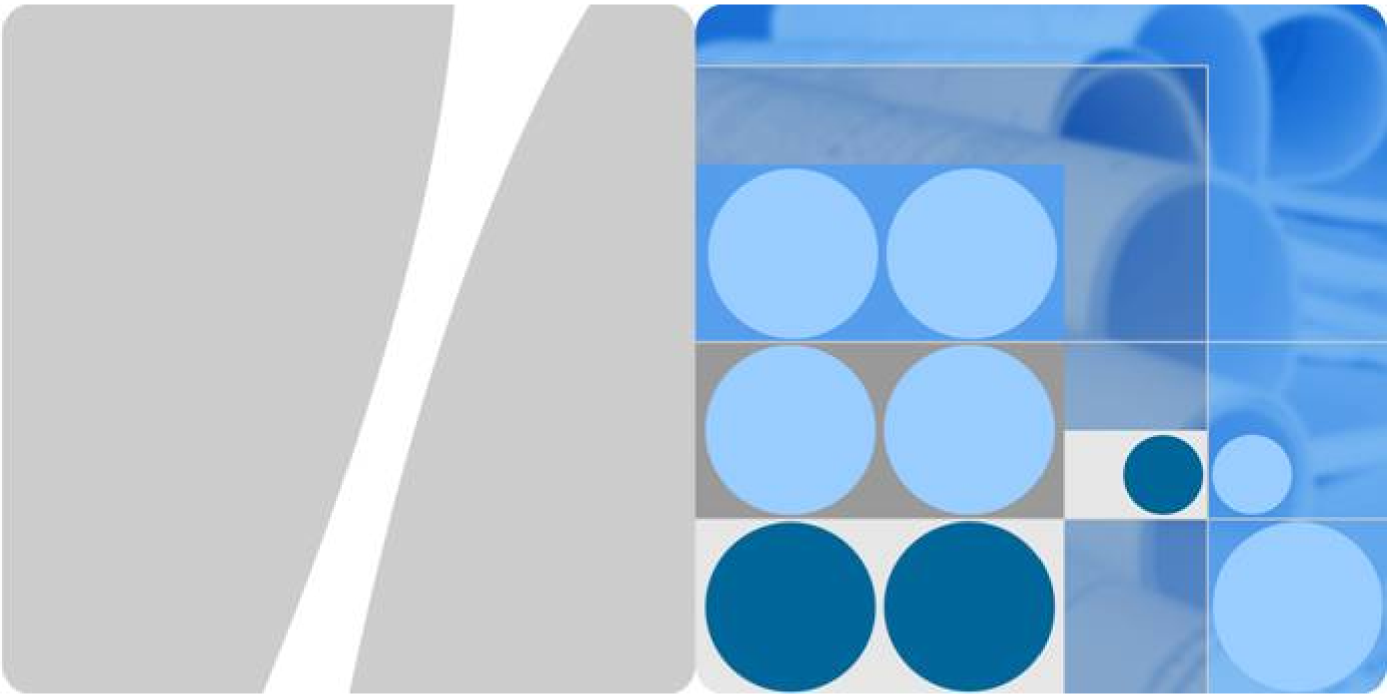


EG860

V200R003C00

User Guide

Issue	**02**
Date	**2015-04-10**

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address:	Huawei Industrial Base Bantian, Longgang Shenzhen 518129 People's Republic of China
Website:	http://www.huawei.com
Email:	support@huawei.com

About This Document

Introduction

This document describes hardware, functions, networking, installation, configurations, and operation and maintenance (O&M) information of an EG860.

Product Version

This document (guide) is intended for EG860 in the following models:

Product Name	Product Version
EG860-C71	V200R003C00
EG860-D61	

Intended Audience

This document is intended for:

- System engineers
- Product engineers

Organization

1 Change History

Updates between document issues are cumulative. Therefore, the latest document issue contains all updates made in previous issues.

2 Introduction

This section describes functions, networking, and technical specifications of an EG860.

3 Hardware

This section describes hardware components and cables of an EG860.

4 Installation

This chapter describes how to install an EG860.

5 Configuration

Data configuration for EG860 can be performed by using WebUI or by auto-configuration.

6 Maintenance

This chapter describes how to maintain an EG860.

7 Reference

This chapter describes how to use the Web network management system (NMS).

8 Alarm Reference

This chapter describes possible alarms related to EG860, and how to handle them.

9 Glossary

This table provides the related glossary for reference.

Conventions

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
⚠ DANGER	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
⚠ WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
⚠ CAUTION	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
⚠ NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
🕮 NOTE	Calls attention to important information, best practices and tips. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

General Conventions

The general conventions that may be found in this document are defined as follows.

Convention	Description
Times New Roman	Normal paragraphs are in Times New Roman.
Boldface	Names of files, directories, folders, and users are in **boldface**. For example, log in as user **root**.
Italic	Book titles are in *italics*.
`Courier New`	Examples of information displayed on the screen are in Courier New.

Command Conventions

The command conventions that may be found in this document are defined as follows.

Convention	Description
Boldface	The keywords of a command line are in **boldface**.
Italic	Command arguments are in *italics*.
[ ]	Items (keywords or arguments) in brackets [ ] are optional.
{ x | y | ... }	Optional items are grouped in braces and separated by vertical bars. One item is selected.
[x | y | ...]	Optional items are grouped in brackets and separated by vertical bars. One item is selected or no item is selected.
{ x | y | ... }*	Optional items are grouped in braces and separated by vertical bars. A minimum of one item or a maximum of all items can be selected.
[x | y | ...]*	Optional items are grouped in brackets and separated by vertical bars. Several items or no item can be selected.

GUI Conventions

The GUI conventions that may be found in this document are defined as follows.

Convention	Description
Boldface	Buttons, menus, parameters, tabs, window, and dialog titles are in **boldface**. For example, click **OK**.
>	Multi-level menus are in **boldface** and separated by the ">" signs. For example, choose **File** > **Create** > **Folder**.

Keyboard Operations

The keyboard operations that may be found in this document are defined as follows.

Format	Description
Key	Press the key. For example, press **Enter** and press **Tab**.
Key 1+**Key 2**	Press the keys concurrently. For example, pressing **Ctrl**+**Alt**+**A** means the three keys should be pressed concurrently.
Key 1, **Key 2**	Press the keys in turn. For example, pressing **Alt**, **A** means the two keys should be pressed in turn.

Mouse Operations

The mouse operations that may be found in this document are defined as follows.

Action	Description
Click	Select and release the primary mouse button without moving the pointer.
Double-click	Press the primary mouse button twice continuously and quickly without moving the pointer.
Drag	Press and hold the primary mouse button and move the pointer to a certain position.

Contents

About This Document......ii

1 Change History......1

2 Introduction......5

2.1 Product Functions......6

2.2 Network Networking......6

2.3 Technical Specifications......8

2.4 Product Security......14

2.4.1 Network Security......14

2.4.2 Application Security......15

2.4.2.1 Wireless Security......15

2.4.2.2 OM Security......15

2.4.2.2.1 User Authentication and Access Control......15

2.4.2.2.2 OM System Security......16

2.4.2.2.3 Digital Signature of Software......17

2.5 Certification Information......18

3 Hardware......19

3.1 EG860 Hardware......20

3.1.1 Appearance......20

3.1.2 Front Panel......20

3.1.3 Indicators......22

3.1.4 Ports......23

3.2 EG860 Cables......23

3.2.1 PoE Cable......23

3.2.2 Power Cable......25

3.2.3 PGND Cable......26

4 Installation......28

4.1 Site Preparations......29

4.2 Installation Preparations......30

4.3 Installation Procedure......32

4.3.1 Mounting an EG860 on a Pole......32

4.3.1.1 Mounting EG860 Equipment on a Pole......34

4.3.1.2 Connecting Cables to an EG860 Mounted on a Pole..39
4.3.2 Mounting an EG860 on a Wall...47
4.3.2.1 Mounting EG860 Equipment on a Wall...48
4.3.2.2 Connecting Cables to an EG860 Mounted on a Wall..52
4.4 Checking Installation...61

5 Configuration...64
5.1 Onsite Configuration (WebUI)..65
5.1.1 Log in to the WebUI...65
5.1.2 Configuring Basic Data...65
5.1.3 Configuring Transmission Data...66
5.1.4 Configuring Dedicates Bearers..73
5.2 Remote Configuration (Auto-configuration) 73

6 Maintenance..76
6.1 Preparations for Site Maintenance...77
6.2 Powering on/off an EG860...77

7 Reference...79
7.1 Status...80
7.1.1 Internet..80
7.1.2 LAN...80
7.1.3 WLAN..81
7.2 General Settings..82
7.2.1 SIM Card Settings..82
7.2.2 Internet Settings...82
7.2.3 DHCP Settings...84
7.2.4 WLAN Settings..85
7.2.5 WLAN Multi-SSID...85
7.2.6 WLAN Access Restrictions...86
7.2.7 Internet MTU..87
7.2.8 Routing...87
7.2.9 Dedicated Context...88
7.2.10 IGMP Management...89
7.2.11 L2TP Settings..90
7.2.12 FTP Settings..90
7.2.13 Security access Settings...91
7.3 Security Settings...91
7.3.1 Firewall General...91
7.3.2 MAC Filtering...92
7.3.3 IP Filtering..93
7.4 NAT Settings..94
7.5 QoS Management...95

7.6 VPN....96
7.7 System....98
7.7.1 Device Information....98
7.7.2 Reset....98
7.7.3 Backup & Recovery....98
7.7.4 Upgrade....99
7.7.5 Password Change....99
7.7.6 Password Complexity....100
7.7.7 Password security Settings....101
7.7.8 Date & Time....101
7.7.9 Diagnosis....101
7.7.10 Log....103
7.7.11 Device Switch....103
7.7.12 Bandinfo Number Configuration....104
7.7.13 Work Frequency....104
7.7.14 SIM Configuration....105
7.7.15 Alarm Configuration....105
7.8 Logout....107

8 Alarm Reference....108

8.1 ALM-50001 Lan state....109
8.2 ALM-50002 High Temperature....110
8.3 ALM 50003-RadioSignal Weak....111

9 Glossary....113

1 Change History

Updates between document issues are cumulative. Therefore, the latest document issue contains all updates made in previous issues.

02 (2015-04-10)

This is the second release of the V200R003C00 version.

Compared with issue V200R003C00 01, the documentation does not contain any new information.

Compared with issue V200R003C00 01, the documentation includes the following changes:

Topic	Change Description
● **5.1.3 Configuring Transmission Data** ● **7.2.2 Internet Settings**	Modified the displayed information for enabling **Routing Behind MS**.

Compared with issue V200R003C00 01, the documentation does not delete any information.

01 (2015-03-24)

This is the first release of the V200R003C00 version.

Compared with issue V200R003C00 Draft C, the documentation does not contain any new information.

Compared with issue V200R003C00 Draft C, the documentation includes the following changes:

Topic	Change Description
● 2.3 Technical Specifications ● 3.1.3 Indicators ● 4.3.1 Mounting an EG860 on a Pole ● 5.2 Remote Configuration (Auto-configuration) ● 7.2.3 DHCP Settings ● 7.2.10 IGMP Management ● 7.7.10 Log ● 7.7.15 Alarm Configuration	Optimized the content.

Compared with issue V200R003C00 Draft C, the documentation deletes the following information.

Reference > **General Settings** > **WLAN WPS**

Draft C (2014-12-01)

This is the Draft C release of the V200R003C00 version.

Compared with issue V200R003C00 Draft B, the documentation does not contain any new information.

Compared with issue V200R003C00 Draft B, the documentation includes the following changes:

Topic	Change Description
● 4.2 Installation Preparations ● 4.3.1 Mounting an EG860 on a Pole ● 5.1.1 Log in to the WebUI ● 7.2.4 WLAN Settings ● 7.7.9 Diagnosis ● 7.7.11 Device Switch	Optimized the content.

Compared with issue V200R003C00 Draft B, the documentation does not delete any information.

Draft B (2014-11-11)

This is the Draft B release of the V200R003C00 version.

Compared with issue V200R003C00 Draft A, the documentation does not contain any new information.

Compared with issue V200R003C00 Draft A, the documentation includes the following changes:

Topic	Change Description
● 3.2.1 PoE Cable ● 5.1.1 Log in to the WebUI ● 5.2 Remote Configuration (Auto-configuration) ● 7.2.12 FTP Settings ● 7.2.13 Security access Settings	Optimized the content.

Compared with issue V200R003C00 Draft A, the documentation does not delete any information.

Draft A (2014-10-30)

This is the Draft A release of the V200R003C00 version.

Compared with issue V200R002C00 05, the documentation includes the following new information:

- **2.4 Product Security**
- **7.2.12 FTP Settings**
- **7.2.13 Security access Settings**
- **7.2.11 L2TP Settings**
- **7.5 QoS Management**
- **7.6 VPN**
- **7.7.6 Password Complexity**
- **7.7.7 Password security Settings**
- **7.7.13 Work Frequency**

Compared with issue V200R002C00 05, the documentation includes the following changes:

Topic	Change Description
2.1 Product Functions	Modified the main function of EG860.
2.3 Technical Specifications	Modified the technical specifications of EG860.
5.1.1 Log in to the WebUI	Modified the default password of WebUI.
5.1.3 Configuring Transmission Data	Added the configuration steps for L2TP.
7.2.1 SIM Card Settings	Modified the steps for setting SIM card.

Topic	Change Description
7.7.9 Diagnosis	Deleted the Tmsi information query. Added the configuration of WAN ICMP function.
7.7.11 Device Switch	Added the configuration of **Antenna status** parameter.
7.7.14 SIM Configuration	Deleted the default value of PLMN.
● **5.2 Remote Configuration (Auto-configuration)** ● **7.1.1 Internet** ● **7.1.2 LAN** ● **7.1.3 WLAN** ● **7.2.2 Internet Settings** ● **7.2.3 DHCP Settings** ● **7.2.4 WLAN Settings** ● **7.2.5 WLAN Multi-SSID** ● **7.2.7 Internet MTU** ● **7.7.5 Password Change**	Optimized the content.

Compared with issue V200R002C00 05, the documentation deletes the following information.

Reference>FTP Management

2 Introduction

About This Chapter

This section describes functions, networking, and technical specifications of an EG860.

2.1 Product Functions
An EG860, as a data service device on the Internet of Things (IoT), is used in a long term evolution (LTE) network to upload or download user data. It provides data service (in route mode), security service (firewall/NAT), and equipment maintenance and management. NAT is short for Network Address Translation.

2.2 Network Networking
An EG860 is a wireless broadband access terminal that serves as a major device in a wireless Internet of Things (IoT) data private network. It can be installed indoors or outdoors.

2.3 Technical Specifications
The technical specifications of an EG860 cover mechanical, power, surge protection, performance, antenna, and environment specifications.

2.4 Product Security
EG860 security includes network security and application security. Application security includes wireless security and OM security.

2.5 Certification Information
This section describes the certification that EG860 has passed.

2.1 Product Functions

An EG860, as a data service device on the Internet of Things (IoT), is used in a long term evolution (LTE) network to upload or download user data. It provides data service (in route mode), security service (firewall/NAT), and equipment maintenance and management. NAT is short for Network Address Translation.

Background Information

A wireless data private network is an important part of **IoT** infrastructures. The wireless data private network is based on the wired government private network and requires base stations and access fibers as supplements. It provides secure and reliable channels for transmitting, converging, processing, and distributing sensor messages of various **IoT** applications. The wireless data private network uses unified standards for receiving sensor messages and is capable of identity authentication and secure transmission to meet the requirements for operating security and emergency management of a metro **IoT**.

Functions

IoT is about to introduce a new wave in the information industry following computers, Internet, and mobile communications.

