

Ethernet Switch (Industrial Managed Switch)

Quick Start Guide








Foreword

General

This manual mainly introduces the hardware, installation, wiring steps, and quick configurations of the industrial managed 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, 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 Port and Indicator | 2 |
| 2.1 Front Panel | 2 |
| 2.2 Side Panel | 4 |
| 3 Installation | 5 |
| 4 Wiring | 6 |
| 4.1 Connecting GND | 6 |
| 4.2 Connecting Power Cord | 6 |
| 4.3 Connecting SFP Ethernet Port | 8 |
| 4.4 Connecting Ethernet Port | 9 |
| 4.5 Connecting PoE Ethernet Port | 10 |
| 4.6 Connecting Alarm Terminal | 10 |
| 4.7 Connecting RS-485 Terminal | 11 |
| 4.8 Connecting Console Port | 11 |
| 5 Quick Operation | 13 |
| 5.1 First Login through Console Port | 13 |
| 5.2 Login through Web | 14 |
| 5.3 Restoring to Factory Settings | 14 |
| Appendix 1 Cybersecurity Recommendations | 15 |

1 Overview

1.1 Introduction

The device is designed for on-site transmission and application in severe environment. Equipped with high performance switching engine and large buffer memory, it features low transmission delay and high reliability. The solid and sealed all-metal case design and efficient surface heat dissipation make it can work in the environment from $-40\text{ }^{\circ}\text{C}$ to $+75\text{ }^{\circ}\text{C}$. The protection for power input end overcurrent, overvoltage and EMC can effectively resist the interference from static electricity, lightning, and pulse. The dual power backup guarantees stable operation for the system. With Telnet, 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 corridors and offices.

1.2 Features

- All-gigabit port design. Uplink port includes two forms: Ethernet port and optical port.
- All ports meet the requirements of IEEE802.3af and IEEE802.3at standards. The red ports also conform to Hi-PoE and IEEE802.3bt standards, and the orange ports conform to Hi-PoE standard.
- 250 m long-distance PoE transmission (10 Mbps).
- PoE watchdog (available for models with PoE Ethernet port).
- Supports STP, RSTP, and MSTP.
- IEEE802.1Q-based VLAN configuration.
- Manual link aggregation and static LACP.
- Wide voltage design.
- Desktop mount and DIN-rail mount.

2 Port and Indicator

2.1 Front Panel

The following figures are for reference only, and might differ from the actual product.

Figure 2-1 Front panel (with PoE port)

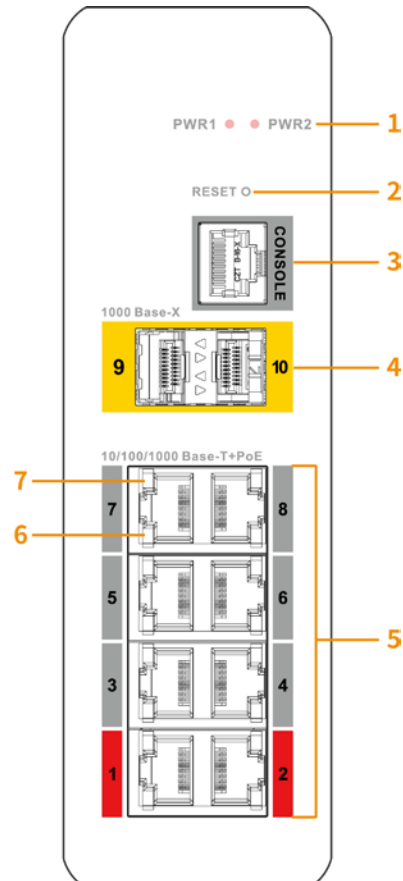
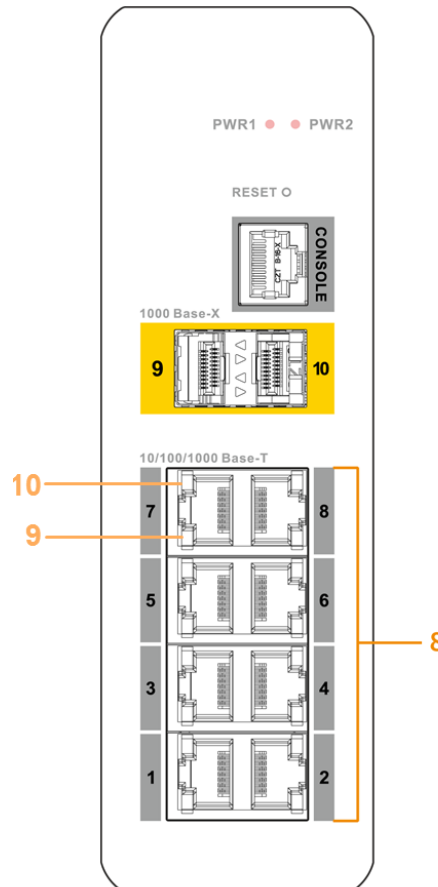


