

8-Port ePoE Switch

User's Manual








Foreword

General

This manual introduces the installation, functions and operations of the 8-Port ePoE switch (hereinafter referred to as "the device"). 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.	February 2023

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, and comply with the guidelines when using it.

Transportation Requirements



Transport the device under allowed humidity and temperature conditions.

Storage Requirements



Store the device under allowed humidity and temperature conditions.

Installation Requirements



- Do not connect the power adapter to the device while the adapter is powered on.
- Strictly comply with the local electrical safety code and standards. Make sure that the ambient voltage is stable and meets the power supply requirements of the device.
- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.



- Do not place the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.
- Put the device in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the device label.
- 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.

Operation Requirements



- 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 use.
- Make sure the device is powered off before disassembling wires to avoid personal injury.
- Do not unplug the power cord on the side of the device while the adapter is powered on.



- Use the device under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the device, and make sure that there is no object filled with liquid on the device to prevent liquid from flowing into it.
- This is a class A product. In a domestic environment this may cause radio interference in which case you may be required to take adequate measures.
- Do not block the ventilator of the device with objects, such as a newspaper, table cloth or curtain.
- Do not place an open flame on the device, such as a lit candle.

Maintenance Requirements.



- Power off the device before maintenance.
- Mark key components on the maintenance circuit diagram with warning signs.

Table of Contents

Foreword	I
Important Safeguards and Warnings	III
1 Overview	6
1.1 Introduction.....	6
1.2 Features.....	6
1.3 Typical Application.....	7
2 Structure	8
2.1 Front Panel.....	8
2.2 Rear Panel.....	9
2.3 PoE Power Supply.....	9
3 Installation	10
Appendix 1 ePoE Power Supply Specifications (CAT)	11
Appendix 2 ePoE Power Supply Specifications (RG59 Coaxial Cable)	12
Appendix 3 Cybersecurity Recommendations	13

1 Overview

1.1 Introduction

8-Port ePoE Switch is a two-layer hardened switch, which supports long distance Ethernet power supply. It provides eight 10/100 Mbps Ethernet ports, one 1000 Mbps Ethernet port and one 1000 Mbps fiber port. The device is equipped with 3 self-adaptive transmission modes including IEEE, E100 and E10. It supports both twisted-pair transmission and coaxial cable transmission.

1.2 Features

Common Features

- Two-layer hardened PoE switch.
- Supports IEEE802.3, IEEE802.3u, IEEE802.3ab/z and IEEE802.3X standards.
- MAC auto study and aging, and MAC address list capacity is 4K.
- Supports MDI/MDIX self-adaptive.
- Port 1-8 are RJ45 ports, which support 10/100 Mbps self-adaptive, and support IEEE802.3af, IEEE802.3at standard power supply; Port 9 is a RJ45 port which supports 10/100/1000 Mbps self-adaptive.
- Industrial wide temperature design.
- Adopts metal structure.

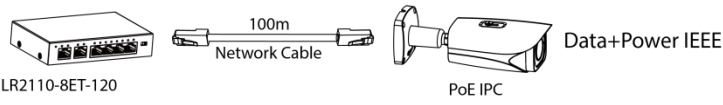
Individual Features

- The device owns one 1000 Mbps self-adaptive fiber port, one 10/100/1000 Mbps self-adaptive RJ45 port and eight 10/100 Mbps self-adaptive RJ45 ports.
- No.1 port and No.5 port support IEEE802.3bt standard 90 W power supply.
- It supports 3 transmission modes, which includes IEEE, E100 and E10. IEEE mode is the standard Ethernet mode when it is transmitted via twisted-pair, which supports a maximum transmission distance up to 100 m; E100 mode supports up to 300 m and E10 mode supports up to 800 m. When it is transmitted via coaxial cable, IEEE mode supports a maximum transmission distance up to 100 m, E100 mode supports up to 400 m and E10 mode supports up to 1000 m.
- The device adopts 120 W power adapter.

