MPT320 Accessories

Quick Start Guide

V1.0.0

Foreword

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 Date
V1.0.0	First release.	October 2020

Important Safeguards and Warnings

This chapter introduces the contents covering proper handling of the device, hazard prevention, and prevention of property damage. Read these contents carefully before using the device, comply with them when using, and keep the manual well for future reference.

Operating requirements

- Do not place and install the Terminal in an area exposed to direct sunlight or near heat generating device.
- Keep the Terminal away from dampness, dust or soot.
- Install the Terminal horizontally or in a stable place to prevent it from falling.
- Do not drip or splash liquid onto the Terminal, and make sure that there is no object filled with liquid on the Terminal to prevent liquid from flowing into it.
- Operate the product within the rated range of power input and output.
- Do not dissemble the product.
- Transport, use and store the product under the allowed humidity and temperature conditions.

Electrical Safety

- Improper battery use might result in fire, explosion, or inflammation.
- When replacing battery, make sure that the same model is used!
- Use the power adapter provided with the Parking Detector; otherwise, it might result in people injury and device damage. The charging base supports PoE power supply (12V, 2A).

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 jurisdictions. For detailed information, refer to 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, 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 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 occurring when using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Table of Contents

Foreword ..... **I**
Important Safeguards and Warnings ..... **II**
1 Camera **1**
1.1 Appearance 1
1.2 Installation 2
1.3 Video/Capture 3
2 Charging base **5**
2.1 Appearance 5
2.2 Functions 6
3 Leather Holster **7**
3.1 Appearance 7
3.2 Installation 7
Appendix 1 Cybersecurity Recommendations **8**

1 Camera

1.1 Appearance

Shoulder Camera

Figure 1-1 Shoulder camera (1)

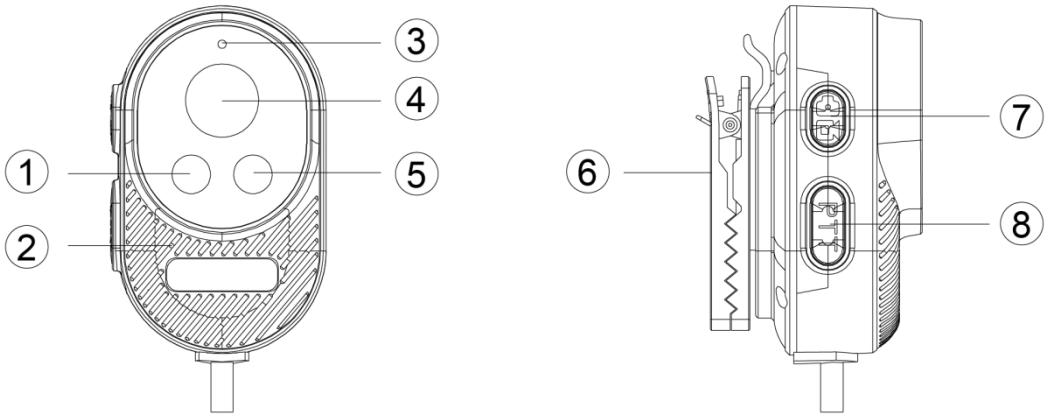
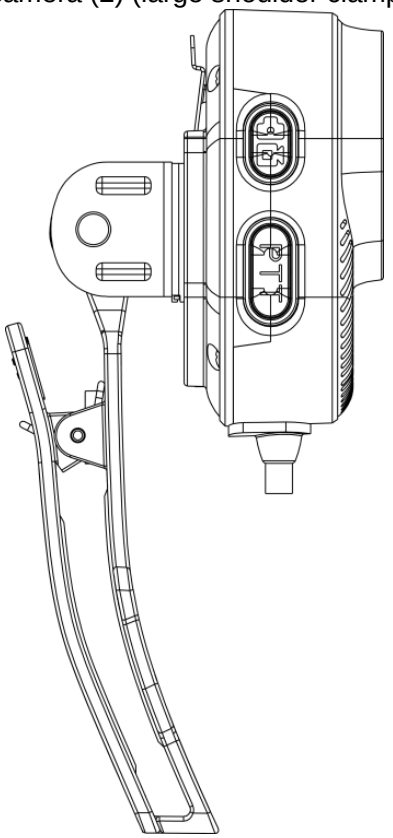


Table 1-1 Introduction of shoulder camera

No.	Name	Description
1	IR LED	Auto switch with the brightness change.
2	MIC	Acquires audio signal.
3	LED indicator	● On: Powered on. ● Flashing: Recording videos.
4	Lens	Captures pictures and videos.
5	Light sensor	Controls IR LED.
6	Shoulder clamp	Fixes the camera on the chest, shoulder, or collar.
7	Video/Capture button	Press to take picture.
		Press and hold to start recording.
8	Voice talk button	Works with voice talk app of host group, press the button to start voice talk, and release the button to receive audio.