Figure 2-2 Front panel (without PoE port)



The following are all the ports and indicators on the front panel of the industrial managed switch. The actual device may only have a part of them.

Table 2-1 Description of front panel

| No. | Description |
|-----|---|
| 1 | Power Indicator. <ul style="list-style-type: none"> ● Green: Normal power connection. ● Red: Abnormal power connection. |
| 2 | Reset button. Press and hold it for more than 5 s, and release after the panel status indicators are all on to restore the device to default settings. |
| 3 | Console port. |
| 4 | 1000 Mbps optical port. |
| 5 | 10/100/1000 Mbps adaptive PoE port. |
| 6 | Single-port connection or data transmission status indicator (Link/Act). <ul style="list-style-type: none"> ● On: Connected to device. ● Off: Not connected to device. ● Flashes: Transmitting data. |
| 7 | Single-port PoE status indicator. <ul style="list-style-type: none"> ● On: Powered by PoE. ● Off: Not powered by PoE. |
| 8 | 10/100/1000 Mbps Ethernet port. |

| No. | Description |
|-----|---|
| 9 | Single-port data transmission status indicator (Act). <ul style="list-style-type: none"> Flashes: Transmitting data. Off: No data transmission. |
| 10 | Single-port connection status indicator (Link). <ul style="list-style-type: none"> On: Connected to device. Off: Not connected to device. |

2.2 Side Panel

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

Figure 2-3 Side panel

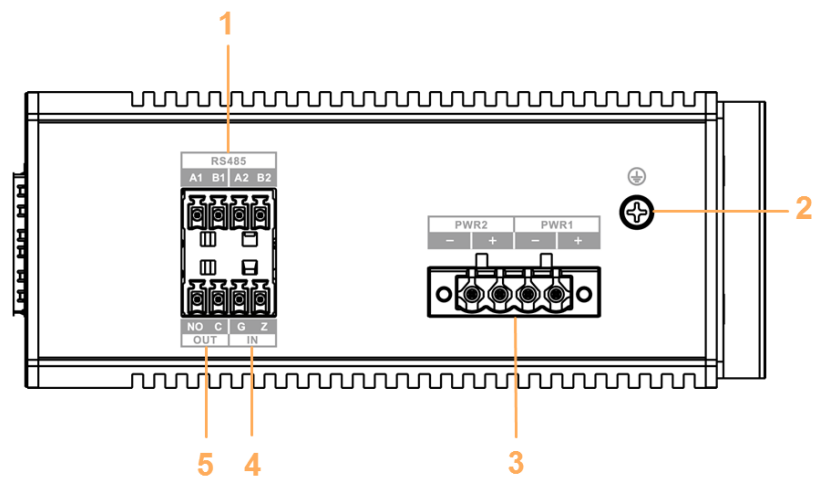


Table 2-2 Port description

| No. | Description |
|-----|--------------------------------|
| 1 | RS-485 port |
| 2 | GND screw |
| 3 | Power port (dual power backup) |
| 4 | Alarm input port |
| 5 | Alarm output port |

