



dahua L3 Managed PoE Switch User Guide

[Home](#) » [Dahua](#) » dahua L3 Managed PoE Switch User Guide 

dahua L3 Managed PoE Switch



Contents

1 Foreword

1.1 General

1.2 Safety Instructions

1.3 Revision History

1.4 Privacy Protection Notice

1.5 About the Manual

2 Important Safeguards and Warnings

2.1 Transportation Requirements

2.2 Storage Requirements

2.3 Installation Requirements

2.4 Operation Requirements

2.5 Maintenance Requirements

3 Device Installation

3.1 Installation Notes

3.2 Installation Tools

3.3 Mounting Methods

3.4 Installation

4 Port Description

5 Appendix 1 FAQ

6 Appendix 2 Specifications

7 Appendix 3 Cybersecurity Recommendations

8 Documents / Resources

9 Related Posts






Foreword

General

This manual introduces the installation, functions and operations of L3 Managed PoE Switch. Read carefully before using the device, and keep the manual safe for future reference.

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, 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
V1.0.0	First release.	September 2022

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, comply with the guidelines when using it, and keep the manual safe for future reference.

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 electric safety standards.
- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not leave outdoor models of the device hanging in the air or facing outwards when installing onto poles that are on top of buildings.



- Do not place the device in a place exposed to sunlight or near heat sources.
- Place the device in a well-ventilated place, and do not block its ventilation.
- Use an adapter or chassis power supply from the manufacturer.
- 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.
- Outdoor models of the device must be securely installed on poles or brackets that are perpendicular to the ground. Make sure the entire surface of the device and all its related components are covered with anti-oxidation coating (such as rust preventive paint), and that the installation site and height of the device meet the requirements of the plan.
- Install outdoor models of the device on top of buildings where there is little to no direct sunlight to avoid the device becoming overheated. Make sure to take all necessary measures to protect the device.
- Face the side with the Ethernet port downwards, and arrange the wires in a downward direction when installing outdoor models of the device.

Operation Requirements



WARNING

- 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 running the device.
- When removing the cable device first to avoid personal injury.
- Do not unplug the power cord on the side of the device when the adapter is powered on.



- Use the device under allowed humidity and temperature conditions.
- Operating temperature: 0 °C to +45 °C (+32 °F to +113 °F).
- This is a class B product. In a domestic environment this may cause radio interference in which case you may be required to take adequate measures.

Maintenance Requirements



WARNING

- Do not disassemble it unless necessary.
- Power off the device before maintenance.
- Mark key components on the maintenance circuit diagram with warning signs.

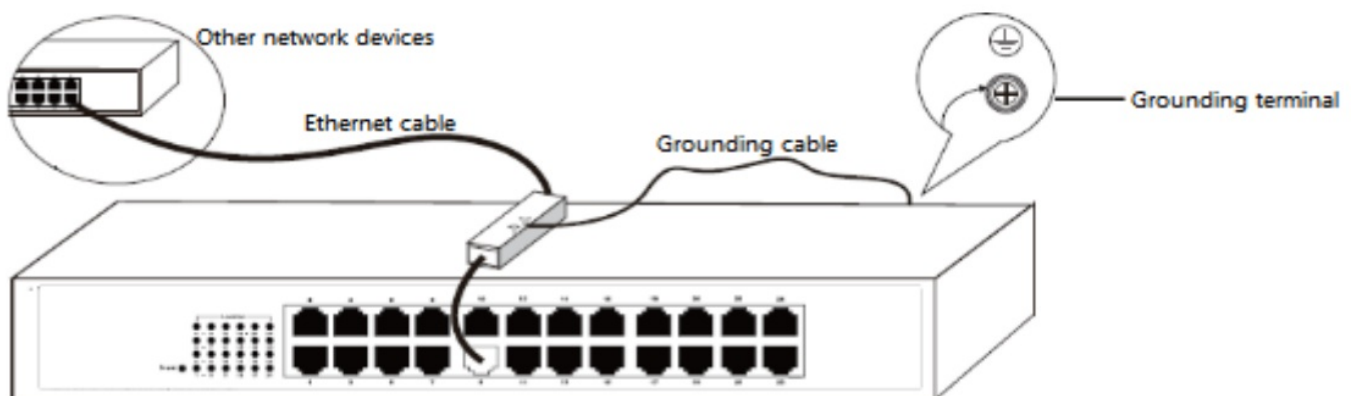
Device Installation

Installation Notes

Follow the notes below to avoid device damages or personal injuries caused by mis-operation:

- Wear the ESD bracelet or gloves before installation and do not power on the switch before finishing installation.
- Use the included power cord to supply power to the switch.
- Make sure that the input voltage matches the value of the switch specified in this manual.
- Do not block any ventilation openings.
- Do not remove the housing of the switch.
- Keep the air in the ambient environment clean. Regularly perform dedusting.
- Disconnect the switch from the power supply before cleaning it. Do not scrub the switch with any liquid. Clean only with dry cloth.
- Position the switch away from power line, electric lamp, or power system.
- Do not place any heavy things on this switch.
- If outdoor cabling is required, we recommended you deploy a port lightning arrester (see the following figure for connection method) or AC power supply lightning arrester.

Figure 1-1 Installation diagram



There is a void sticker covering one of the screws on the housing of the switch. Do not remove the sticker without permission from the local agent.

Installation Tools

- Desktop mount: ESD bracelet (or gloves).
- Rack mount: ESD bracelet (or gloves), Phillips screwdriver, and screws.

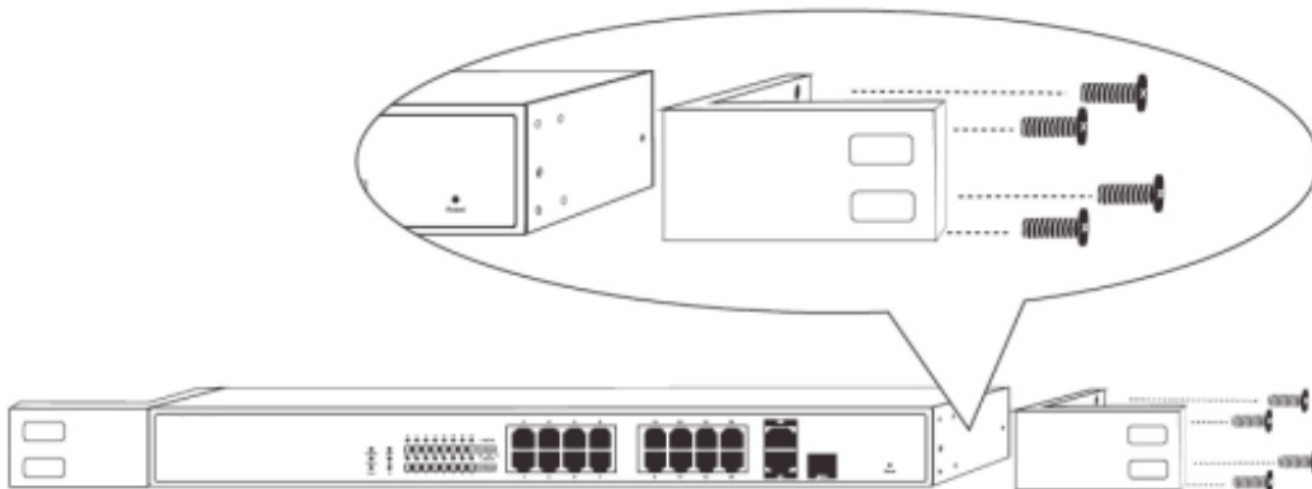
Mounting Methods

Rack Mount

Step 1 Ensure that the subrack is stable and level, and is properly grounded.