Figure 1-2 Shoulder camera (2) (large shoulder clamp is optional)



Helmet Camera

Figure 1-3 Helmet camera

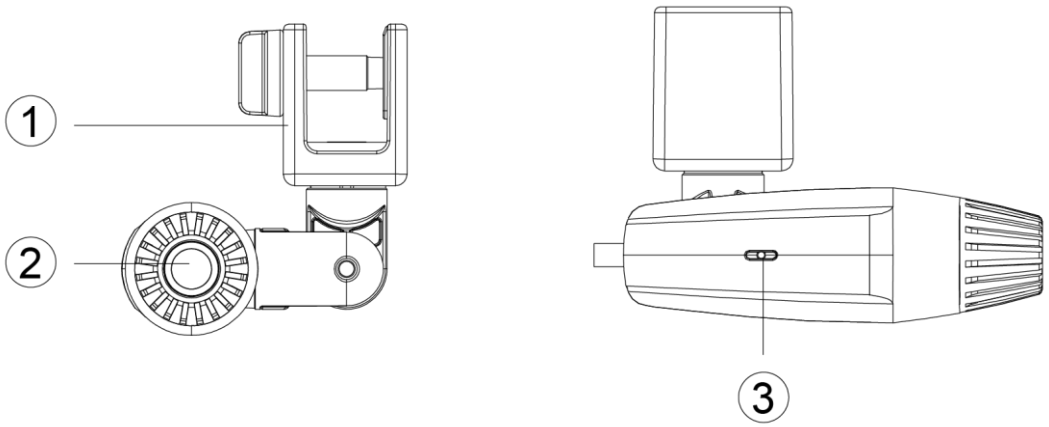


Table 1-2 Introduction of helmet camera

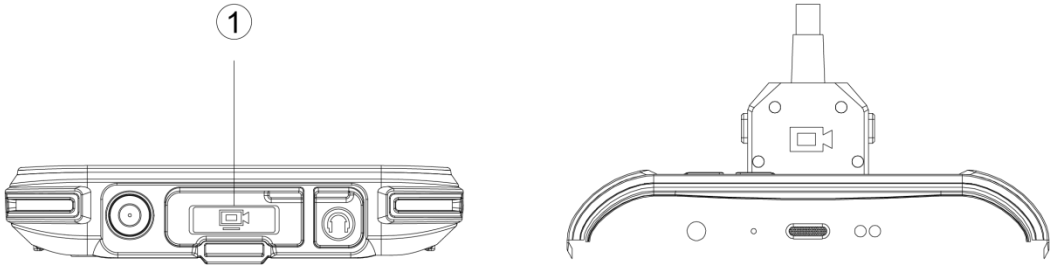
No.	Name	Description
1	Helmet clamp	Fixes the camera on helmet.
2	Lens	Captures videos and pictures.
3	MIC	Acquires audio signal.

1.2 Installation

Connect the camera to the terminal through the peripheral port ①.

- Press the snap joints at the two sides to take out the camera.
- Take out the camera when it is not in use to avoid power consumption.
- Do not twine the cable on the host to avoid cable aging.

Figure 1-4 Peripheral port



For helmet camera, install the camera at the right side of the helmet.

Figure 1-5 Installation of helmet camera

1.3 Video/Capture

Press and hold the video/capture button to start recording, or tap  on the main interface to go to **Video/Capture** interface**.** Tap the camera icon to select the external camera, and then click  to capture pictures and record videos.