A wireless data private network has the following attractions:

- Provides a unified, secure, omnipresent, and standard channel for transmitting sensor messages applicable to service and emergency management of a city.
- Avoids repeated construction of sensor networks.
- Reduces the cost of constructing **IoT** applications, fully utilizes limited frequency resources, and ensures information security.

An EG860 provides the following functions:

- Software management: bandwidth, software upgrading, wireless backhaul, dual tunnels, virtual **SIM** card, physical **SIM** card, multicast, static routing, routing behind **MS**, L2TP tunnel, QoS, data service encryption, and status management.
- Configuration management: auto-configurable commissioning and configuration management. The NMS manages an EG860 using the TR069 protocol, including configuration delivery from the NMS to an EG860, software upgrade, status and performance monitoring, log collection, alarm management, and health check.
- O&M: web-based local maintenance and performance statistics.
- Fault management: alarm, connectivity diagnosis, and log management.

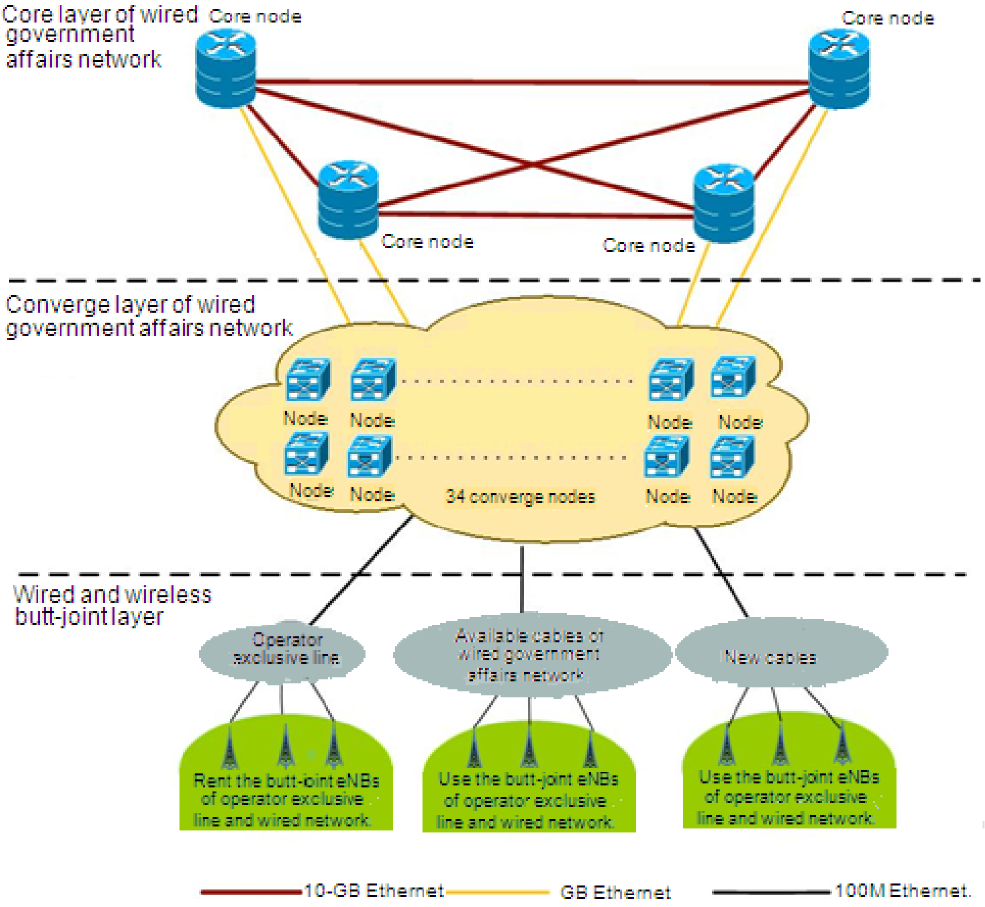
2.2 Network Networking

An EG860 is a wireless broadband access terminal that serves as a major device in a wireless Internet of Things (IoT) data private network. It can be installed indoors or outdoors.

A government private network is a wired MAN that runs over existing optical cables and **SDH** or **MSTP** networks at the physical layer and adopts **MPLS VPN** architecture at the **IP** layer, to isolate different types of services that coexist over the same network.

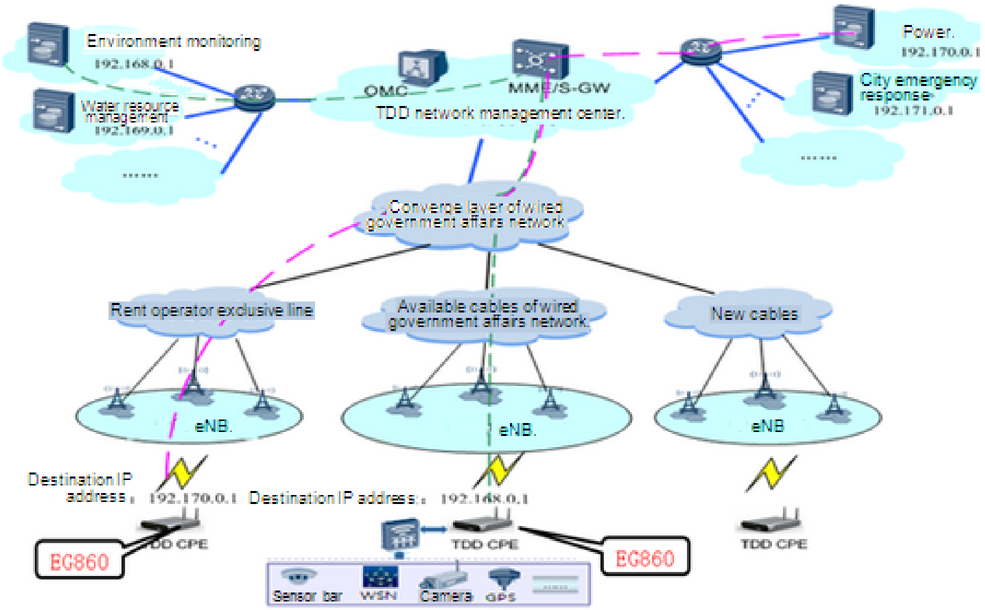
A government private network covers agencies, offices, and business units regardless of size within a municipality. The integrated network is shown as **Figure 2-1**.

Figure 2-1 A government integrated network


Core layer of wired government affairs network
Core node
Core node
Core node
Core node
Converge layer of wired government affairs network
Node
Node
Node
Node
Node
Node
Node
Node
34 converge nodes
Wired and wireless butt-joint layer
Operator exclusive line
Available cables of wired government affairs network
New cables
Rent the butt-ioint eNBs of operator exclusive line and wired network.
Use the butt-joint eNBs of operator exclusive line and wired network.
Use the butt-joint eNBs of operator exclusive line and wired network.
10-GB Ethernet
GB Ethernet
100M Ethernet.

The networking of wireless networks is shown as **Figure 2-2**.

Figure 2-2 The networking of wireless networks


Environment monitoring
192.168.0.1
Water resource management
192.169.0.1
....
OMC
MME/S-GW
TDD network management center.
Power.
192.170.0.1
City emergency response
192.171.0.1
....
Converge layer of wired government affairs network
Rent operator exclusive line
Available cables of wired government affairs network.
New cables
eNB.
eNB.
eNB
Destination IP address: 192.170.0.1
Destination IP address: 192.168.0.1
TDD CPE
TDD CPE
TDD CPE
EG860
EG860
Sensor bar
WSN
Camera
GPS

An EG860 operates on an LTE network. Data from a sensor travels through a **FE** port of the EG860 and, after being encapsulated to **IPv4** packets by the EG860, is transferred to backend servers.

NOTE

Personal information will be anonymized to protect user privacy.

2.3 Technical Specifications

The technical specifications of an EG860 cover mechanical, power, surge protection, performance, antenna, and environment specifications.

Mechanical specifications

Table 2-1 lists the mechanical specifications of an EG860.

Table 2-1 Mechanical specifications

Dimension	Weight
240 mm (H) x 200 mm (W) x 61 mm (D)	⩽ 2 kg

Electrical specifications

Table 2-2 lists the electrical specifications of an EG860.

Table 2-2 Electrical specifications of an EG860

Equipment	Rated voltage	Power
EG860	24 V DC (PWR)	Maximum power consumption: 30 W
	-48 V DC (POE)	

Surge Protection Specifications

Table 2-3 lists the surge protection specifications of the EG860.

Table 2-3 Surge protection specifications

Port	Surge Protection Specifications
Power and signal ports	1,000 V

Specifications

Table 2-4 and Table 2-5 list the radio frequency (RF) specifications of an EG860-C71 and EG860-D61 respectively.

Table 2-4 RF specifications of EG860-C71

Mode	Item	Description
LTE	Frequency	1447 MHz-1467 MHz 1785 MHz-1805 MHz 832 MHz-862 MHz (uplink)/ 791 MHz-821 MHz (downlink)
	Carrier configuration	5 MHz/10 MHz/20 MHz
	Maximum transmit power	23 dBm±2 dBm
	Output frequency spectrum template and stray specifications	3GPP TS 36.101-compliant

Mode	Item	Description
	Receiver sensitivity	● 1.8G and 1.4G – -92dBm/20MHz – -95dBm/10MHz – -98dBm/5MHz ● 800M – -88dBm/20MHz – -92dBm/10MHz – -95dBm/5MHz
	Blocking	3GPP TS 36.101-compliant
Wi-Fi	Working mode	IEEE 802.11b/g/n: 2.4 GHz
	Output power	IEEE 802.11b: <16dBm IEEE 802.11g: <15dBm IEEE 802.11n: <13dBm
	Receiver sensitivity	IEEE 802.11b: ≤-76 dBm@11Mbps IEEE 802.11g: ≤-65 dBm@54Mbps IEEE 802.11n: ≤-75 dBm@54Mbps

Table 2-5 RF specifications of EG860-D61

Mode	Item	Description
TD-LTE	Frequency	380MHz~450MHz
	Carrier configuration	In the fixed topology: 3MHz/5MHz/10MHz/20MHz In the vehicle-mounted communications system: 5MHz/10MHz/20MHz
	Maximum transmit power	25 dBm±2 dBm
	Output frequency spectrum template and stray specifications	3GPP TS 36.101-compliant

Mode	Item	Description
	Receiver sensitivity	-92dBm/20MHz -95dBm/10MHz -98dBm/5MHz -100.2dBm/3MHz
	Blocking	3GPP TS 36.101-compliant
Wi-Fi	Working mode	IEEE 802.11b/g/n: 2.4 GHz
	Output power	IEEE 802.11b: <16dBm IEEE 802.11g: <15dBm IEEE 802.11n: <13dBm
	Receiver sensitivity	IEEE 802.11b: ≤-76 dBm@11Mbps IEEE 802.11g: ≤-65 dBm@54Mbps IEEE 802.11n: ≤-75 dBm@54Mbps

Antenna Specifications

Table 2-6 and **Table 2-7** list the antenna specifications of an EG860-C71 and EG860-D61 respectively.

Table 2-6 Antenna specifications of EG860-C71

Item	LTE Antenna (1.4G)	LTE Antenna (1.8G)	LTE Antenna (800M)	Wi-Fi Antenna
Mode	Built-in directional antenna or external antenna	Built-in directional antenna or external antenna	External antenna	Built-in omnidirectional antenna
Frequency	Built-in directional antenna: 1447MHz~1467MHz External antenna: 1350MHz~1500MHz	Built-in directional antenna: 17857MHz~1805MHz External antenna: 1710MHz~1880MHz	760MHz~870MHz	2400MHz~2500MHz

Item	LTE Antenna (1.4G)	LTE Antenna (1.8G)	LTE Antenna (800M)	Wi-Fi Antenna
Gain	Built-in directional antenna: ⩾ 7.5dBi External antenna: ⩾5dBi	Built-in directional antenna: ⩾ 7.5dBi External antenna: ⩾ 10dBi	⩾5dBi	⩾2dBi
Directivity diagram	Horizontal plane: > 75 vertical plane: > 60	Horizontal plane: > 75 vertical plane: > 60	Omnidirectional	Omnidirectional
Isolation between built-in **LTE** directional antennas	⩾20dB	⩾20dB	None	None
Isolation between built-in **Wi-Fi** omnidirectional antennas	None	None	None	⩾20dB
Isolation between built-in **LTE** directional antennas and built-in **Wi-Fi** omnidirectional antennas	>35dB	>35dB	None	>35dB

Table 2-7 Antenna specifications of EG860-D61

Item	LTE Antenna (400M)	Wi-Fi Antenna
Mode	External antenna	Built-in omnidirectional antenna
Frequency	380MHz~410MHz/ 410MHz~440MHz/ 440MHz~450MHz/ 380MHz~450MHz	2400MHz~2500MHz

Item	LTE Antenna (400M)	Wi-Fi Antenna
Gain	● 380MHz~410MHz/ 410MHz~440MHz/ 440MHz~450MHz:≥3.5 dBi ● 380MHz~450MHz:≥1.5 dBi	≥ 2 dBi
Directivity diagram	Omnidirectional	Omnidirectional
Isolation between built-in **LTE** directional antennas	None	None
Isolation between built-in **Wi-Fi** omnidirectional antennas	None	≥20dB
Isolation between built-in **LTE** directional antennas and built-in **Wi-Fi** omnidirectional antennas	None	

Environment Specifications

Table 2-8 lists the operating environment specifications of an EG860.

Table 2-8 Operating environment specifications

Item	Description
Temperature	-40℃~+50℃
Relative humidity	5%~95%
Temperature change rate	0.5℃/min
Atmospheric pressure	62 kPa~106 kPa
Altitude	≤ 3,000 m
Air flow rate	≤ 50 m/s
Rainfall intensity	6 mm/min
Rainwater temperature	+5℃
Sand	1000 mg/m^3
Earthquake intensity	VIII or higher

Table 2-9 lists the storage environment specifications of an EG860.

Table 2-9 Storage environment specifications

Item	Description
Temperature	-40℃~+70℃
Relative humidity	10%~100%
Temperature change rate	1 ℃/min
Atmospheric pressure	62 Kpa~106 Kpa
Air flow rate	≤ 55 m/s

2.4 Product Security

EG860 security includes network security and application security. Application security includes wireless security and OM security.

2.4.1 Network Security

EG860 network security uses Secure Sockets Layer (SSL) and Hypertext Transfer Protocol Secure (HTTPS).

SSL

The SSL protocol is a security connection technology for the server and client. It provides a confidential, trusted, and identity-authenticating connection to two application layers. SSL is regarded as a standard security measure and has been widely applied to web services.

- Identity authentication

  Identity authentication checks whether a communication individual is the expected object. SSL authenticates servers and clients based on digital certificates and user/password. Clients and servers have their own identifiers. The identifiers are numbered by the public key. To verify that a user is legitimate, SSL requires digital authentication during data exchange in the SSL handshake procedure.

- Connection confidentiality

  Data is encrypted before transmission to prevent data from being hacked by malicious users. SSL uses encryption algorithms to ensure the connection confidentiality.

- Data integrity

  Any tampering on data during transmission can be detected. SSL establishes a secure channel between the client and the server so that all the SSL data can reach the destination intact.

HTTPS

For the EG860, the OM TCP applications can use SSL. HTTP over SSL is generally called HTTPS. HTTPS is used for connections between the NMS/WebUI and EG860. SSL also uses the digital certificate mechanism.

HTTPS provides secure HTTP channels. HTTPS is HTTP to which SSL is added, and SSL ensures the security of HTTPS.

2.4.2 Application Security

EG860 application security includes wireless security and OM security.

2.4.2.1 Wireless Security

EG860 wireless security includes authentication, air-interface data encryption, and integrity protection.

For details, see *Security Feature Manual*.

2.4.2.2 OM Security

OM security includes user authentication, access control, OM system security, and software digital signature.