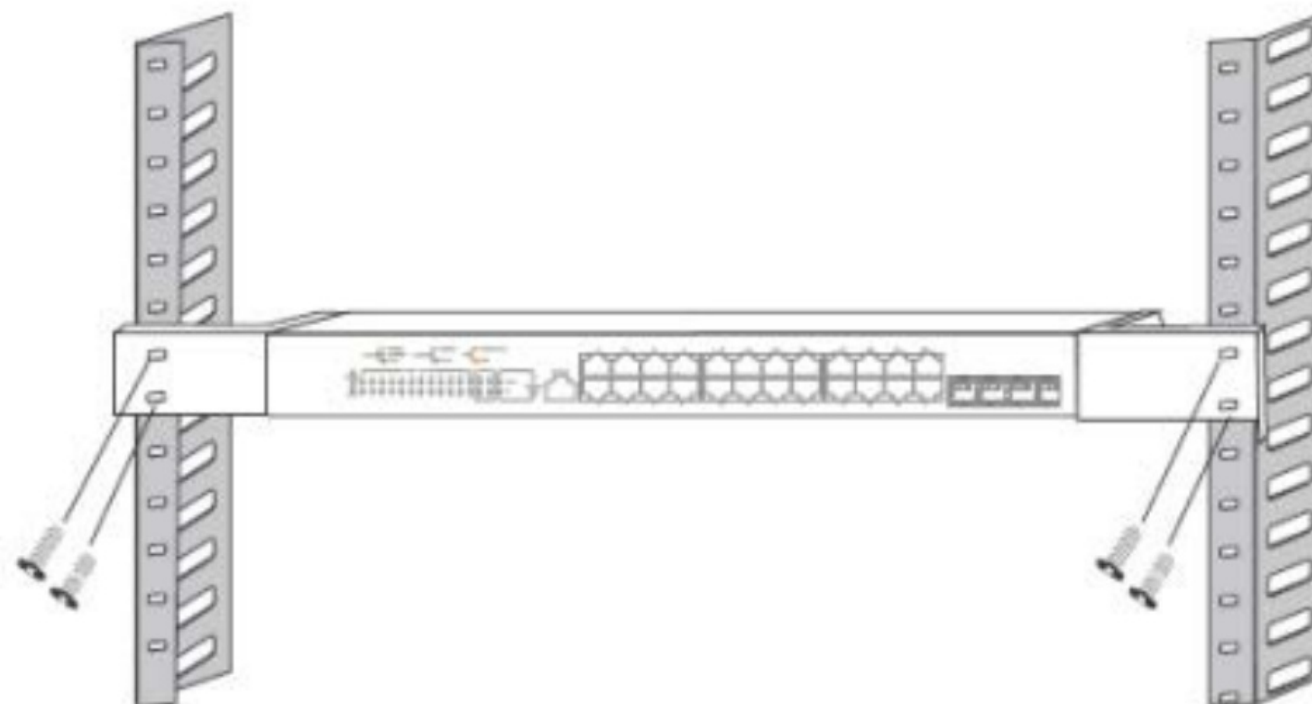
Step 2 Attach the L-shaped brackets to the switch with screws.

Figure 1-2 Fix the brackets



Step 3 Mount the switch at a proper height on the sub rack, and then fix it with screws.

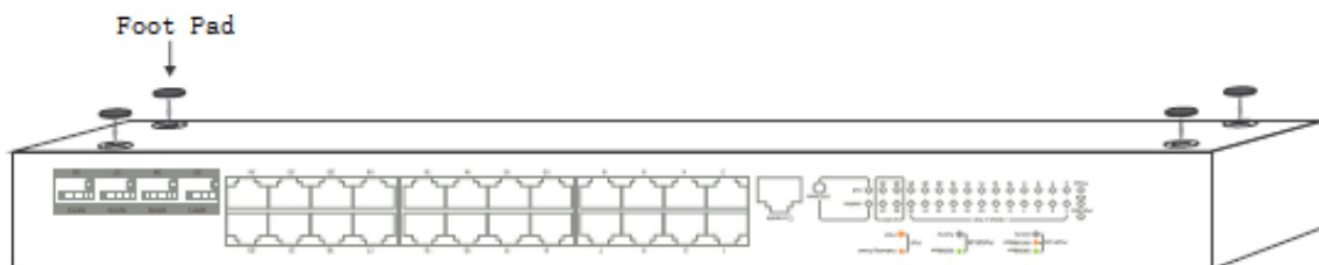
Figure 1-3 Mount the switch



Desktop Mount

Paste the four footpad stickers to the corresponding four recesses on the bottom of the switch. Place the switch up on a clean, stable and flat desktop.