Figure 1-6 Video/Capture

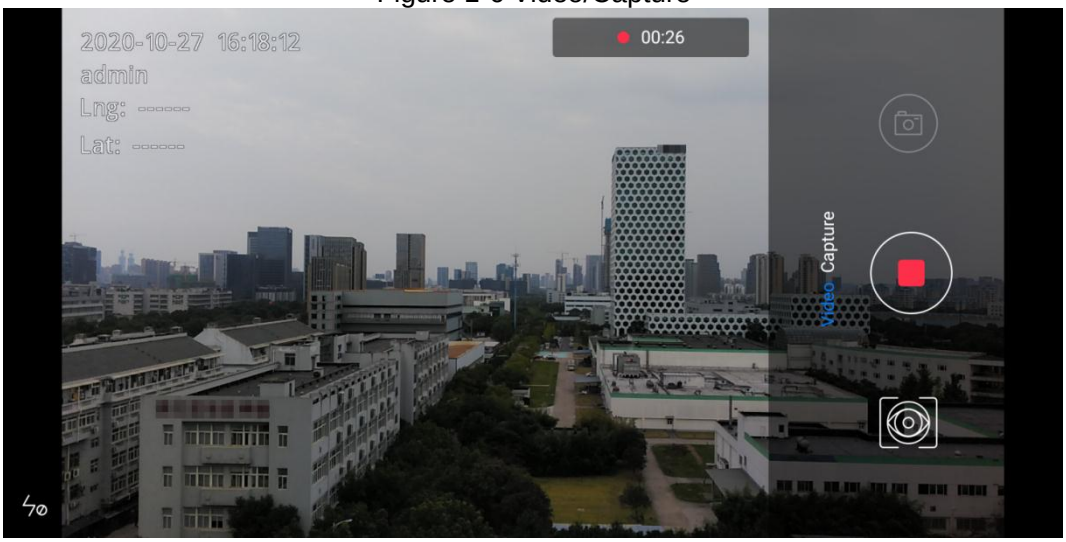


Table 1-3 Icons

Icons	Descriptions
	Tap the icon to select the camera. ●  : Rear camera. ●  : Front-facing camera. ●  : External camera.
	●  : Start recording. ●  : Stop recording.
	Capture picture.

2 Charging base

2.1 Appearance

Figure 2-1 Charging base

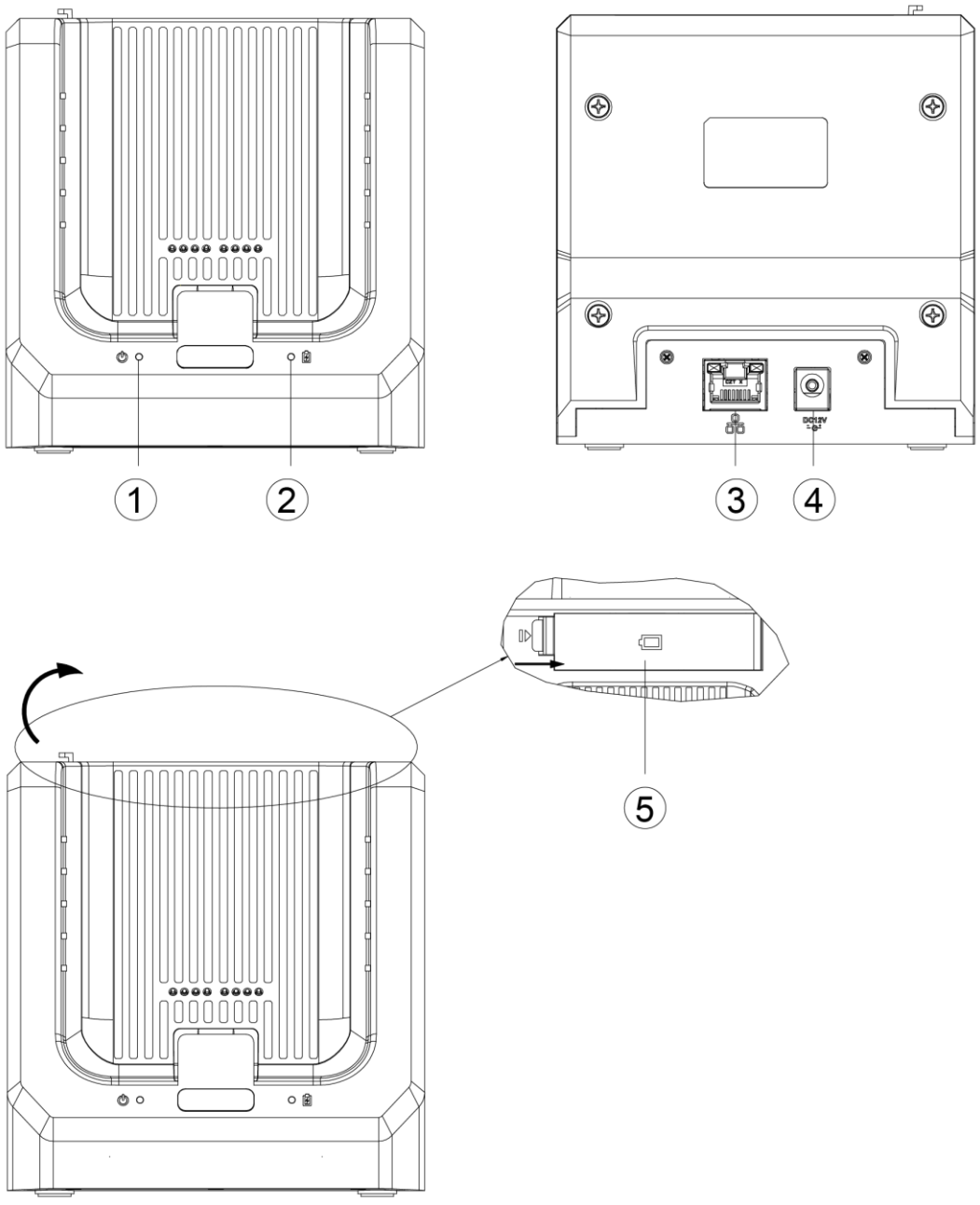


Table 2-1 Introduction of charging base

No.	Name	No.	Name
1	Power indicator	4	12V DC power input
2	Battery charging indicator	5	Battery cover
3	Ethernet port	—	—