2.4.2.2.1 User Authentication and Access Control

User authentication and access control are implemented for users to be served by the EG860. The objective of authentication is to identify users and grant the users with proper permission. The objective of access control is to specify and restrict the operations to be performed and the resources to be accessed by the users.

User Account Management

Local user account management involves modification and query of local user accounts. Information about a local user account includes user name and user description. To improve system security, the following security requirements must be satisfied:

- Password security policies
  - The password must contain 8 to 32 characters
  - The password must contain at least two character types and must not contain three or more than three consecutively same characters
  - The password must not contain the account name or its reversion
  - Maximum number of failed password attempts
  - Threshold of consecutive password modification failures
  - Duration after which a locked password can be automatically unlocked
- Password usage rules
  - Users must enter passwords twice when changing passwords, and the passwords entered cannot be copied.
  - Users can change their own passwords. The old password must be verified when it is changed.
  - User accounts are locked when the number of consecutive password failures reaches a specified threshold.
- Password storage and transmission rules

- Passwords are encrypted and are stored locally.

- Default account management
  - By default, the **admin** user is able to perform all operations except for the functions related to the TR069 protocol on the system. The **acs** user only can control the authentication between eOMC910 and EG860.
- User names and passwords

  Table 2-10 describes the user names and default passwords for an EG860.

Table 2-10 User names and passwords

User Name	Default Password	Description
admin	4GCPE@TD	A user that accesses the EG860 by using the Web management interface.
acs	4GCPE@TD	An eOMC910 user that performs operations on the EG860.

⚠ **NOTICE**

- To enhance system security, users need to change the passwords periodically, preventing brute-force cracking.
- The password of the **acs** user must be changed on both the eOMC910 and the EG860.

User Login Management

The login types supported by NEs include local user login, and machine-machine authentication and certificate authentication for NMS access. All login types must be authenticated before communications. In addition, the following security requirements must be satisfied:

- Identity check mechanism
  - Identity check based on accounts and passwords
  - Automatic logins by programs for machine-machine accounts

2.4.2.2.2 OM System Security

OM system security includes software integrity check.

In the original procedure for releasing and using the software, the software integrity is ensured by using cyclic redundancy check (CRC). CRC can only prevent data loss during transmissions. If data is tampered with during transmissions, a forged CRC value will be regarded as valid by the CRC. Therefore, the receive end cannot rely on the CRC to ensure the consistency between the received data and the original data, adversely affecting the reliability and security for the software.

Software integrity protection implements the Hash algorithm or adds a digital signature to software (including mediation layers and configuration files) when releasing software, and then uploads software to the target server or device. When a target device downloads, loads, or runs software, the target device performs the Hash check or authenticates the digital signature. By doing so, software integrity protection ensures end-to-end software reliability and integrity.

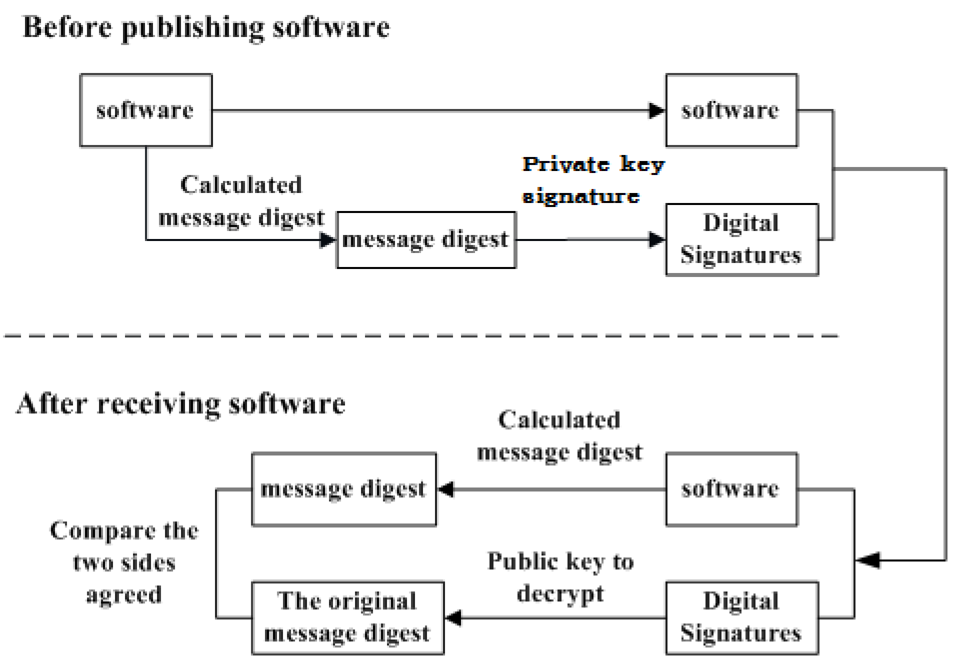
Software integrity protection helps detect viruses or malicious tampering in a timely manner, preventing insecure or virus-infected software from running on the device.

2.4.2.2.3 Digital Signature of Software

A digital signature of software is used to identify the software source. It ensures the integrity and reliability of software.

When software is released, its digital signature is delivered with the software package. After the software package is downloaded to an NE, the NE verifies the digital signature of the software package before using it. If the digital signature passes the verification, the software is intact and reliable. If the verification fails, the software package is invalid and cannot be used. **Figure 2-3** illustrates the principles of a software digital signature.

Figure 2-3 Digital signature of software



- Before a software package is released, all files in the software package are signed with digital signatures. That is, after a message digest is calculated for all files in the software package, the message digest is digitally signed using a private key.
- After a software package with a digital signature is loaded to an NE through a media such as the software release platform, the NE first verifies the digital signature of the software package. That is, the NE uses a public key to decrypt the digital signature and obtain the original message digest. Then, the NE recalculates the message digest and compares the new message digest with the original one.
  - If the two message digests are the same, the software package passes the verification and can be used.

– If the two message digests are different, the software package fails the verification and cannot be used.

The public key used to decrypt digital signatures is stored in the secure storage area of an NE and cannot be queried or exported.

2.5 Certification Information

This section describes the certification that EG860 has passed.

Table 2-11 describes the certification that EG860 has passed.

Table 2-11 Certification that EG860 has passed

Certification Name	Description
Conformite Europende (CE)	Products with the CE marking comply with the electromagnetic compatibility directive (89/336/EEC) and low voltage directive (73/23/EEC) issued by European Commission. The CE marking is a mandatory conformity mark for products placed on the European market.
Restriction of the use of certain hazardous substances (RoHS)	RoHS restricts the use of certain hazardous materials in the manufacturing of electronic and electrical equipment, in consideration of human health and environmental protection. RoHS is enforced in each member state of the European Union.

3 Hardware

About This Chapter

This section describes hardware components and cables of an EG860.

3.1 EG860 Hardware
This section describes the exterior, front panel, indicators, and ports of an EG860.

3.2 EG860 Cables
This section describes the cables of an EG860, including power over Ethernet (PoE) cables, power cables and protection ground (PGND) cables.

3.1 EG860 Hardware

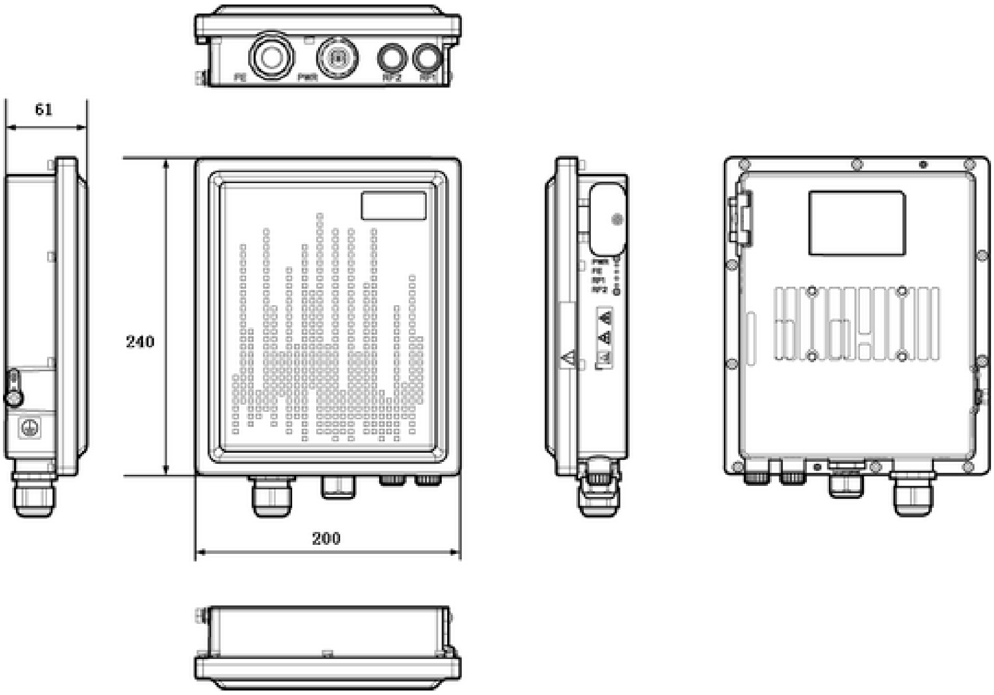
This section describes the exterior, front panel, indicators, and ports of an EG860.

3.1.1 Appearance

The exterior of an EG860 provides you a fair idea of major components.

Figure 3-1 shows the exterior of an EG860.

Figure 3-1 EG860 exterior (unit: mm)



3.1.2 Front Panel

An EG860 has an FE port, a power port, external antenna ports, subscriber identity module (SIM) card window, indicators, a nameplate, and a ground screw on its front panel.

Figure 3-2 shows the front panel of an EG860.

Figure 3-2 EG860 front panel

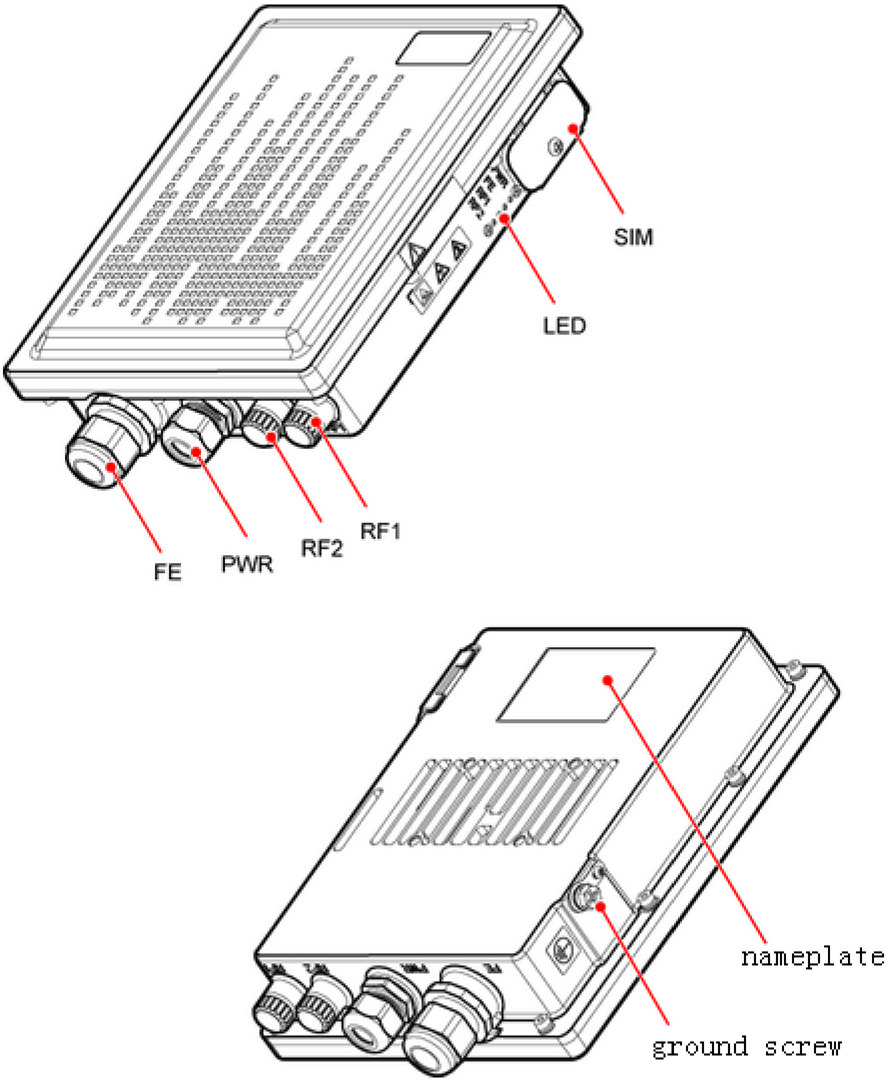


Table 3-1 provides port description for the front panel.

Table 3-1 Ports of the EG860 front panel

Item	Port	Description
FE	Data service port	Receives/Transmits data services and supplies power to an EG860.
PWR	Power port	Connects to a power supply.
RF1	External antenna port	Connects to an external antenna.
RF2		

Item	Port	Description
LED	None	Indicates the operating status of an EG860. For details, see **3.1.3 Indicators**.
SIM card window	None	Houses **SIM** cards.
Nameplate	None	Displays manufacturer information.
Ground screw	None	Connects ground cables.

3.1.3 Indicators

All the indicators are on the front panel to show the operating status of an EG860.

Table 3-2 provides status explanation of the indicators.

Table 3-2 EG860 indicators

Indicator	Color	Status	Description
PWR	Red	On	Power supply is functional.
		Off	Power supply is absent.
RF1/RF2	Green	Steady on	Air interface signals are strong, with the real **RSRP** ranging between –95 dBm and –44 dBm.
		Blinks on (green) and off at 3 Hz	Air interface signals are weak, with the real **RSRP** ranging between –105 dBm and –95 dBm.
		Steady off	No air interface signal is available, or air interface signals are very weak, with the real **RSRP** ranging between–141 dBm and –105 dBm.
FE	Green	Steady on	An FE port is working properly.

Indicator	Color	Status	Description
		Blinks on (green) and off at 3 Hz	An FE port transmits/ receives data at the speed of 10 Mbit/s.
		Blinks on (green) and off at 12 Hz	An FE port transmits/ receives data at the speed of 100 Mbit/s.
		Steady off	No connection exists at an FE port.

3.1.4 Ports

An EG860 has an FE port, a power port, and external antenna ports.

The following provides functions of these ports:

- An **FE** port receives/transmits data services and supplies power to an EG860 by connecting to a **POE** injector.
- A power port supplies **DC** power to an EG860.
- Two external antenna ports are used for connecting external antennas.

3.2 EG860 Cables

This section describes the cables of an EG860, including power over Ethernet (PoE) cables, power cables and protection ground (PGND) cables.

3.2.1 PoE Cable

A PoE cable is a shielded network cable that connects EG860's FE port and the POE adaptor's PoE port.

Background Information

POE technology enables DC power supply and data transmission to an EG860 through an Ethernet cable.

Configuration Rules

- Both ends of an **POE** cable that is used to connect the EG860 and **POE** adaptor are shielded RJ45 connectors and configured in compliance with the following requirements:
  - Configure an EG860 with one PoE cable.
  - Use a **POE** cable with the length of 5 m or 20 m.
- Both ends of the cable that is used to connect the camera and **POE** adaptor are shielded RJ45 connectors and configured in compliance with the following requirements
  - Only one cable of this kind is used for each camera.

- Use a **POE** cable with the maximum length of 60 m.
- Standard Cat 5e outdoor network cables are used.

Technical Specifications

Table 3-3 lists the specifications of a **POE** cable.