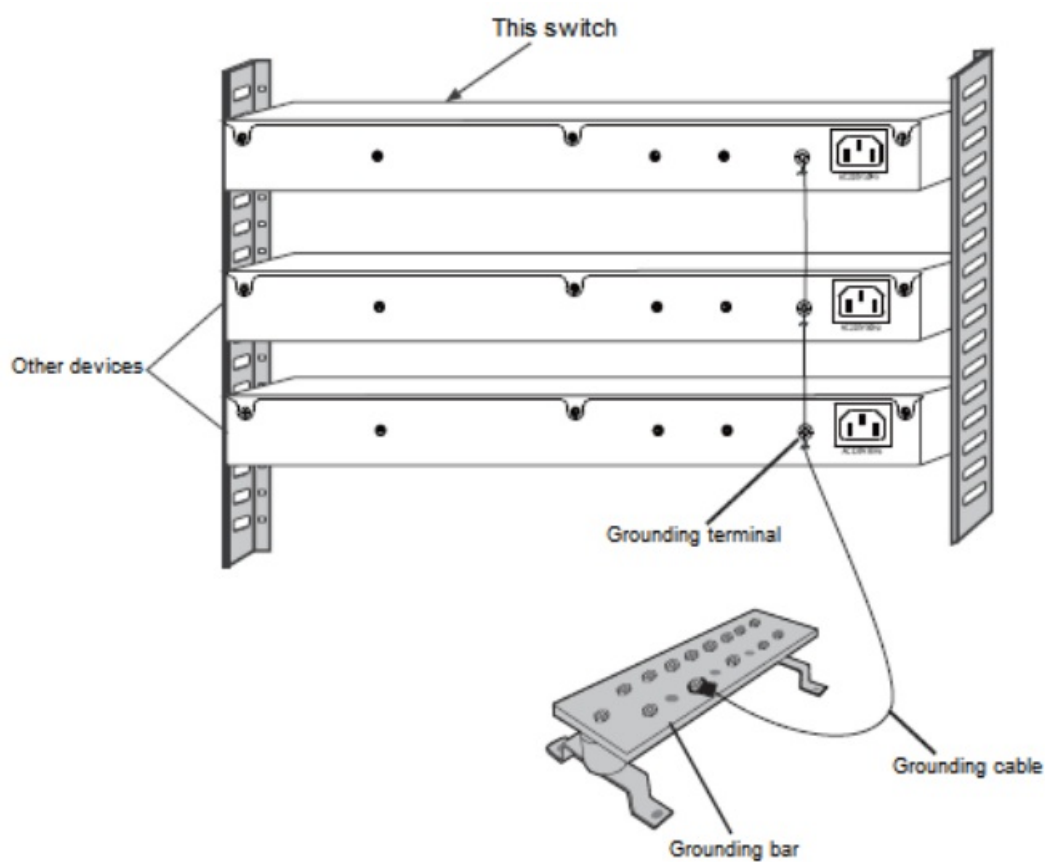
Figure 1-4 Paste the footpad



Installation

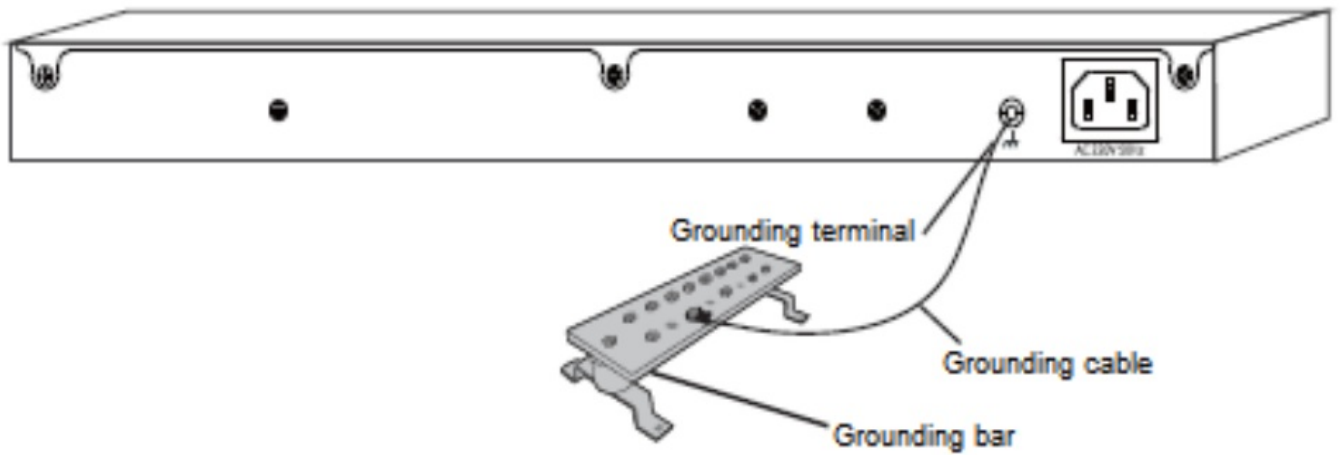
Step 1 Connect one side of the grounding cable to the grounding terminal of the switch.