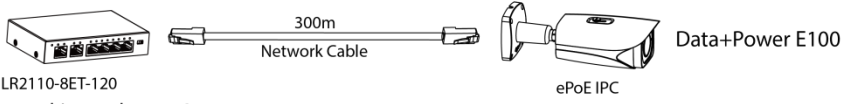
1.3 Typical Application

Figure 1-1 Typical application

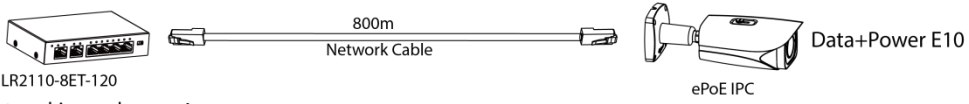
Networking scheme 1



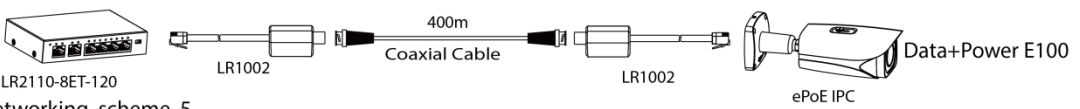
Networking scheme 2



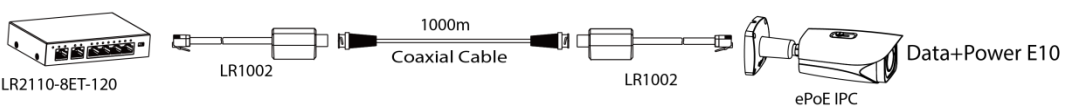
Networking scheme 3



Networking scheme 4



Networking scheme 5



2 Structure

2.1 Front Panel

Figure 2-1 Front panel

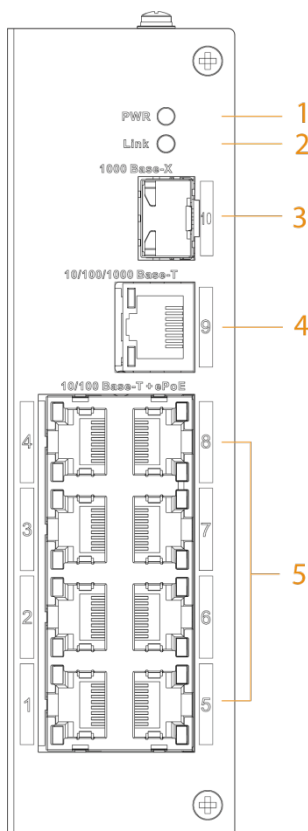


Table 2-1 Panel description

No.	Name	Description
1	PWR	Power indicator light. Used as PoE power supply status indicator light as well, refer to the following table for more details.
2	Link	Fiber port status indicator light.
3	100/1000 Base-X	1000 Mbps self-adaptive fiber port.
4	10/100/1000 Base-T	10/100/1000 Mbps self-adaptive RJ45 port.
5	10/100 Base-T	8 × 10/100 Mbps self-adaptive PoE power supply ports.

The power indicator light can display the current operation status of PoE power supply, which includes three statuses: single port device power on, single port device power off and total device consumption overload.

Table 2-2 Power indicator description

No.	Display mode	Operation status
1	Flashes twice.	Single port device powers on.
2	Flashes once.	Single port device powers off.

Port indicator light can display the status of the current transmission mode for the port, which includes IEEE mode, E100 and E10.

Table 2-3 Port indicator description

No.	Display mode	Working mode
1	Normally on.	IEEE mode
2	On for 3 seconds, off for 1 second.	E100
3	On for 1 second, off for 1 second.	E10

2.2 Rear Panel

Figure 2-2 Rear panel

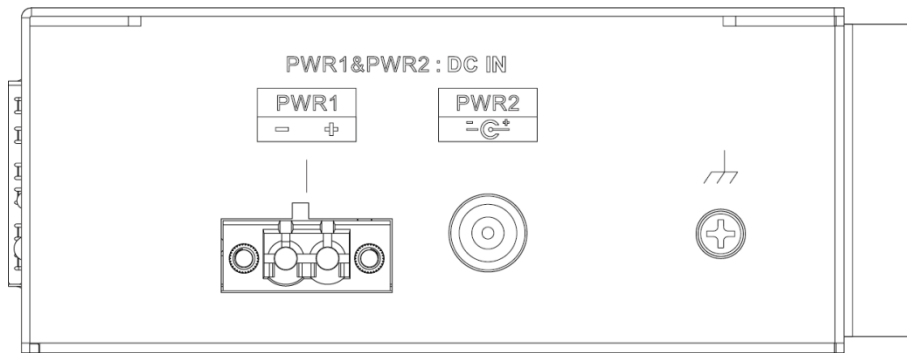


Table 2-4 Parameter description

Parameter	Description
PWR1	Supports 54 VDC.
PWR2	Supports 54 VDC.
⊕	Ground wire.