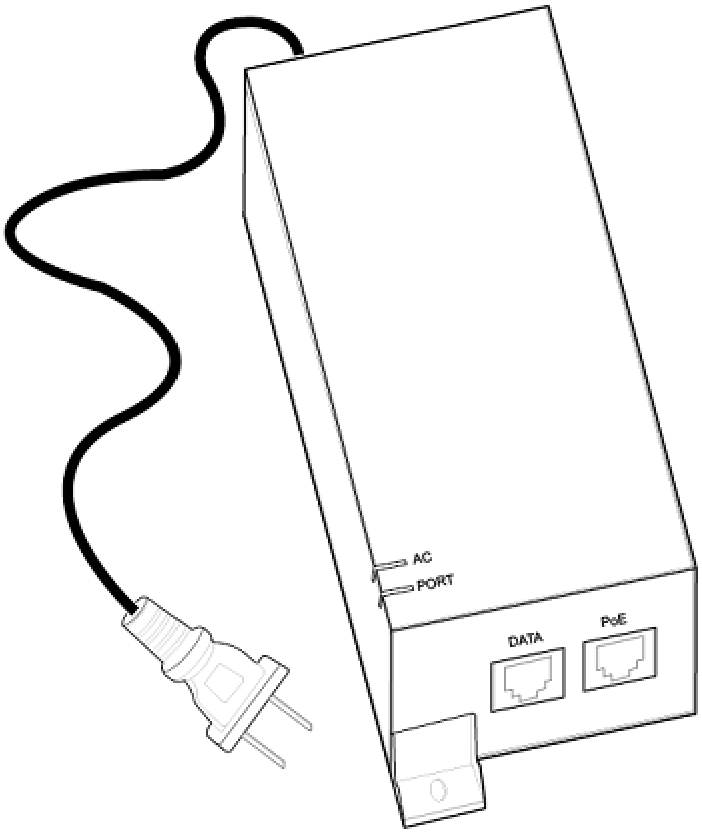
Table 3-3 Technical specifications of a PoE cable

Item	Specifications
Color	Black
Number of wires	Four twisted pairs (eight signal cables)
Cross-sectional area	0.2 mm² (24 AWG)
External diameter	6.8 mm ± 0.3 mm
Operating temperature	-40℃~75℃
Minimum installation temperature	-20℃
Actual highest operating voltage	100 V
Actual highest operating voltage	2 A

Power Adapter

Figure 3-3 shows the appearance of a power adapter.

Figure 3-3 Connecting a PoE adapter



DATA: connects to the network cable of a computer or a camera. PoE: connects to a **POE** cable.

Table 3-4 lists the specifications of a power adapter.

Table 3-4 Specifications of a power adapter

Item	Specifications	Application Scenario	Temperature Range
35 W POE power adapter	-40degC-50degC-90 V-264V-54V/0.65A-C8/RJ45-GE	When power is supplied through the **POE** port.	-40℃~50℃

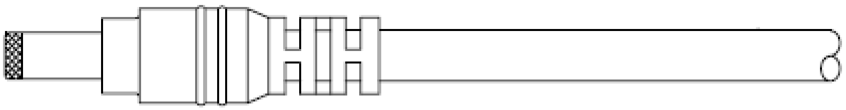
3.2.2 Power Cable

The power cable transmits 24V DC power. It applies only to the solar scenario.

Appearance

Figure 3-4 shows the appearance of a power cable.

Figure 3-4 Power cable appearance



Pin Assignment

A power cable (24V) is a two-core cable. **Table 3-5** describes the pin assignment for the wires of a power cable (24V).

Table 3-5 Pin assignment for the wires of a power cable

Wire	Color
NEG(-)	Blue
RTN(+)	Black

Technical Specifications

Table 3-6 lists the specifications of a power cable.

Table 3-6 Technical specifications of a power cable

Item	Specifications
Color	Black
Cross-sectional area of conductor	0.52mm²
External diameter	6.85mm±0.2mm
Operating temperature	-40℃ to 80℃
Storage temperature	-40℃ to 80℃
Minimum installation temperature	-40℃
Rated voltage	300V

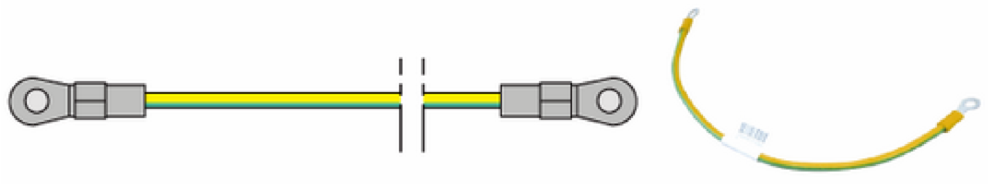
3.2.3 PGND Cable

A protection ground (PGND) cable ensures the grounding of an EG860.

Appearance

A **PGND** cable is green and yellow with a cross-sectional area of 6 mm^2. Both ends of the cable are OT terminals. If a **PGND** cable is self-provided, a copper-conductor cable with a cross-sectional area equal to or more than 6 mm^2 is recommended. **Figure 3-5** shows the exterior of a **PGND** cable.

Figure 3-5 PGND cable exterior



Technical Specifications

Table 3-7 lists the specifications of a **PGND** cable.

Table 3-7 Technical specifications of a PGND cable

Item	Specifications
Color	Yellow and green
Cross-sectional area	6 mm^2 (9 AWG)
External diameter	5.1 mm ± 0.3 mm
Operating temperature	-25℃70℃
Storage temperature	-40℃-50℃
Minimum installation temperature	-10℃
Rated voltage	600 V

4 Installation

About This Chapter

This chapter describes how to install an EG860.

4.1 Site Preparations
This section describes how to prepare a site before EG860 installation.

4.2 Installation Preparations
This section describes how to unpack and check the goods onsite and prepare installation tools before EG860 installation.

4.3 Installation Procedure
This section describes how to install an EG860 on a pole and wall.

4.4 Checking Installation
Check hardware and power-on status of an EG860 after installation.

4.1 Site Preparations

This section describes how to prepare a site before EG860 installation.

Select a site and space for installing an EG860 that meets the following requirements to ensure installation, commissioning, and operating of the equipment.

Requirements for Site Selection

To ensure long-term reliability of an EG860, select a site based on the network plan and technical requirements of the equipment, as well as considerations such as hydrology, geology, and transportation.

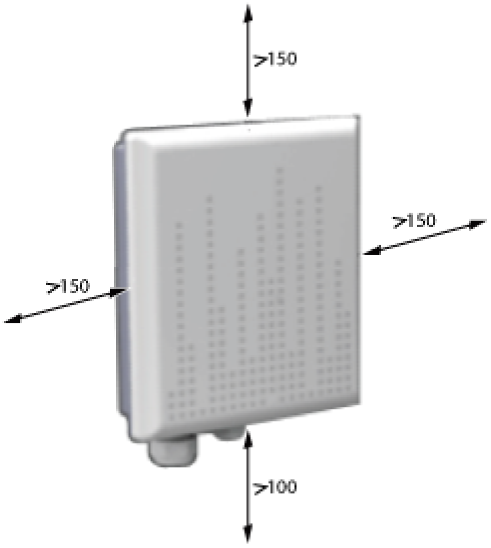
Site selection must meet the following requirements:

- Keep the site away from high temperature, dusty location, poisonous gases, explosive objects, and unstable voltages.
- Keep the site away from any electric substation, industrial boiler, and heating boiler.
- Keep the site away from any radar station, large-power radio transmitting station, and other interference sources. The field strength of interference sources cannot exceed that of unwanted radiation that an EG860 can shield.
- Keep an outdoor EG860 site 500 m away from the sea.
- Keep the site away from pollution sources. If this is not possible, deploy the site in perennial upwind direction of pollution sources.
- Keep the site at least 5 km away from heavy pollution sources such as a refinery and coal mine.
- Keep the site at least 3.7 km away from moderate pollution sources such as a chemical plant, a rubber plant, and an electroplating factory.
- Keep the site at least 2 km away from light pollution sources such as a food factory and a leather processing plant.
- The air intake vents of the communication equipment must be far away from the sewer pipe, septic tank, and sewage disposal pool. The atmospheric pressure inside the equipment room must be higher than that outside the equipment room. Otherwise, corrosive gases may enter the equipment room and corrode the components and circuit boards.
- Keep an indoor EG860 site away from livestock rearing houses and fertilizer warehouses. If this is not possible, the room must be located at a place that is in the upwind direction of the livestock room or fertilizer warehouse.
- Deploy an indoor EG860 site higher than the second floor in a building. Alternatively, mount an EG860 at least 600 mm higher than the record flood stage.

Requirements for Installation Space

To facilitate O&M, adhere to the following space requirements as shown in **Figure 4-1**.

Figure 4-1 Space requirements for installing an EG860 (unit: mm)



Requirements for Operating Environment

For details about operating environment requirements, see **2.3 Technical Specifications**.

4.2 Installation Preparations

This section describes how to unpack and check the goods onsite and prepare installation tools before EG860 installation.

Prerequisites

Upon the device arrival, inspect the device and ensure that the device is intact.

Verify that:

1. The quantity of devices is consistent with the packing list.
2. The shipping containers are intact.
3. The types and number of devices in the shipping containers are consistent with the packing list.
4. The devices are intact.

If short, wrong, excessive or damaged goods are found, maintain the goods while contacting the supplier as soon as possible.

Precautions

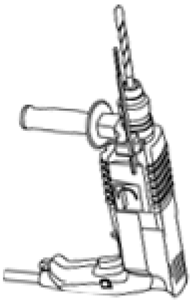
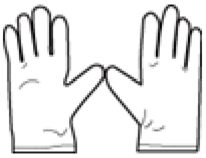
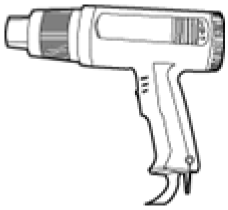
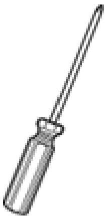
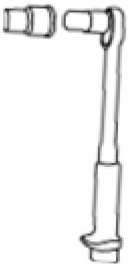
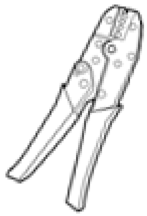
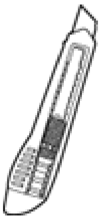
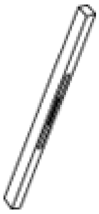
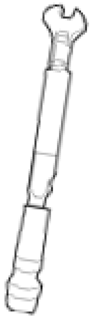
- Power on an EG860 within 24 hours after unpacking it. If you power off an EG860 for maintenance, restore power to the EG860 within 24 hours.

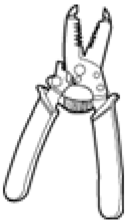
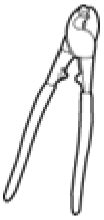
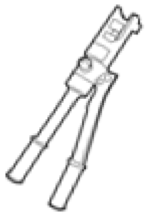
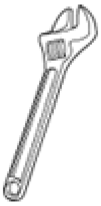
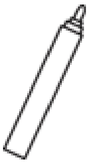
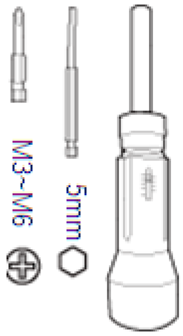
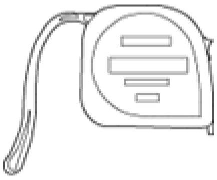
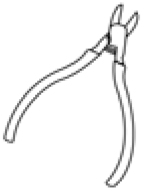
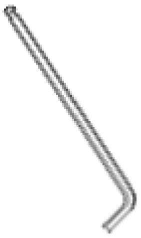
- If the temperature is -10℃ or below, it is recommended to heat EG860 by setting **Heat status** to **Enable** in **System** > **Hardware Settings** in WebUI.

Installation Tools

Table 4-1 lists the tools used to install an EG860.

Table 4-1 Installation tools

 Hammer drill (with Ø14 and Ø12 drill bits)	 ESD gloves	 Vacuum cleaner	 Heat gun
 Flat-head screwdriver (M2.5–M6)	 Phillips screwdriver (M2.5–M6)	 Socket wrench (M10)	 Crimping tool
 Rubber mallet	 Utility knife	 Level	 Torque wrench (5 N m–40 N·m)

 Wire stripper	 Wire clipper	 Multimeter	 Hydraulic pliers
 Adjustable wrench (capacity ⩾ 32 mm)	 Marker (diameter ⩽ 10 mm)	 Combination wrench (21 mm–21 mm) for installation on a pole (17 mm–17 mm) for installation on a wall	 Torque screwdriver 1 N m–5 N m
 Measuring tape	 Diagonal pliers	 Hex key (5 mm)	

4.3 Installation Procedure

This section describes how to install an EG860 on a pole and wall.

4.3.1 Mounting an EG860 on a Pole

This section describes how to mounting an EG860 on a pole in outdoor scenarios.

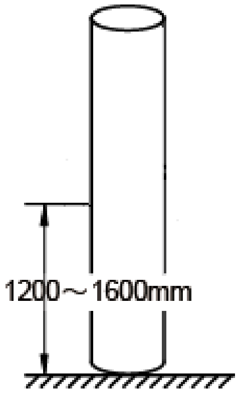
Context

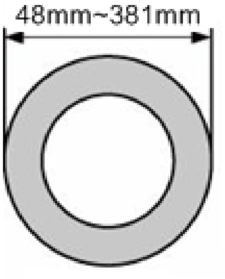
The following provides the requirements for installation space and components.

- Requirements for a mental pole of EG860

  Figure 4-2 shows the requirements for a mental pole of EG860.

Figure 4-2 Requirements for a mental pole of EG860 (unit: mm)





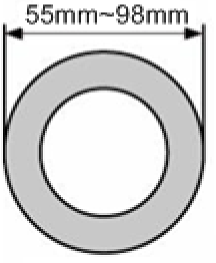
NOTE

- The product fitting bag contains 4 steel ties. Two of them are used for the mental pole whose diameter is lager than 114 mm, and the other two are used for the mental pole whose diameter is equal to or less than 114 mm.
- The steel tie for the mental pole whose diameter is lager than 114 mm is different from that for the mental pole whose diameter is equal to or less than 114 mm. Select different steel ties based on diameters of mental poles.

- Requirements for a mental pole of an antenna.

  Figure 4-3 shows the requirements for a mental pole of an antenna.

  Figure 4-3 Requirements for a mental pole of an antenna (unit: mm)

  The requirements for antenna installation are as follows:

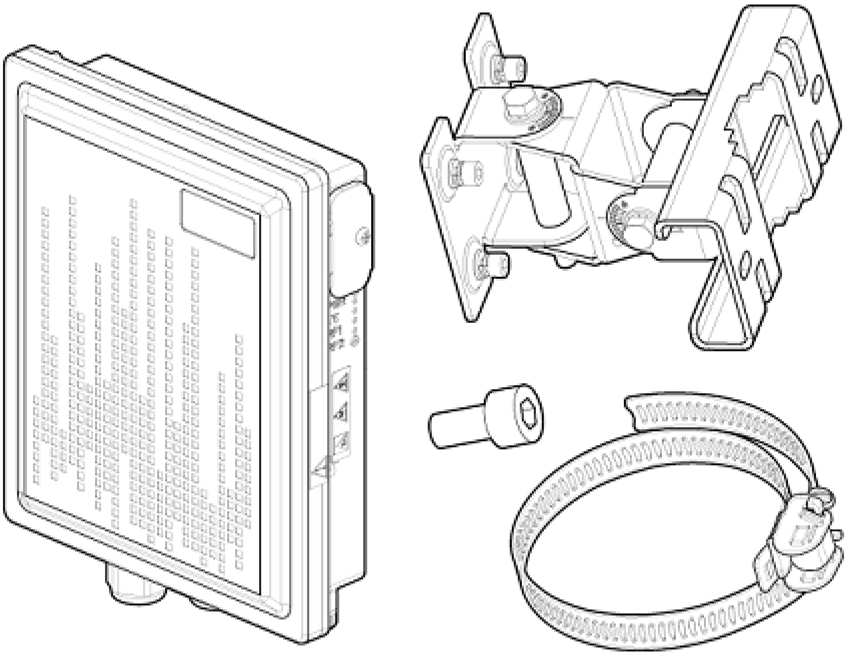
  – The installation of lightning rod is required.