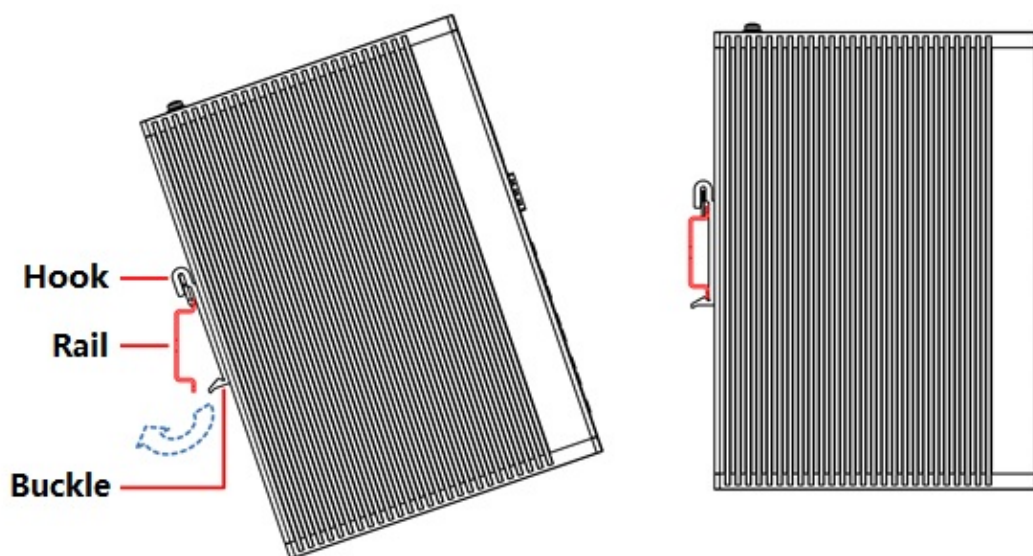
3 Installation

The device supports DIN-rail mount. Hang the switch hook on the rail, press the switch to make the buckle stuck into the rail.



The width of the guide rail supported by the device is 50 mm.

Figure 3-1 DIN rail

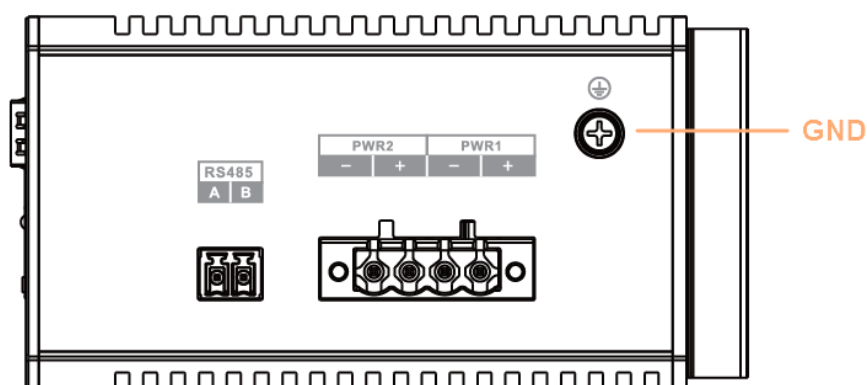


4 Wiring

4.1 Connecting GND

Device GND connection helps ensure 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.

Figure 4-1 GND port



- Step 1** Remove the GND screw at the enclosure GND with a cross screwdriver.
- Step 2** Connect one end of the GND cable with the cold-pressed terminal, and fix it on the enclosure GND with the GND screw.
- Step 3** Connect the other end of the GND cable to the ground.



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

4.2 Connecting Power Cord

Redundant power input supports two-channel power, which are PWR2 and PWR1. You can select the other power for continuous power supply when one channel of power breaks down, which greatly improves the reliability of network operation.



WARNING

To avoid personal injury, do not touch any exposed wire, terminal and areas with danger voltage of the device and do not dismantle parts or plug connector during power on.



- Before connecting power, make sure that the power supply conforms to the power supply requirements on the device label. Otherwise, it might cause device damage.
- We recommend using an isolated adapter to connect the device.



The sectional area of power cable shall be more than 0.75 mm^2 (max sectional area 2.5 mm^2); ground resistance is required to be less than 4Ω .