Figure 1-5 Connect the grounding cable (1)



Step 2 Connect the other side of the grounding cable to the grounding terminal of other grounded devices or a grounding bar.

Figure 1-6 Connect the grounding cable (2)



Connect the grounding cable to the grounding system in the equipment room. Do not connect it to a fire main or lightning rod.

Port Description

Refer to the following network topology to connect the switch to other network devices.

Figure 2-1 Network topology

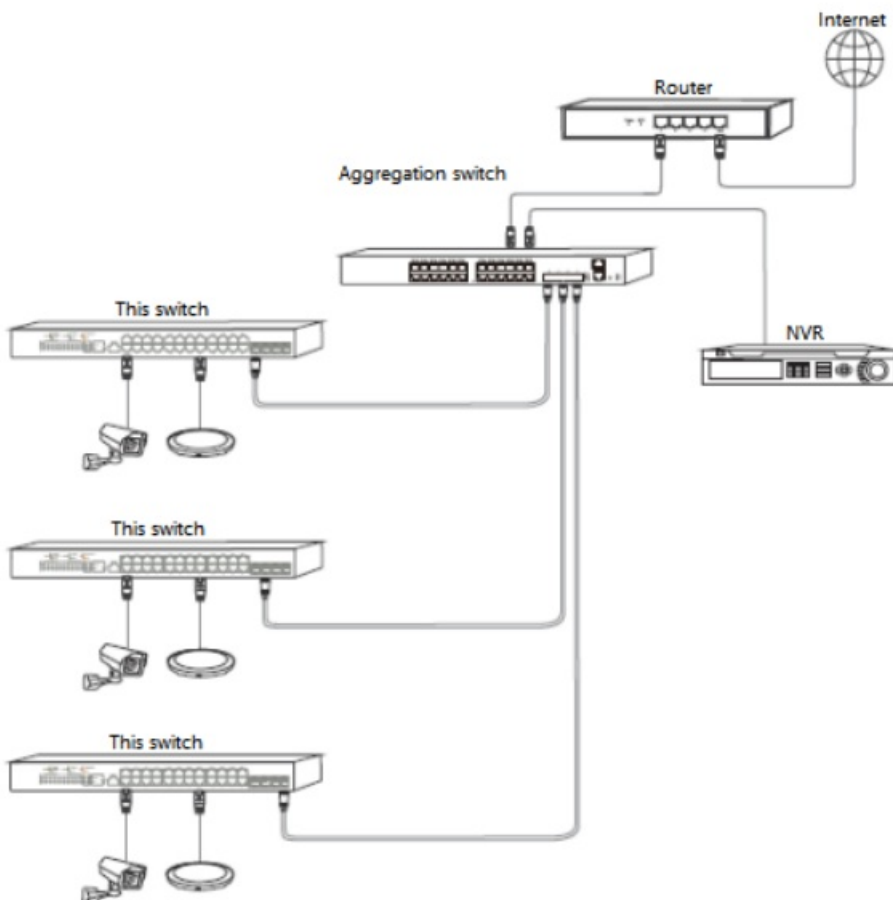


Table 2-1 Description of Indicators and buttons

Indicator	Description
-----------	-------------

PoE-Max	<ul style="list-style-type: none"> • Solid on: The total output power of the switch reaches the maximum value. • Off: The total output power of the switch does not reach the maximum value.
SYS	<ul style="list-style-type: none"> • Flashing: The system works properly. • Solid on: The system is not working properly. • Off: The system is starting up or not working properly.
Power	<ul style="list-style-type: none"> • Solid on: The switch is powered on properly. • Off: The switch is not powered on, or not powered on properly.
Link/Act or PoE	<p>Indicator of Link/Act and PoE. It indicates the connection status or PoE power supply status of RJ45 ports based on the status of the LED Mode button. When the Link/Act indicator is solid on, the descriptions of the Link/Act or PoE indicators are shown as follows:</p> <ul style="list-style-type: none"> • Solid on: The corresponding port is connected to a network device, but no data is being transmitted over the port. • Flashing: Data is being transmitted over the corresponding port. • Off: The corresponding port is not connected or is not connected properly. <p>Green light indicates that the negotiation speed of the corresponding port