  – The antenna must be mounted vertically.

  – The antenna must be mounted on the top of metal pole. If the antenna is to be mounted horizontally with the metal pole, the horizontal distance between the antenna and metal pole should not be less than 2λ (c=λ*f).

- Figure 4-4 shows an EG860 and installation components.

Figure 4-4 EG860 and installation components



NOTICE

To avoid direct lightning, EG860 must be installed in the protection angle of 45 degrees below a separate lightning rod, or protection angle of 45 degrees below a surrounding high-rise building.

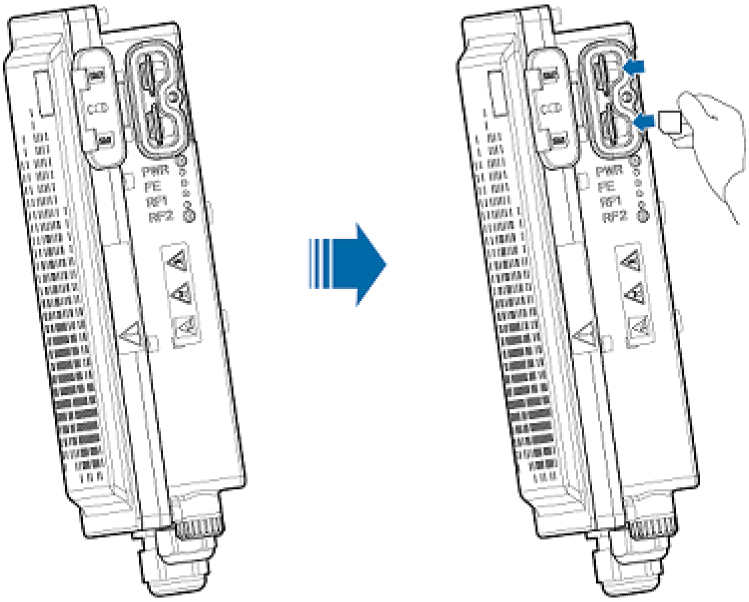
4.3.1.1 Mounting EG860 Equipment on a Pole

This section describes how to mount EG860 equipment on a pole.

Procedure

Step 1 **Optional:** Open the EG860 **SIM** card window and insert a **SIM** card, as shown in **Figure 4-5**.

Figure 4-5 Inserting a SIM card

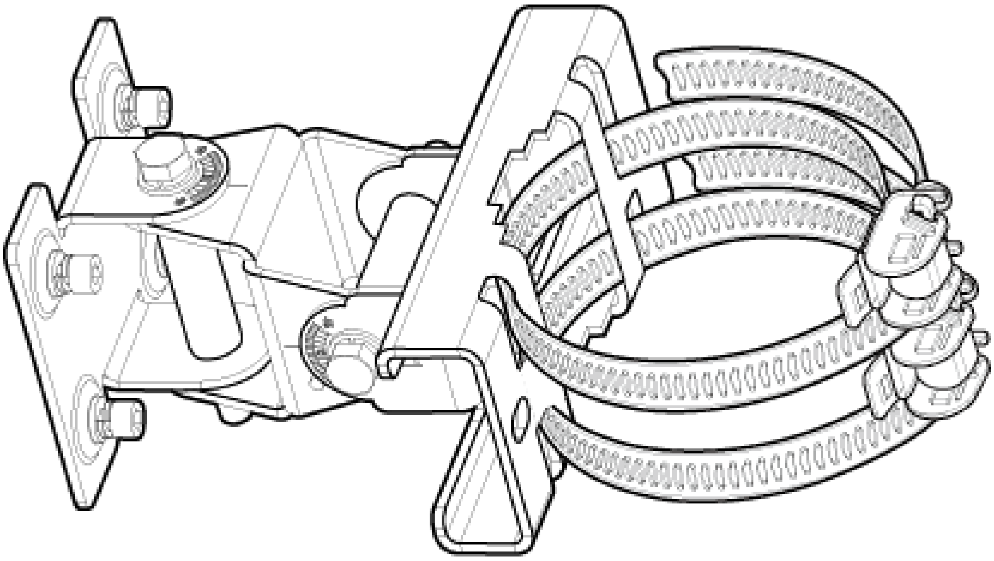


NOTE

Use a tweezer or a pair of needle-nose pliers to remove SIM cards.

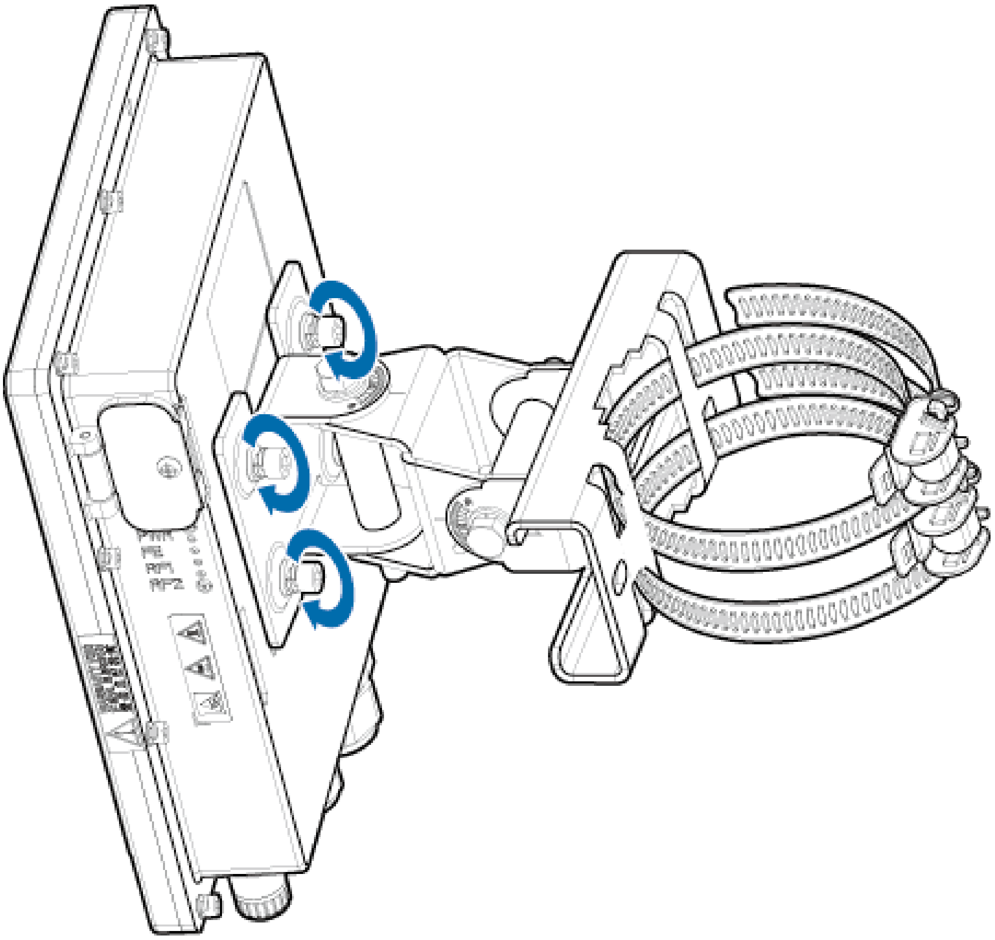
Step 2 Assemble steel strapping tapes with the installation component, as shown in **Figure 4-6**.

Figure 4-6 Assembling steel strapping tapes with the installation component



Step 3 Install the assembled installation component on the EG860, with the torque being 48 kgf.cm, as shown in **Figure 4-7**.

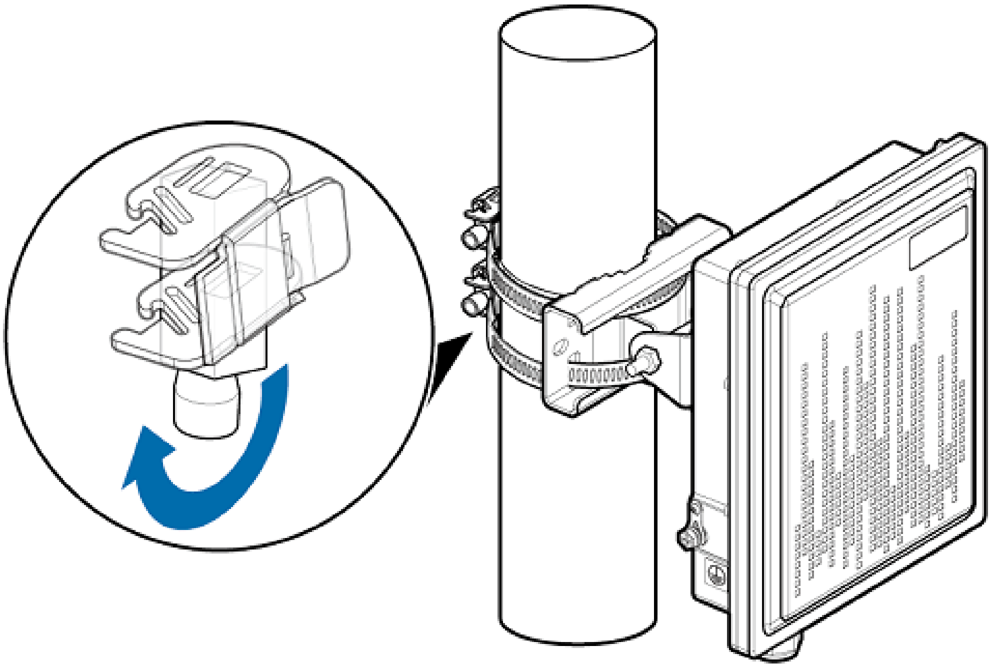
Figure 4-7 Installing an EG860 installation component



Step 4 Mounting the EG860 with the assembled installation component on the pole.

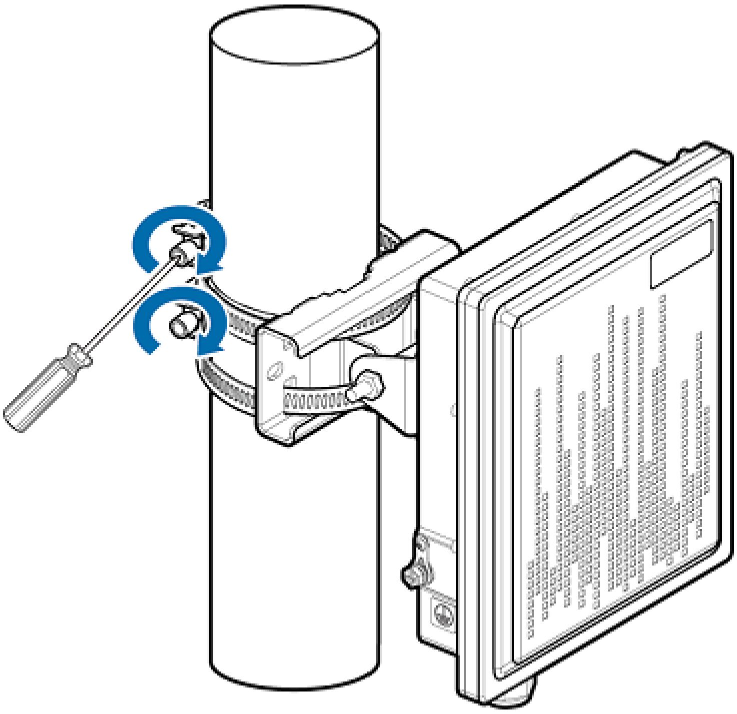
1. Roll the steel strapping tapes on the pole, let them go through the bayonet, and buckle up the bayonet after proper adjustment, as shown in **Figure 4-8**.

Figure 4-8 Buckle up the bayonet



2. Use the inner hexagon tool to tighten the steel strapping tapes, with the torque being 48 kgf.cm, as shown in **Figure 4-9**.

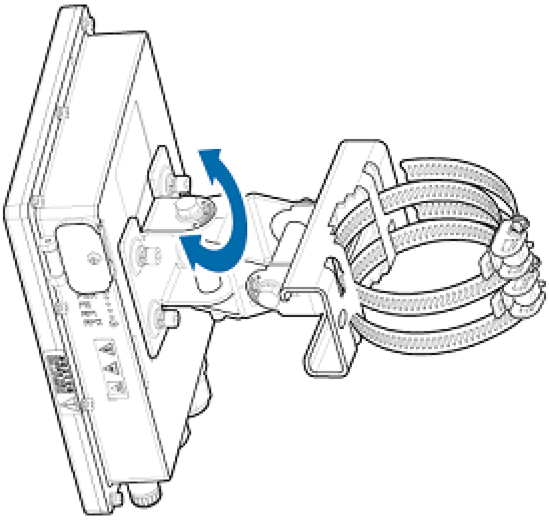
Figure 4-9 Tightening steel strapping tapes



Step 5 Properly adjust horizontal and vertical angles and tighten the screws on the top and side of the installation component.

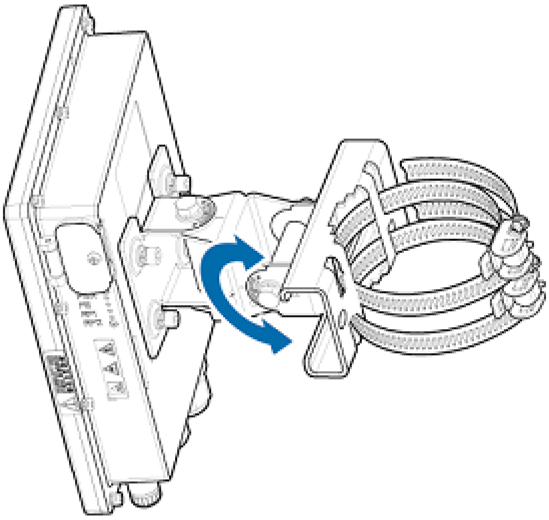
- Properly adjust the horizontal angle and tighten the screws on the top of the installation component, with the torque being 120 kgf.cm and a maximum of 45 degrees adjustment, as shown in **Figure 4-10**.

Figure 4-10 Horizontal angle adjustment



- Properly adjust the vertical angle and tighten the screws on the side of the installation component, with the torque being 120 kgf.cm and a maximum of 45 degrees adjustment, as shown in **Figure 4-11**.

Figure 4-11 Vertical angle adjustment



----End

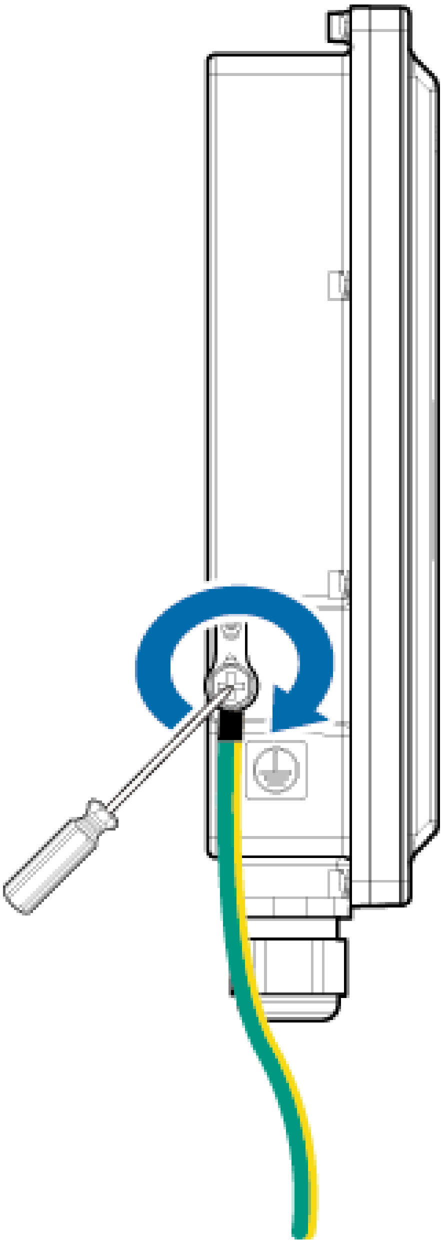
4.3.1.2 Connecting Cables to an EG860 Mounted on a Pole

This section describes how to connect cables to an EG860 mounted on a pole.