Figure 4-2 Power terminal

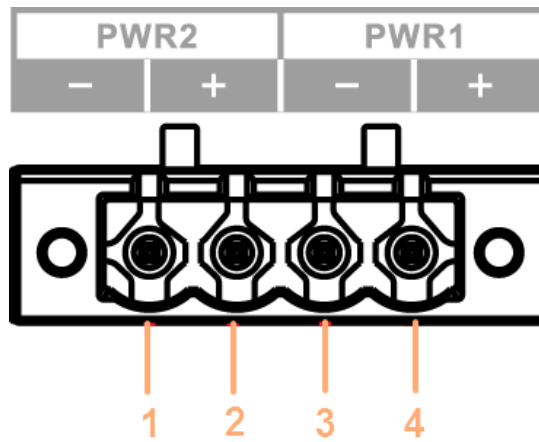


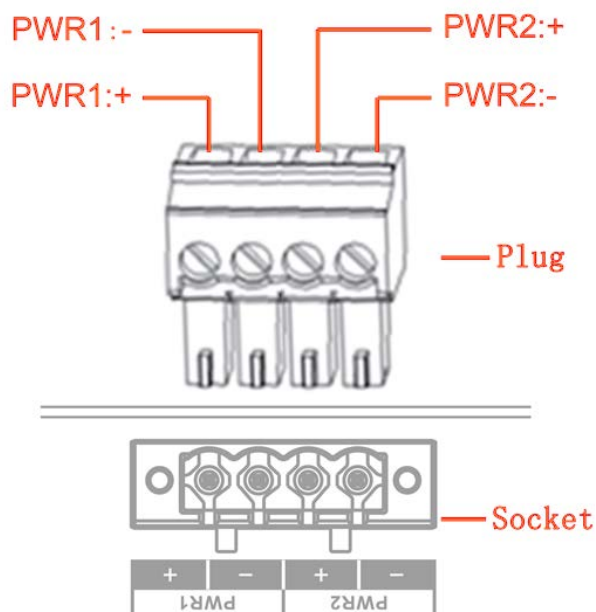
Table 4-1 Power terminal description

| No. | Signal Name | DC Wiring Definition |
|-----|-------------|----------------------|
| 1 | - | PWR2- |
| 2 | + | PWR2+ |
| 3 | - | PWR1- |
| 4 | + | PWR1+ |

The operation steps of connecting power terminal plug and socket are shown as follows.

- Step 1** Connect the device to ground.
- Step 2** Take off the power terminal plug from the device.
- Step 3** Insert one end of the power cable into the power terminal plug according to the requirement.

Figure 4-3 Fix the power cable



- Step 4** Insert the plug which is connected to power cable back to the corresponding power

terminal socket of the device.

- Step 5** Connect the other end of power cable to the corresponding external power supply system according to the power supply requirement marked on the device, and check if the corresponding power indicator light of the device is on, it means power connection is correct if the light is on.



The device supports 48 V–57 V DC. Please confirm if the power supply conforms to the requirement marked on the device before connecting to power, which is to avoid causing damage to the device.

4.3 Connecting SFP Ethernet Port

We recommend wearing antistatic gloves before installing SFP module, and then wear antistatic wrist, and confirm the antistatic wrist is well linked to the surface of the gloves.

- Step 1** Lift the handle of SFP module upward vertically and make it get stuck to the top hook.

- Step 2** Hold the SFP module on both sides and push it gently into the SFP slot till the SFP module is firmly connected to the slot (You can feel that both the top and bottom spring strip of the SFP module are firmly stuck with the SFP slot).



WARNING

The device uses laser to transmit signal via optical fiber cable. The laser conforms to the requirements of level 1 laser products. To avoid injury upon eyes, do not look at the 1000 Base-X optical port directly when the device is powered on.



- 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 port.
- Do not directly insert the SFP optical module with the optical fiber inserted into the slot. Unplug the optical fiber before installing it.

Figure 4-4 SFP module structure

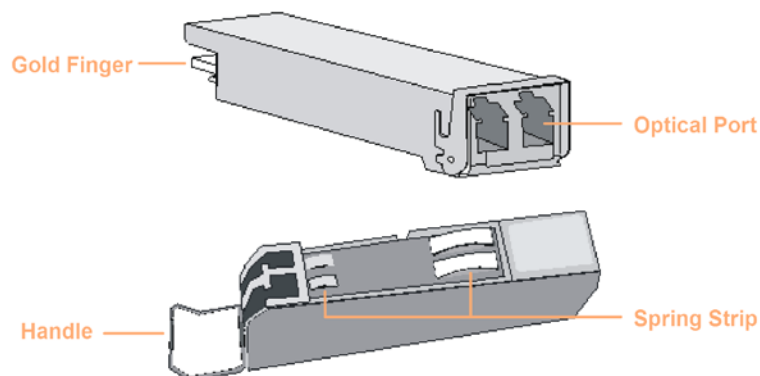
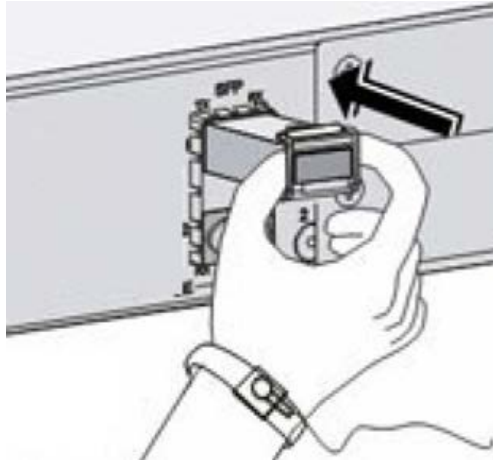


