN configuration.
- Manual link aggregation and static LACP.
- Desktop mount and rack mount.

2 Port and Indicator

2.1 Front Panel

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

Figure 2-1 Front panel
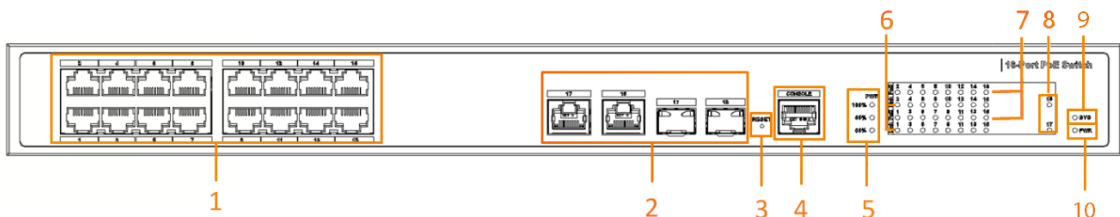
Following are all the ports and indicators on the front panel of the 16/24-port managed desktop switch. Your actual device might only have some of them.

Table 2-1 Description of the front panel

No.	Description
1	10/100 Mbps self-adaptive PoE Ethernet ports.
2	Uplink port, including 10/100/1000 Mbps self-adaptive Ethernet ports and 1000 Mbps optical port.
3	Reset button. Press and hold it for more than 5 seconds, and release after the panel status indicators all turn on to restore the device to its default settings.
4	Console port.
5	PoE output power indicators. ● Solid green: Total power ≤ 50%. ● Solid green and yellow: 50% < total power ≤ 80%. ● Solid green, yellow and red: 80% < total power.
6	Single-port connection status indicators (Link). ● On: Connected to device. ● Off: Not connected to device.
7	PoE port status indicators. ● On: Powered by PoE. ● Off: Not powered by PoE.
8	Uplink port connection status indicators (Link). ● On: Connected to device. ● Off: Not connected to device.
9	System status indicator (SYS). ● Flashing: Operation is normal. ● Off: Operation is not normal.
10	Power indicator. ● On: Power on. ● Off: Power off.

2.2 Rear Panel

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

Figure 2-2 Rear Panel

Table 2-2 Description of the rear panel

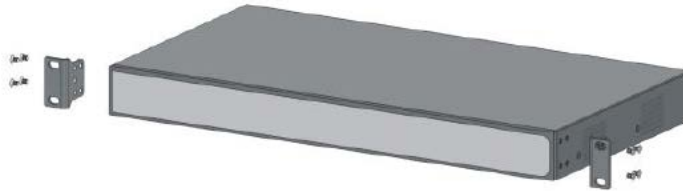| No.	Description
1	Power switch.
2	Power port, supports 100–240 VAC.
3	Ground terminal.

3 Installation

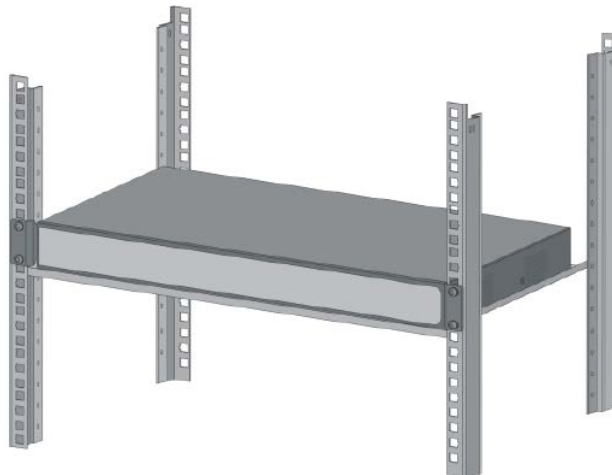The Device supports rack mount.

Step 1   Attach the mounting bracket to the Device side panel (one on each side) and secure it with the screws provided with the rack.

Figure 3-1 Install bracket

Step 2   Attach the Device to the rack with screws.

Figure 3-2 Install device

4 Wiring

4.1 Connecting GND

Grounding the Device can protect it against lightning and interference.

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
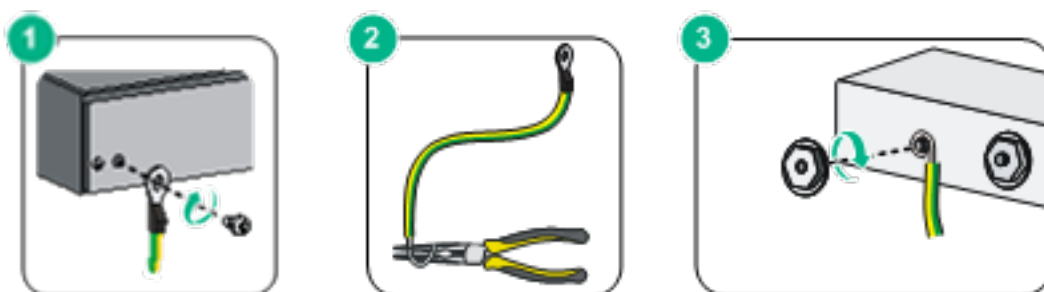
4.2 Connecting Power Cord

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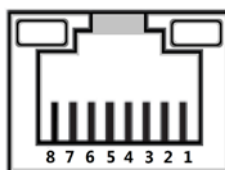
The cable connection of RJ-45 connector conforms to the 568B standard (1-orange white, 2-orange, 3-green white, 4-blue, 5-blue white, 6-green, 7-brown white, 8-brown).