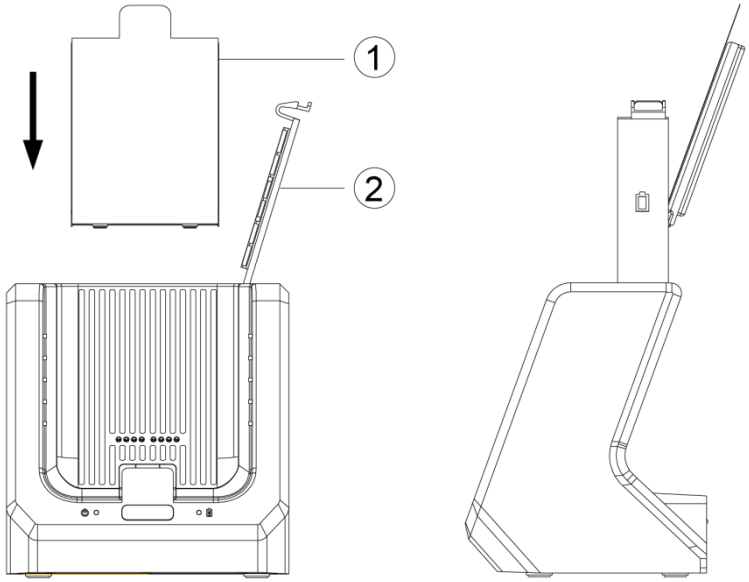
2.2 Functions

Step 1 Insert the mobile portable terminal to the external charging base (do not hit against the probe), and connect the base to power through the 12V DC power input port and PoE network cable to charge the terminal.

- When the power indicator light grows red, it indicates that the base is powered on.
- When the battery charging indicator light grows red, it indicates that the battery is being charged; when the indicator light grows green, it indicates that the charging finished.

Step 2 Open the battery cover ①, and then put in the battery ② for charging.

Figure 2-2 Install the battery



Step 3 On the **Pedestal Connection Settings** interface, tap **Enable**, and then set the IP address which can be obtained automatically or entered manually. You can connect the terminal MPT320 to the Internet for data transmission.

- If the terminal cannot be charged through charging base, check whether the contact point on the bottom of the terminal is dirty. If yes, clear the contact point and try again.
- Do not shock the base to avoid poor contact.
- For details, see the corresponding user's manual.

3 Leather Holster

3.1 Appearance

Figure 3-1 Leather holster

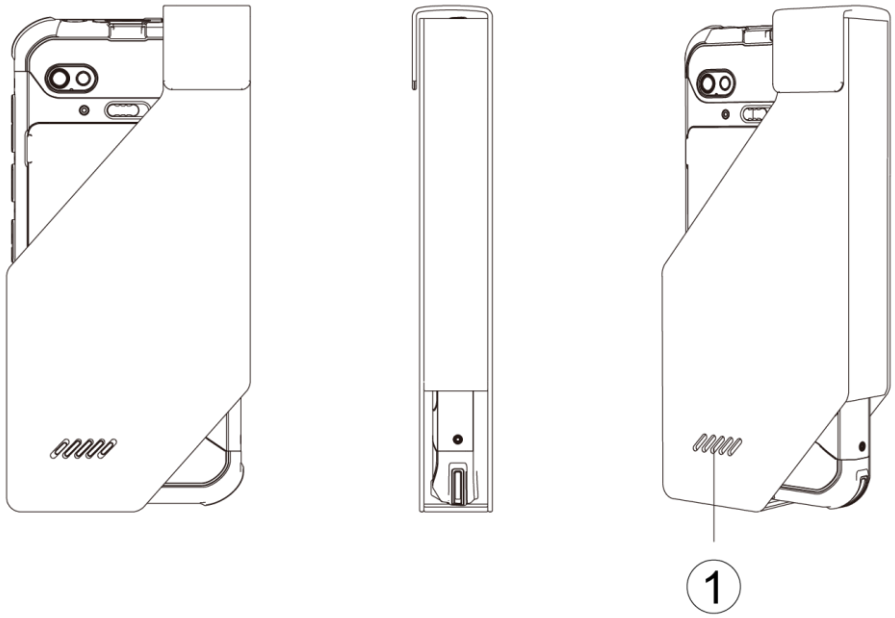


Table 3-1 Introduction of laser holster

No.	Name
1	Speaker position.

3.2 Installation

Step 1 Put the terminal into the leather holster.
Make sure that the speaker of the terminal is on the speaker position of holster, so that the speaker can work normally.

Step 2 Wear the leather holster on the belt.

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.