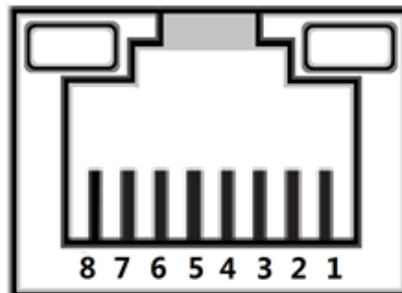
Figure 4-5 SFP module installation



4.4 Connecting Ethernet Port

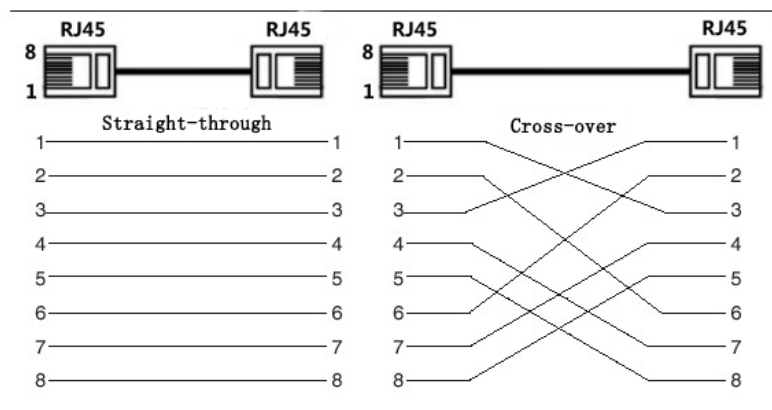
Ethernet port is a standard RJ-45 port. With self-adaptation function, it can be automatically configured to full duplex/half-duplex operation mode. It supports MDI/MDI-X self-recognition of the cable, therefore, you can use cross-over cable or straight-through cable to connect terminal device to network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

Figure 4-6 Ethernet port pin number



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).

Figure 4-7 Cable connection



4.5 Connecting PoE Ethernet Port

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

4.6 Connecting Alarm Terminal

The alarm terminal is located on the side panel of the device, which is used for alarm input and output. When the device detects the alarm input signal (alarm in low level), it will switch the alarm output terminal for a short time (after the alarm out level is raised for 5 s, it will be lowered again).

Figure 4-8 Alarm terminal



C pin is a normally open switch, and NO pin is a normally closed switch. When the device is working, the C pin is closed and the NO pin is disconnected. When an alarm occurs, the C pin is disconnected and the NO pin is closed.

Table 4-2 External port electrical parameters

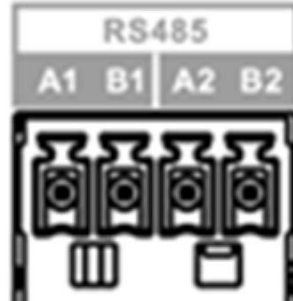
| Parameter | Value |
|--|-----------------|
| Max. voltage | 125V AC/ 60V DC |
| Max. current | 2A |
| Max. power | 60W |
| Max. insulation and voltage resistance | 2kV |

- Step 1** Take off the alarm terminal plug from the device.
- Step 2** Insert the two wires of the alarm terminal into plugs of alarm terminal according to the description above, and fix the wires firmly.
- Step 3** Insert the alarm terminal plug which is connected to cable back to the corresponding alarm terminal socket of the device.

4.7 Connecting RS-485 Terminal

The RS-485 data conversion port is located on the side panel of the device. There are two groups in total. Each group can independently convert between RS-485 data and Ethernet data (tcp/udp).