Procedure

Step 1 Connect the **PGND** cables, as shown in **Figure 4-12**.

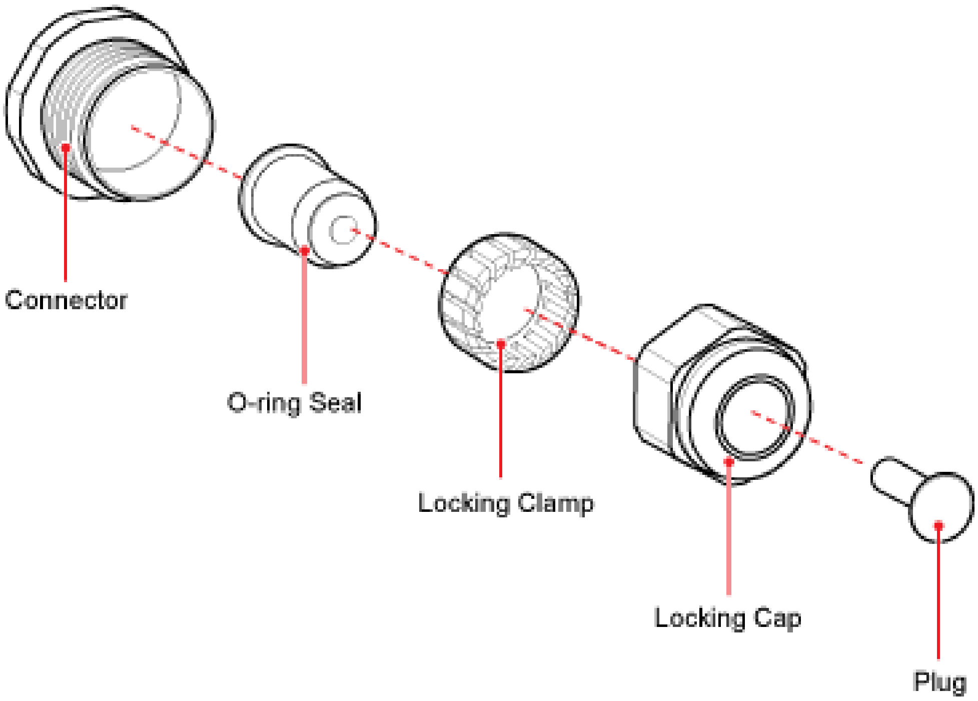
Figure 4-12 Connecting the PGND cable to the EG860



Step 2 Install the **POE** cable.

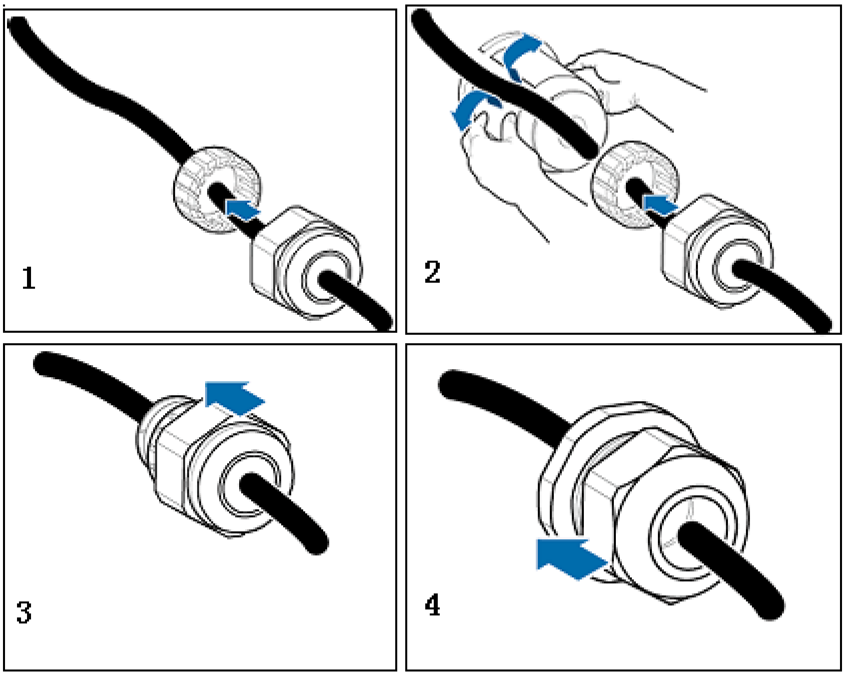
1. Loosen the PG connector at the **FE** port on the EG860. **Figure 4-13** shows the structure of the connector.

Figure 4-13 PG connector



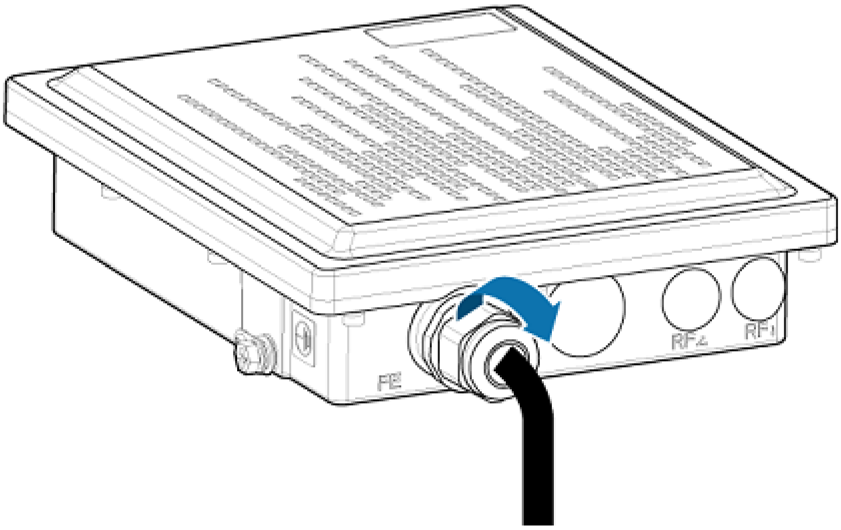
2. Insert a **POE** cable into the PG connector and ensure that the lock nut, rubber seal, and connector are compact, as shown in **Figure 4-14**.

Figure 4-14 Inserting a PoE cable into the PG connector



3. Inserting a **POE** cable into the **FE** port on the EG860, as shown in **Figure 4-15**.

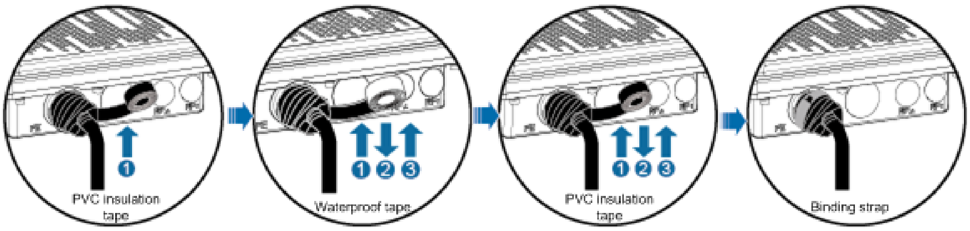
Figure 4-15 Inserting a PoE cable into the FE port on the EG860



4. **Optional:**

   In outdoor scenarios, waterproof the connecting joints as shown in **Figure 4-16**.

Figure 4-16 Waterproof



NOTE

- Before wrapping waterproof tape, stretch the tape evenly until the width of the tape is half of its original width.
- Wrap each layer of tape around the connector tightly and neatly, and ensure that each layer of tape overlaps more than 50% of the preceding layer.

a. Wrap each connector with one layer of insulation tape from bottom up.

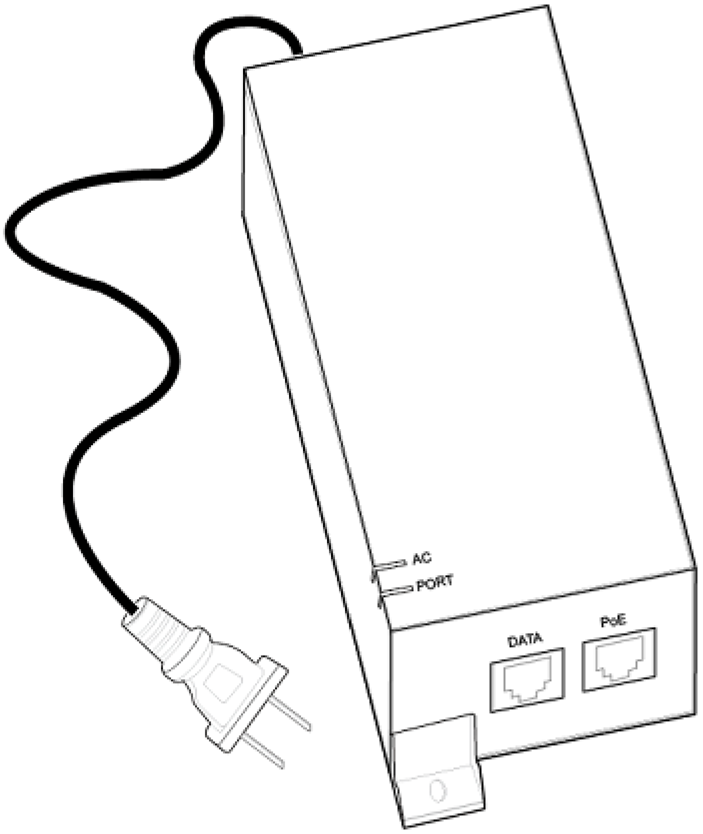
b. Wrap each connector with three layers of waterproof tape, from bottom up, then from top down, and finally from bottom up. Do not cut the tape until all the three layers of the tape are already wrapped. Wrap each layer of tape around the connector tightly.

c. Wrap each connector with three layers of PVC insulation tape, from bottom up, then from top down, and finally from bottom up. Do not cut the tape until all the three layers of the tape are already wrapped. Wrap each layer of tape around the connector tightly.

d. Bind the both ends of the tape by cable tie.

5. Connect one end of the **POE** cable to the **POE** adapter as shown in **Figure 4-17**.

Figure 4-17 Connecting a PoE adapter



DATA: connects to the network cable of a computer or a camera. PoE: connects to a **POE** cable.

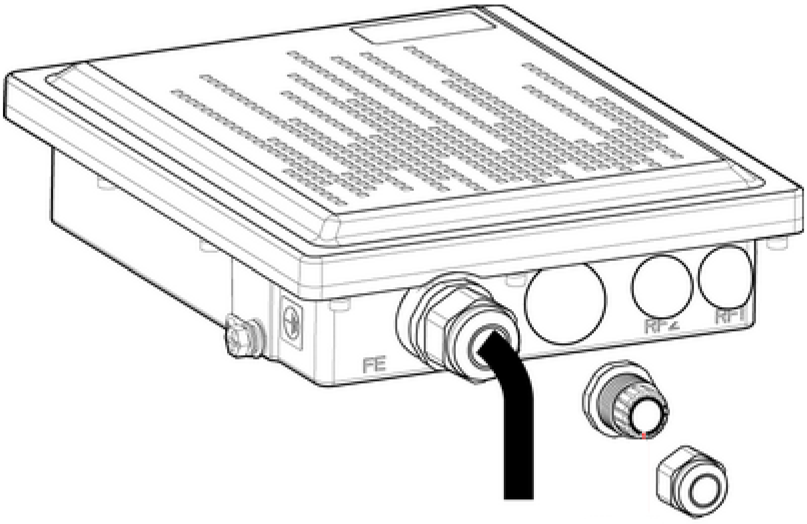
NOTE

In the outdoor, it is recommended to place the **POE** adapter in a surge protection box (provided by customer).

Step 3 Optional: Connect the power cable.

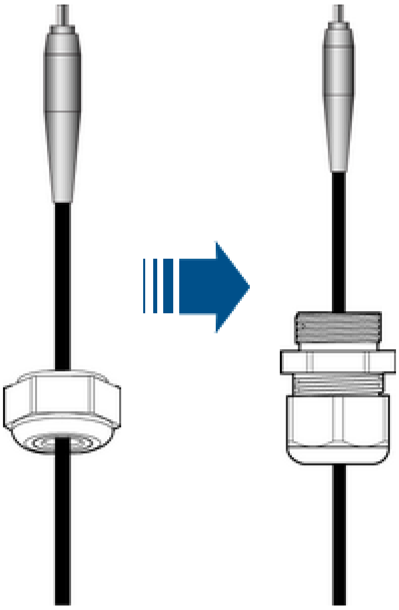
1. Screw the waterproof cover off the PWR connector, as shown in **Figure 4-18**.

Figure 4-18 Screwing the waterproof cover off the PWR connector



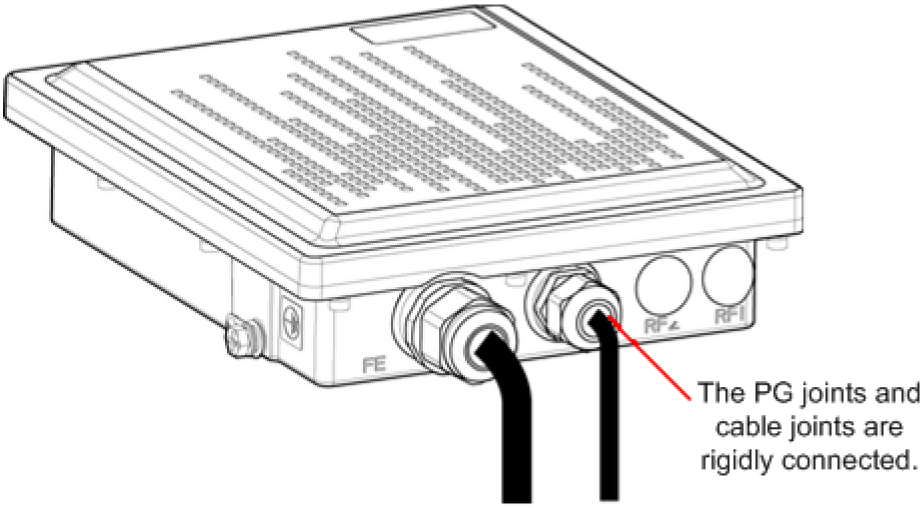
2. Pass the power cable through the PWR connector and tighten the waterproof cover, as shown in **Figure 4-19**.