is 1000 Mbps, and orange light indicates a rate of 10 Mbps or 100 Mbps. When the PoE indicator of LED Mode is solid on, the descriptions of the Link/Act or PoE indicators are shown as follows:</p> <ul style="list-style-type: none"> • Solid orange: The corresponding port supplies PoE power to a device properly. • Flashing orange: The corresponding port is not supplying PoE power to a device properly. • Off: The corresponding port does not supply PoE power.
Link/Act	<ul style="list-style-type: none"> • Solid on: The corresponding port is connected, but no data is being transmitted over the port. • Flashing: Data is being transmitted over the corresponding port. • Off: The corresponding port is not connected or is not connected properly.

LED/RESET	<p>This multipurpose button is for both indicator converting button and reset button.</p> <ul style="list-style-type: none"> • Press the LED/RESET button to convert the mode of the Link/Act or PoE indicator. <ul style="list-style-type: none"> ◦ When the Link/Act indicator of LED/RESET is solid on, the Link/Act or PoE indicator is in the Link/Act mode. ◦ When PoE indicator of LED/RESET is solid on, the Link/Act or PoE indicator is in the PoE mode. • When the Power indicator is solid on and the SYS indicator is flashing, press and hold the LED Mode button for about 10 seconds, and release it when all indicators light up. The switch is restored to factory settings when the Power indicator is solid on and the SYS indicator flashes again.
-----------	--



All ports of this switch support the auto MDI/MDIX function, so both a straight cable and a crossover cable can be used to connect the switch to Ethernet devices.

Appendix 1 FAQ

1. I cannot log in to the webpage of the switch.

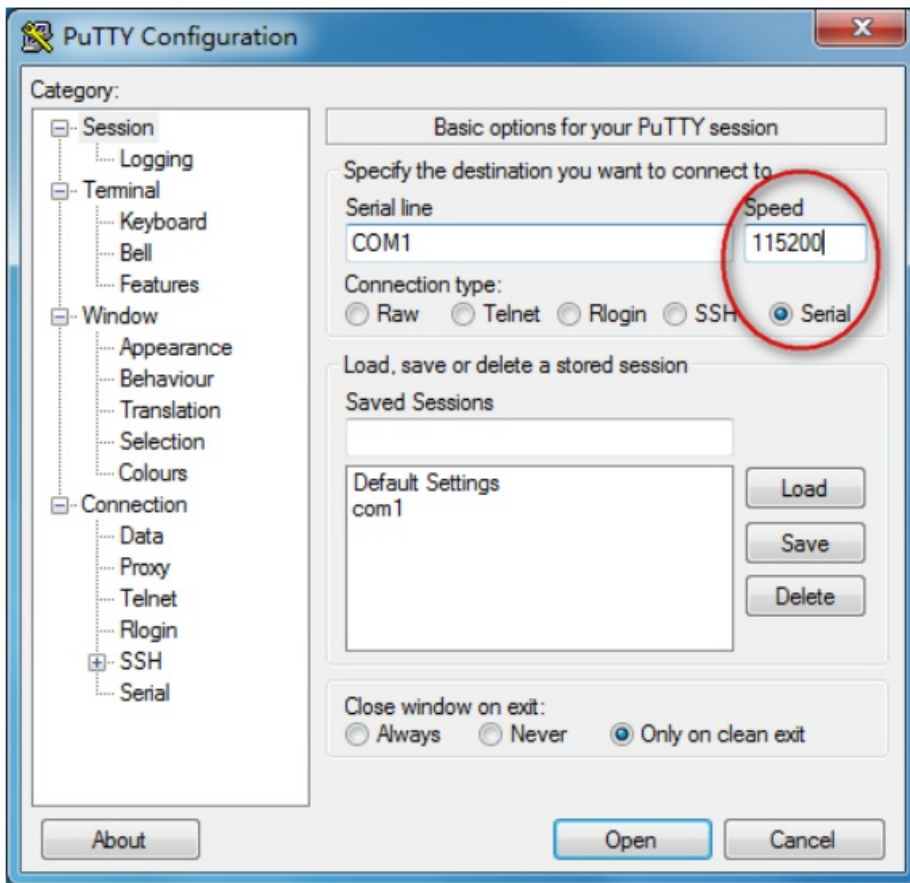
Try the following solutions:

- Check whether the switch is powered on properly.
 - Check whether the computer is connected to the switch properly.
 - Check whether the IP address of the computer is set to 192.168.1.X (X ranges from 2 to 254 and is not be occupied).
 - Clear the cache of the web browser or try another web browser.
 - Disable the firewall of the computer, or try another computer.
 - Check whether only one device with the IP address 192.168.1.110 exists in the local network.
 - If the problem persists, reset the switch and try again. Reset method: When the Power Indicator is solid on and the SYS Indicator is flashing, press and hold the LED Mode button for about 10 seconds, and release it when all Indicators light up. The switch is restored to factory settings when the SYS Indicator flashes again.
2. I forget the login username and password when logging in to the webpage. Try entering the default login username and password (both are admin). If you fail, reset the switch, and then use the default username and password to log in.
3. How to connect to the switch through the Console port?

Follow the procedures below:

- a. Use the included console cable to connect a computer to the Console port of the switch.
- b. Run the connection software of console port on the computer. Putty is taken as an example. Set the Connection type to Serial, Speed to 115200, and click Open on the lower right corner.

Appendix Figure 1-1 PuTTY configuration



c. Double press Enter on your keyboard, and then enter the username and password (both are admin by default) of the switch in the appeared window.

Appendix Figure 1-2 Enter username and password



4. How to deal with power system malfunctions?

You can determine whether the power system malfunctions by observing the power indicator on the front panel of the switch. When the power system works properly, the power indicator is solid on. If the power indicator does not light up, perform the following operations:

- Check whether the switch is properly connected to a power source using the included power cord.
- Check whether the input voltage matches the value required by the switch.

Appendix 2 Specifications

Name		Description
Port	Number of 10/100/1000 Mbps RJ45 port	24
	Number of 1000 Mbps SFP port	4 independent SFP ports
	Console port	1 Baud rate: 115200
Performance	Exchange mode	Store-and-forward
	MAC address table learning	Auto aging, auto learning
	MAC address table	16 K
PoE	PoE standard	IEEE 802.3af, IEEE 802.3at
	PoE power cable core	8 cores: voltage of cores 1, 2, 4, 5 is +, and cores 3, 6, 7, 8 is –
	PoE port	1 to 24
	Maximum output power of a single port	30 W
	Maximum output power of the switch	370 W
Dimensions (L × W × H)		440 mm × 284 mm × 44 mm
Input power		100–240 VAC, 50/60 Hz, 6 A
Lightning protection	RJ45 port	Common mode: 6 kV
	Power	Common mode: 6 kV; Differential mode: 4 kV
Operating environment		Temperature: 0 °C– 45 °C (+32 °F to +113 °F). Humidity : (10%–90%) RH, non-condensing.
Data transmission rate		Ethernet: 10 Mbps (half duplex)/20 Mbps (full duplex) Fast Ethernet: 100 Mbps (half duplex)/200 Mbps (full duplex) Gigabit Ethernet: 2000 Mbps (full duplex)
Transmission media		Ethernet: CAT3 UTP/STP or better Fast Ethernet: CAT5 UTP/STP or better Gigabit Ethernet : CAT5e or CAT6 UTP/STP
Standard		IEEE 802.3, IEEE 802.3u, IEEE 802.3x, IEEE 802.3z, IEEE 802.3ab, IEEE 802.1d, IEEE 802.1p, IEEE 802.1q, IEEE 802.1w, and IEEE 802.1s

Appendix 3 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 from Dahua 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.

Documents / Resources

	dahua L3 Managed PoE Switch [pdf] User Guide PFS4218-16GT-230, PFS4218-16GT-230, L3 Managed PoE Switch, PoE Switch, L3 PoE Switch, Managed PoE Switch
---	--