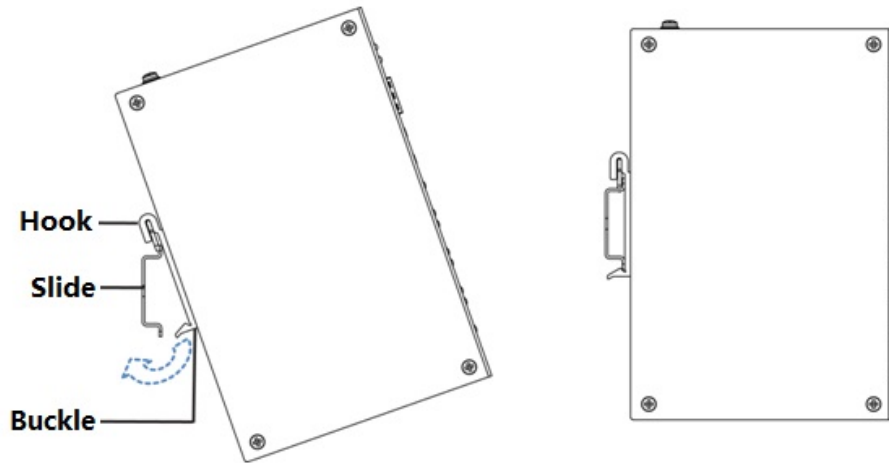
2.3 PoE Power Supply

- 6 × 100 Mbps RJ45 ports, support IEEE802.3af, IEEE802.3at standard power supply.
- 2 × 100 Mbps RJ45 ports, support IEEE802.3af, IEEE802.3at standard and IEEE802.3bt standard 90 W power supply.
- Total power consumption of PoE device is not allowed to exceed the reserve value of device PoE power consumption.

3 Installation

The device supports DIN rail mount. Lay the switch hook on the rail, press the ePoE switch to make the buckle get into the slide.

Figure 3-1 DIN rail mount



Supports the slide width of 28 mm.

Appendix 1 ePoE Power Supply Specifications (CAT)

Cable Length (m)	Communication Bandwidth (Mbps)	PoE Max Load Capacity (W)	Hi-PoE Max Load Capacity (W)	IEEE802.3bt Max Load Capacity (W)	Network Operating Mode
100	100	25.5	53	71.3	IEEE/E100
200	100	25.5	47	52	E100
300	100	25.5	32	40	E100
400	10	23	26	30	E10
500	10	20	20	25	E10
800	10	13	13	13	E10
<p>ePoE switch supply voltage 54 V. CAT6, max. DC resistance < 10 Ω/100 m.</p>					

Appendix 2 ePoE Power Supply Specifications (RG59 Coaxial Cable)

Cable Length (m)	Communication Bandwidth (Mbps)	PoE Max. Load Capacity (W)	Hi-PoE Max. Load Capacity (W)	Network Operating Mode
100	100	25.5	52	IEEE/E100
200	100	25.5	48	E100
300	100	22	28	E100
400	100	15	20	E100
500	10	12	12	E10
800	10	8	8	E10
1000	10	6	6	E10

ePoE switch supply voltage 54 V.
 RG-59, max. DC resistance < 5 Ω /100 m.
 IEEE802.3bt standard is not applicable to RG59 cable solution.



- This user's manual is for reference only.
- Slight difference might be found in user interface.
- All the designs and software here are subject to change without prior written notice.
- All trademarks and registered trademarks are the properties of their respective owners.
- If there is any uncertainty or controversy, please refer to the final explanation of us.
- Please visit our website for more information.

Appendix 3 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.