Figure 4-19 Passing the power cable through the PWR connector and tightening the waterproof cover



3. Connect the power cable to the EG860 and tighten the waterproof cover, as shown in **Figure 4-20**.

Figure 4-20 Connecting the power cable to the EG860



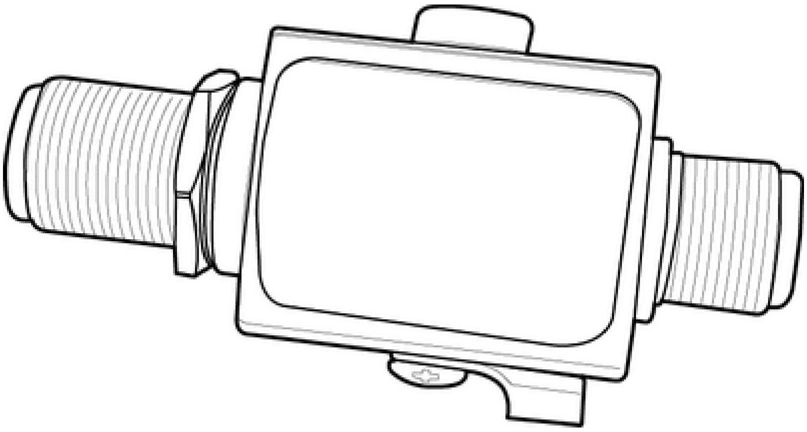
4. **Optional:** In outdoor scenarios, waterproof the connecting joints as shown in **2.4**.

Step 4 (This step is for the installation of external antenna. Please skip this step if built-in antenna is used.) Install an antenna. Connect the antenna to EG860 using a ground device (DC) for the central conductor. **Figure 4-21** shows the DC for the central conductor. The DC for the central conductor is mainly used for detecting external antenna and some surge protection.

EG860 supports single antenna and double antennas.

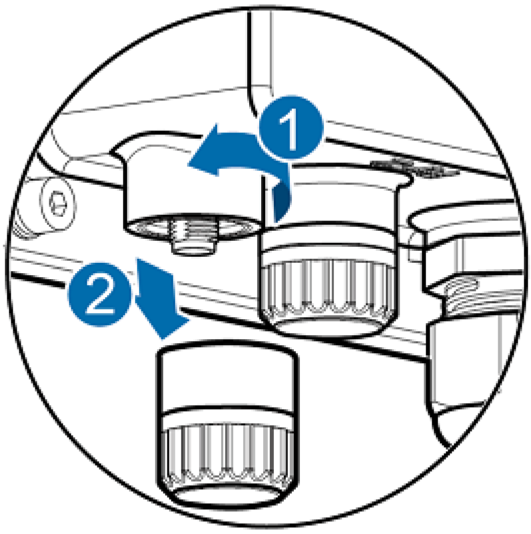
- In single antenna mode, the antenna connects with RF1 of EG860.
- In double antennas mode, the antennas respectively connects with RF1 and RF2 of EG860. The two antennas must be in the same horizontal position, with a minimal interval of 1.5 meters.

Figure 4-21 DC for the central conductor



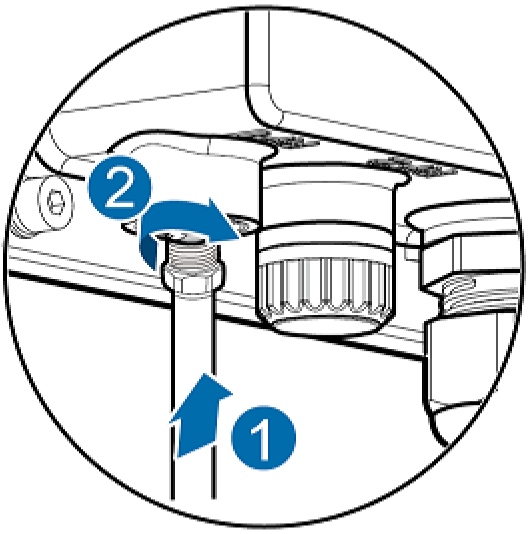
1. Loosen the antenna connector, as shown in **Figure 4-22**.

Figure 4-22 Loosening the antenna connector



2. Screw the **SMA** connector, with the torque being 10 kgf.cm, as shown in **Figure 4-23**.

Figure 4-23 Screwing the SMA connector



3. **Optional:** In outdoor scenarios, waterproof the connecting joints as shown in **2.4**.
4. Connect an external antenna through the DC for the central conductor, as shown in **Figure 4-24** and **Figure 4-25**.

Figure 4-24 Connecting an external antenna (single antenna)

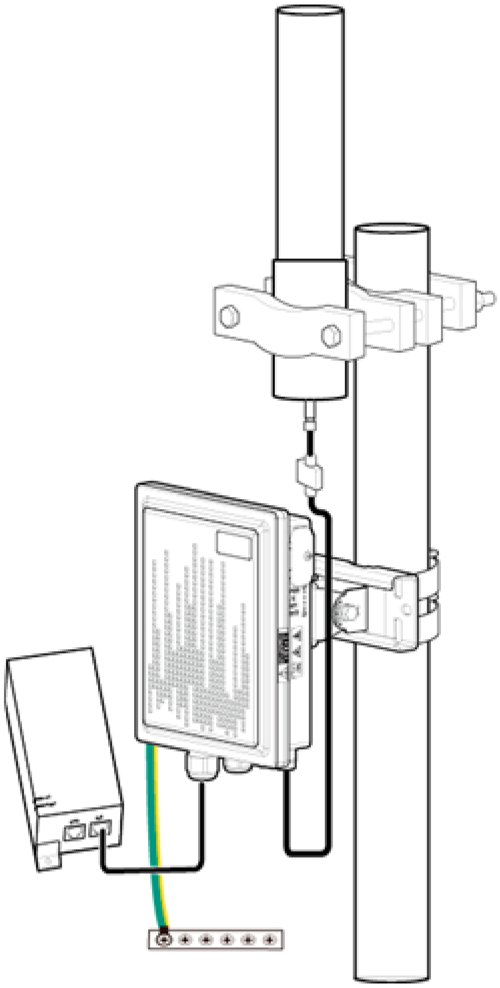
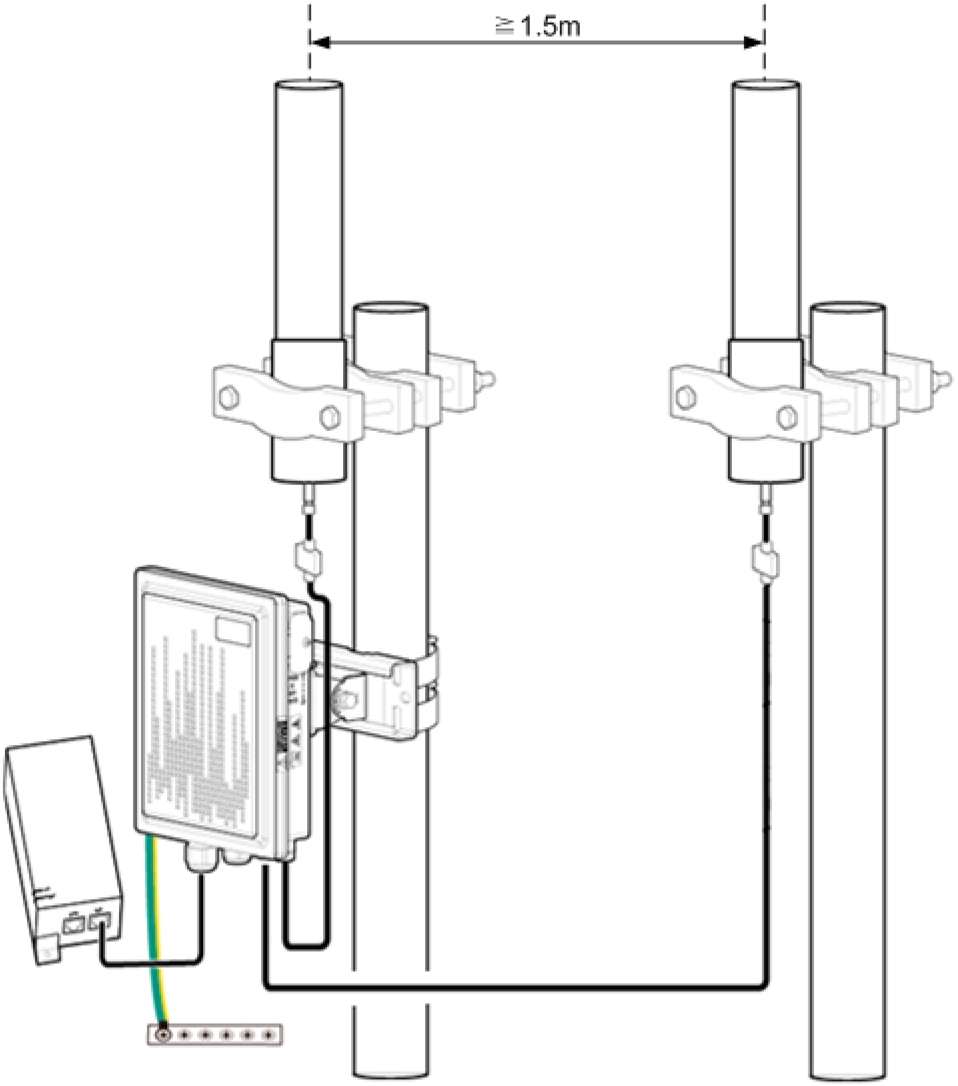


Figure 4-25 Connecting an external antenna (double antennas)



NOTE

- The ground device of central conductor needs to be fixed on the pole or other fixed blocks to avoid any unexpected swing. Also, waterproofing must be done at the connector of the device and RF cables.
- For details about how to install an external antenna, see the Antenna Installation Guide.

----End

4.3.2 Mounting an EG860 on a Wall

This section describes how to mount an EG860 in indoor scenarios.

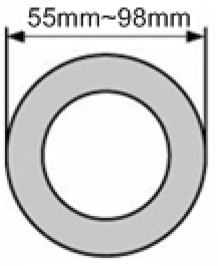
Context

The following provides the requirements for installation space and components.

- Requirements for a metal pole of an antenna.

  Figure 4-26 shows the requirements for a metal pole of an antenna.

  Figure 4-26 Requirements for a metal pole of an antenna (unit: mm)

  The requirements for antenna installation are as follows:

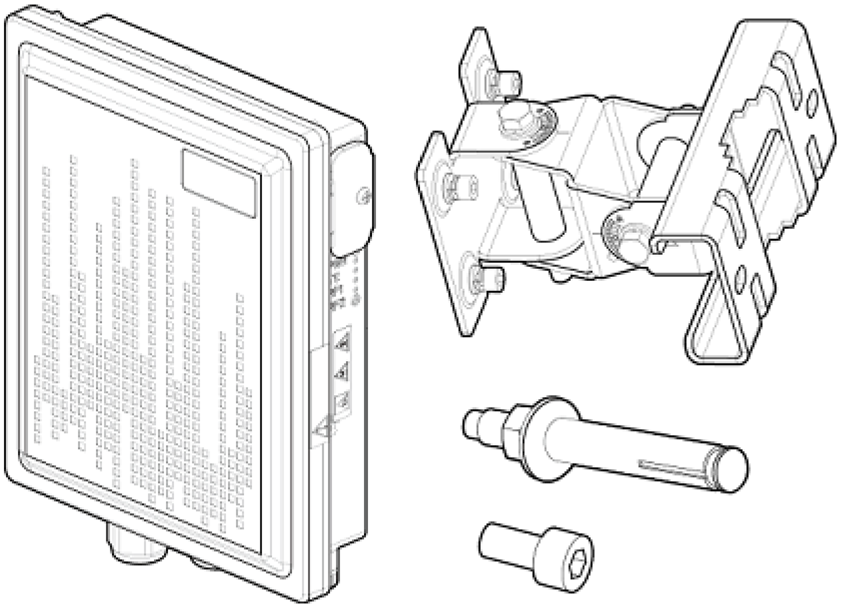
  – The installation of lightning rod is required.

  – The antenna must be mounted vertically.

  – The antenna must be mounted on the top of metal pole. If the antenna is to be mounted horizontally with the metal pole, the horizontal distance between the antenna and metal pole should not be less than 2λ (c=λ*f).

- Figure 4-27 shows an EG860 and installation components.

  Figure 4-27 EG860 and installation components

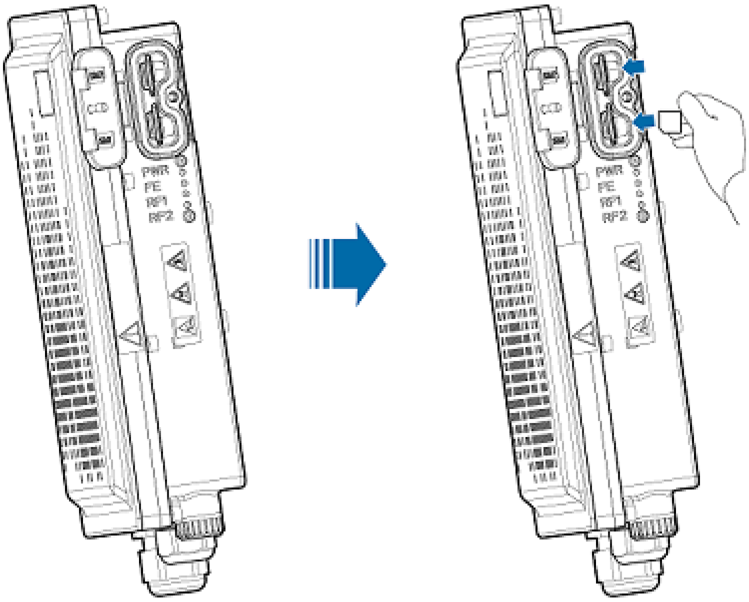
4.3.2.1 Mounting EG860 Equipment on a Wall

This section describes how to mount EG860 equipment on a wall.

Procedure

Step 1 **Optional:** Open the EG860 **SIM** card window and insert a **SIM** card, as shown in **Figure 4-28**.

Figure 4-28 Inserting a SIM card

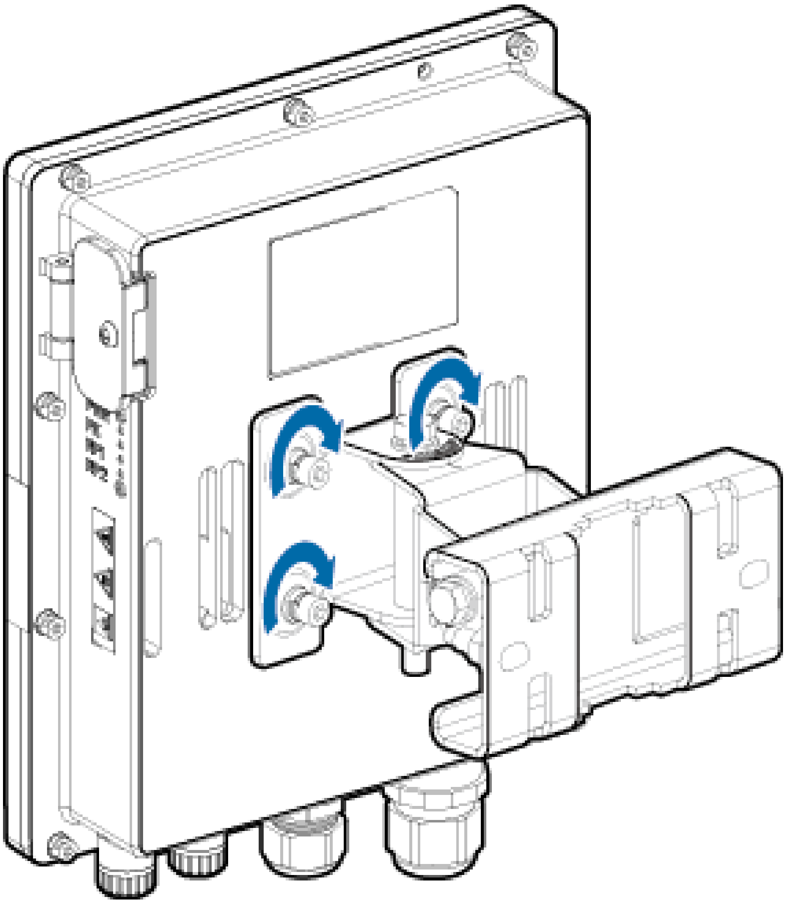


NOTE

Use a tweezer or a pair of needle-nose pliers to remove **SIM** cards.