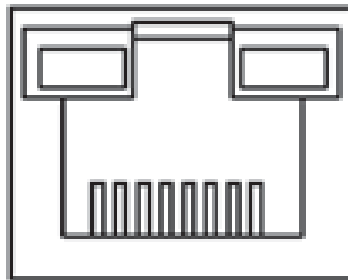
Figure 4-9 RS-485 terminal



4.8 Connecting Console Port

Use RJ-45 to DB-9 cable to connect the device console port and 9-pin serial port on your PC. Operating the hyper terminal software of the Windows system can call the console software of the device. Through the console software, you can configure, manage, and maintain the device.

Figure 4-10 Console port



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

Figure 4-11 Cable sequence

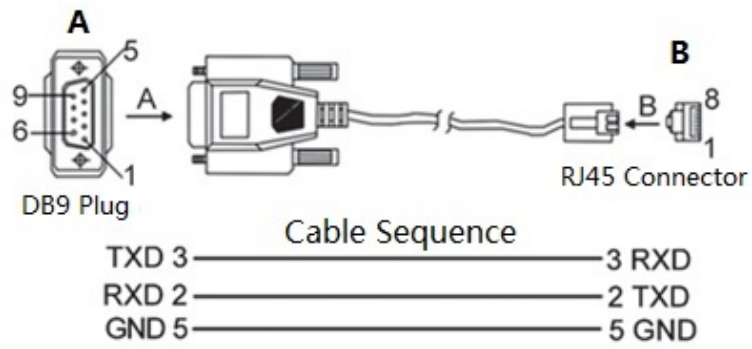


Table 4-3 Port pin description

| DB9 Pin | RJ-45 Pin | Signal | Description |
|---------|-----------|--------|----------------|
| 2 | 3 | RXD | Receive data. |
| 3 | 2 | TXD | Transmit data. |
| 5 | 5 | GND | Ground. |

5 Quick Operation

5.1 First Login through Console Port

You can log in to the local interface through the console port.

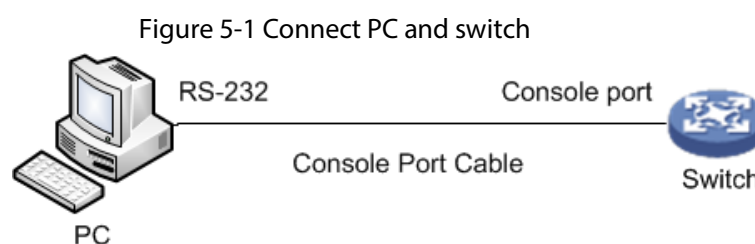
Step 1 Power off the PC.

Step 2 Use default console port cable to connect PC and device. First insert the DB-(hole) plug of console port cable into the 9-pin serial port of PC, and then insert the RJ-45 plug into the console port of the device.

1. Insert the DB-(hole) plug of console port cable into the 9-pin serial port of PC.
2. Insert the RJ-45 plug into the console port of the device.



- Confirm the sign on the port during connection, in case it may plug into the wrong port.
- Plug out RJ-45 and then DB-9 when removing console port cable.



Step 3 Power on the PC.

Step 4 Run terminal simulation program on the PC.

Step 5 Select the serial port which is to connect the device, set the terminal communication parameters. The parameter value has to be in accordance with the value on the device, the default is shown as follows.

- Baud rate: 115200
- Data bit: 8
- Stop bit: 1
- Parity: None
- Flow control: None



If the PC uses Windows Server 2003 operating system, add hyper terminal program in the Windows component and then log in the manage the device according to the way introduced in this manual; If PC uses Windows Server 2008, Windows Vista, Windows 7 or other operating systems, please prepare third-party terminal control software, refer to the software operation guide or online help for operation method.

Step 6 After powering on the device, the device self-check information is displayed on the terminal program.

Step 7 Enter username and press Enter.

Step 8 Enter password and press Enter.

The command line prompt (SWITCH#) is displayed, as shown in the following figure.

```
Press ENTER to get started
```

```
Username: admin
```

```
Password:
```

```
SWITCH#
```

Step 9 (Optional) Enter corresponding command to configure the device or check device operating status.



You can enter ? anytime if you need help.

5.2 Login through Web

You can log in to the device through 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 | <ul style="list-style-type: none">• Web: admin• iLinksView : lt_91_il_02_nmp <p>When using the iLinksView to manage the device, note that the username and password must be the same as that you have set in the iLinksView, otherwise the iLinksView cannot discover the device.</p> |

5.3 Restoring to Factory Settings

There are two ways to restore the device to factory settings.

- Press and hold the **Reset** button for 5 s 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

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.