Figure 4-3 Connect cable
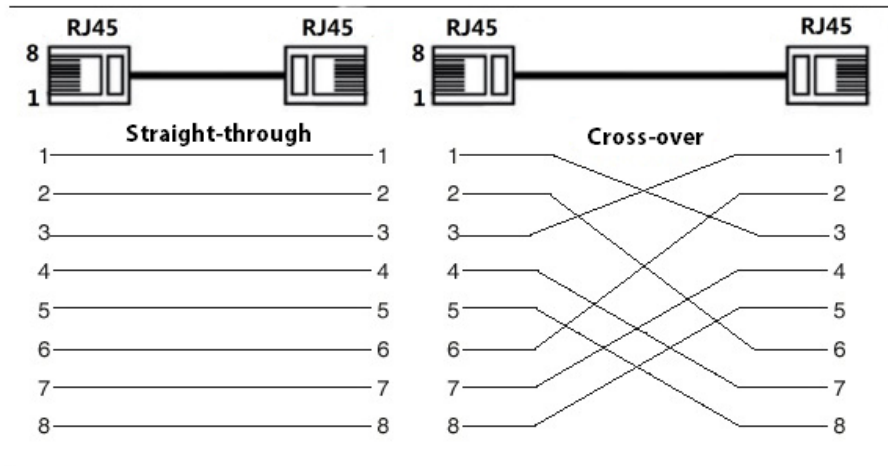
4.4 Connecting SFP Ethernet Port

⚠️ WARNING

- When installing the SFP optical module, do not touch the gold finger of the SFP optical module.
- Do not remove the dust plug of the SFP optical module before connecting the optical fiber.
- Do not directly insert the SFP optical module into the slot while the optical fiber is inserted in it. Unplug the optical fiber before installing it.

Step 1   Wear the antistatic wrist band, and confirm that the antistatic wrist band is in good contact with your skin and the Device is reliably grounded.

Step 2   Turn up the handle of the SFP optical module vertically and hold the optical module on both sides with your hands.

Step 3   Push the optical module gently into the slot in the horizontal direction until the SFP optical module is firmly connected to the slot.

Figure 4-4 Install SFP module
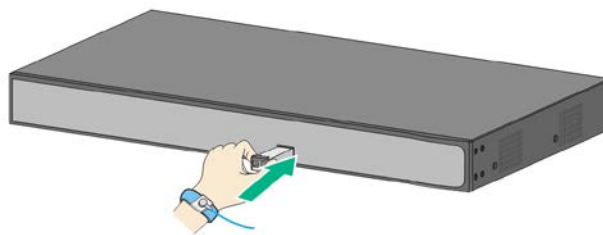
Step 4   Remove the dust cap of the LC connector of the optical fiber and the dust plug of the SFP optical module.

Step 5   Connect the LC connector of the optical fiber to the SFP optical module.

Figure 4-5 Connect optical fiber
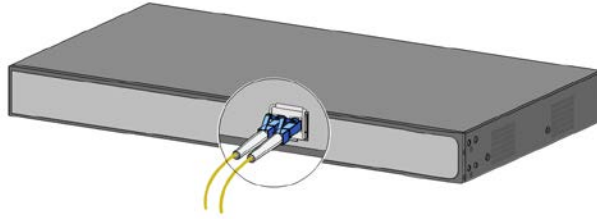
4.5 Connecting PoE Ethernet Port

If the terminal device has a PoE Ethernet port, you can directly connect this port to the Device PoE Ethernet port through the network cable to achieve synchronized network connection and power supply. The maximum distance between the Device and the terminal device is about 100 m.

⚠️

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

5 Quick Operation

5.1 Login through Web

You can log in to the Device through the web for management and operation. For details, see web operation manual.

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

Table 5-1 Default factory configuration

Parameter	Description
IP address	192.168.1.110/255.255.255.0
Username	admin
Password	● Web: No initial password, user-defined during initialization. ● iLinksView: lt_91_il_02_nmp. When using iLinksView for device management, ensure that the username and password of the Device matches that of iLinksView, otherwise iLinksView will not be able to discover the Device.

5.2 Restoring to Factory Settings

There are two ways to restore the Device to factory settings.
● Press and hold the **Reset** button for 5 seconds to restore the Device to factory settings.
● Log in to web or use command line. For details, see the web operation manual or command line reference manual.

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:

2. **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.

3. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

4. **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.

5. **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.

6. **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.

7. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

8. **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.

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 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.

13. **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.

14. **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.