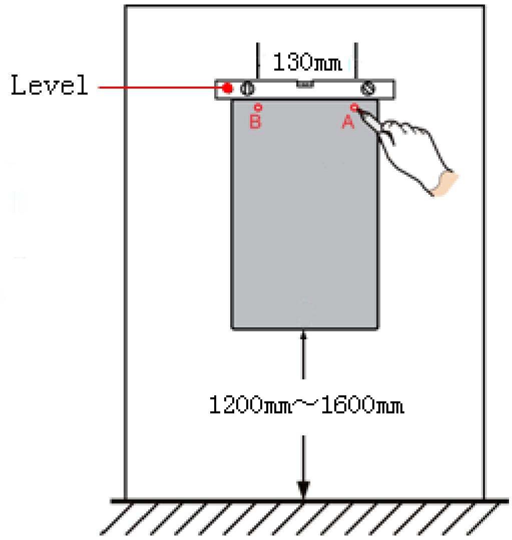
Step 2 Install the installation component on the EG860, with the torque being 48 kgf.cm, as shown in **Figure 4-29**.

Figure 4-29 Installing an EG860 installation component



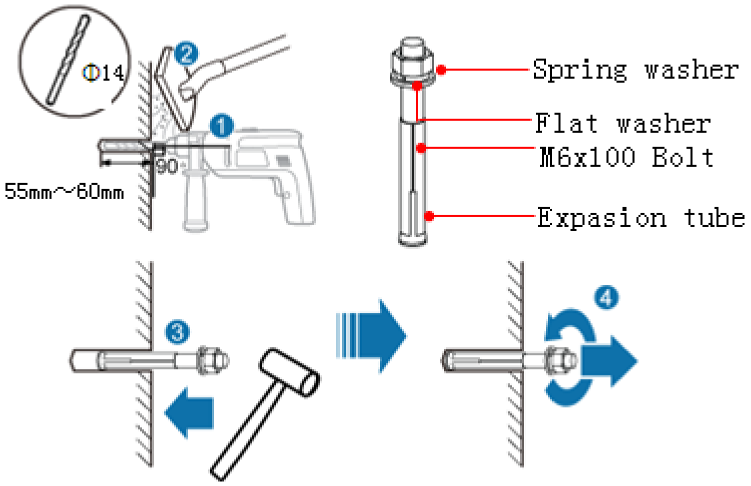
Step 3 Place a marking-off template against the wall, use a level to verify that the marking-off template is placed horizontally, and then mark anchor points with a marker, as shown in **Figure 4-30**.

Figure 4-30 Marking anchor points



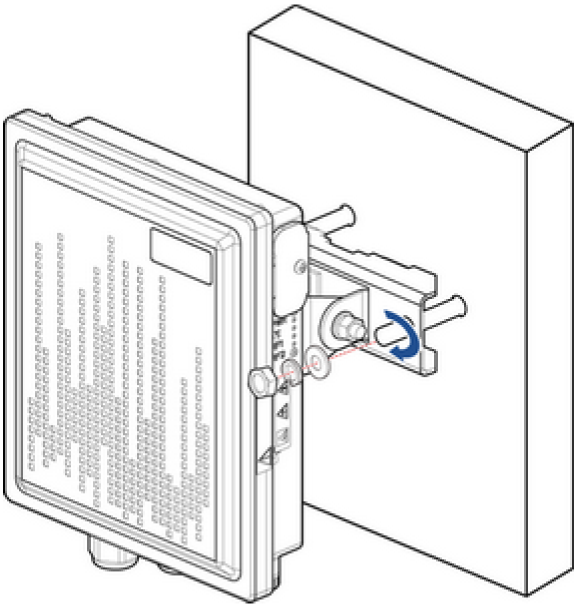
Step 4 Use a hammer drill with a Ø14 drill bit to drill a hole on the anchor points, install expansion bolts, and remove dust from the hole, as shown in **Figure 4-31**.

Figure 4-31 Installing an expansion bolt



Step 5 Align the installation holes in the bracket with the expansion bolt holes in the wall, fasten the nuts of the expansion bolts, and mount the EG860 on the wall, as shown in **Figure 4-32**.

Figure 4-32 Mounting the EG860 on the wall



Step 6 Properly adjust horizontal and vertical angles and tighten the screws on the top and side of the installation component. For details, see Mounting EG860 Equipment on a Pole **Step 5** of **4.3.1.1 Mounting EG860 Equipment on a Pole**.

----End

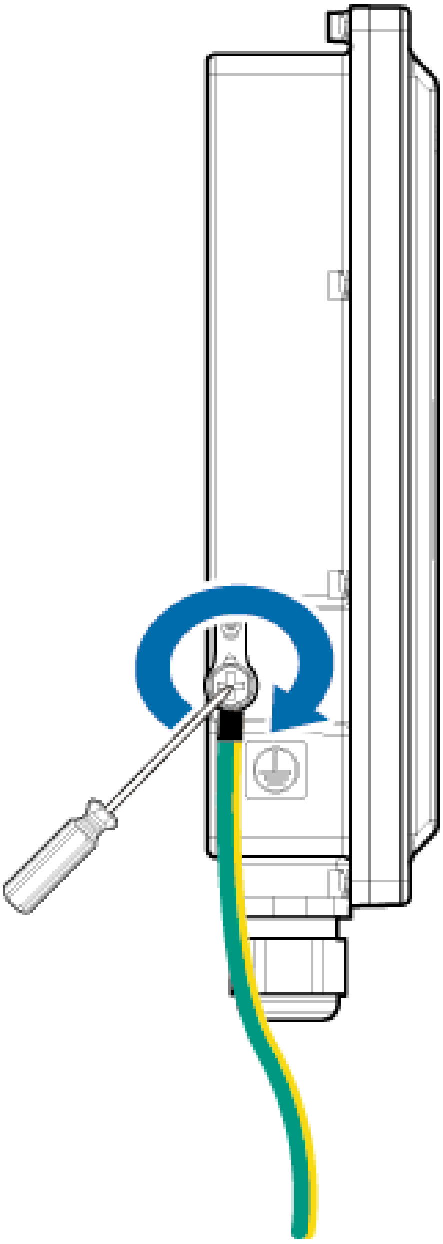
4.3.2.2 Connecting Cables to an EG860 Mounted on a Wall

This section describes how to connect cables to an EG860 mounted on a wall.

Procedure

Step 1 Connect the **PGND** cables, as shown in **Figure 4-33**.

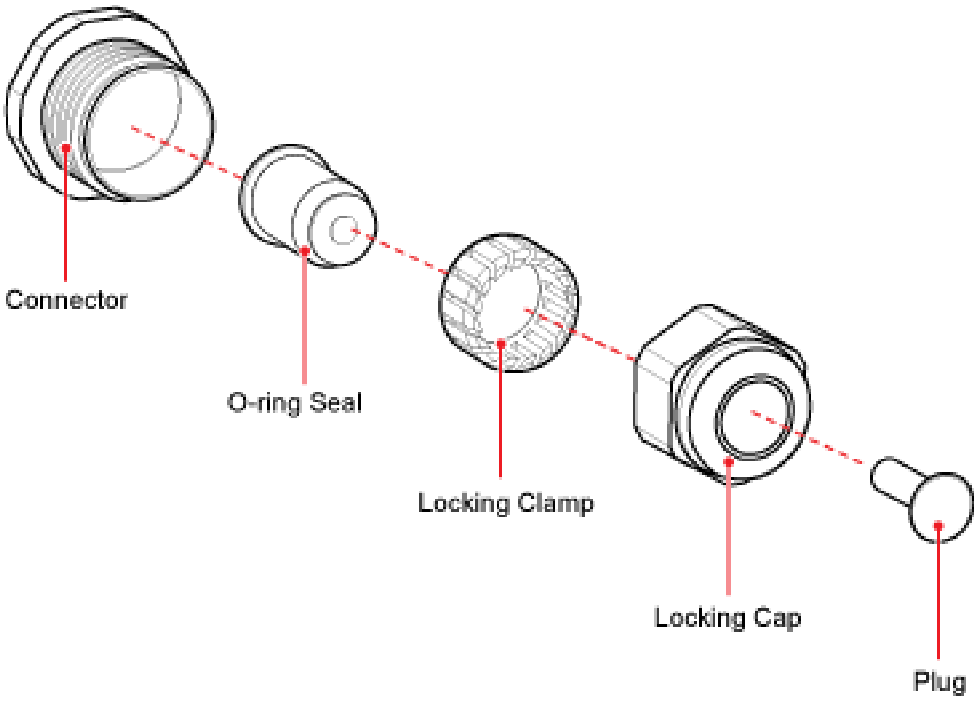
Figure 4-33 Connecting the PGND cable to the EG860



Step 2 Install the **POE** cable.

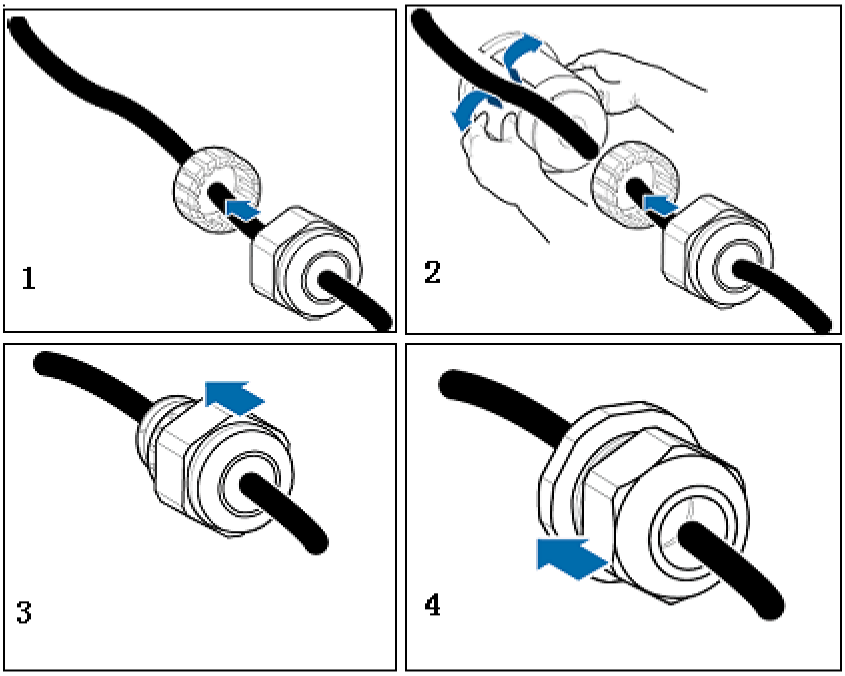
1. Loosen the PG connector at the **FE** port on the EG860. **Figure 4-34** shows the structure of the connector.

Figure 4-34 PG connector



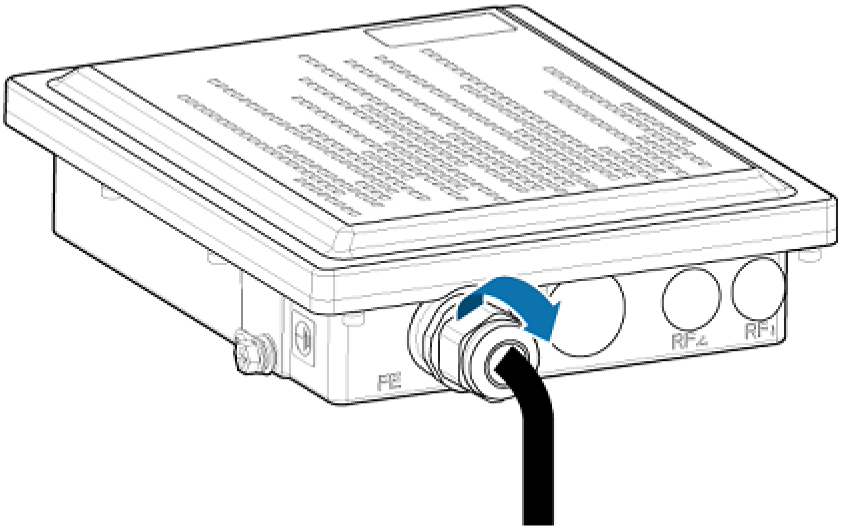
2. Insert a **POE** cable into the PG connector and ensure that the lock nut, rubber seal, and connector are compact, as shown in **Figure 4-35**.

Figure 4-35 Inserting a PoE cable into the PG connector



3. Inserting a **POE** cable into the **FE** port on the EG860, as shown in **Figure 4-36**.

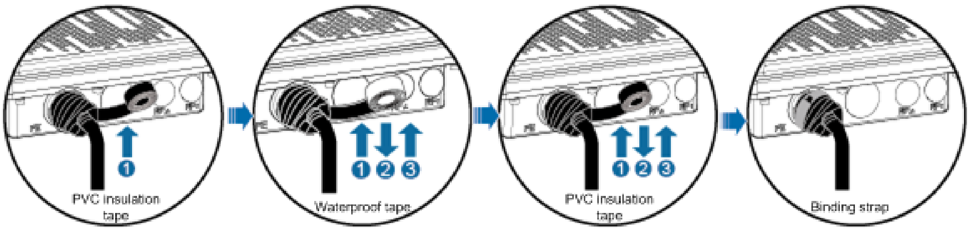
Figure 4-36 Inserting a PoE cable into the FE port on the EG860



4. **Optional:**

   In outdoor scenarios, waterproof the connecting joints as shown in **Figure 4-37**.

Figure 4-37 Waterproof



NOTE

- Before wrapping waterproof tape, stretch the tape evenly until the width of the tape is half of its original width.
- Wrap each layer of tape around the connector tightly and neatly, and ensure that each layer of tape overlaps more than 50% of the preceding layer.

a. Wrap each connector with one layer of insulation tape from bottom up.

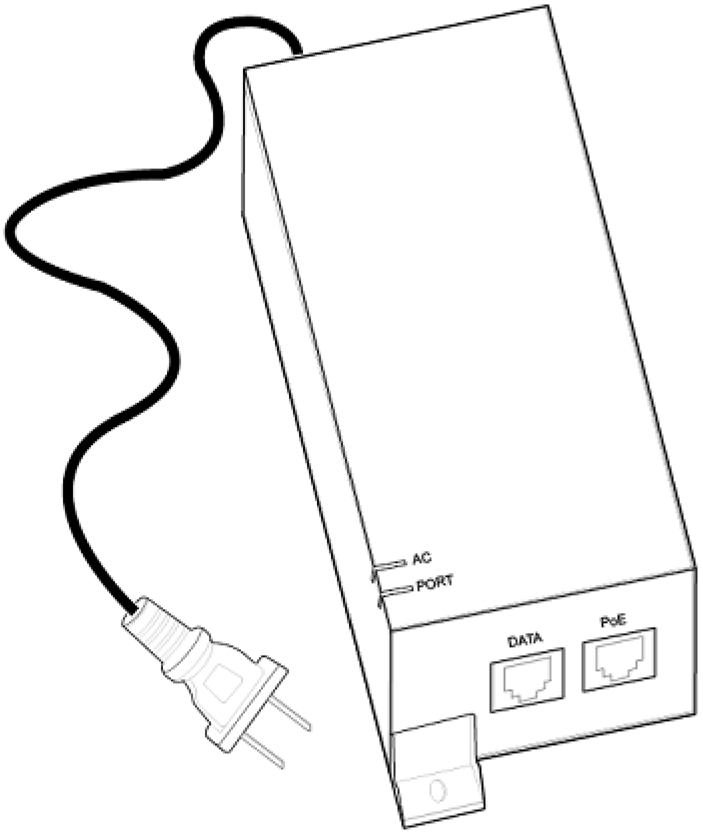
b. Wrap each connector with three layers of waterproof tape, from bottom up, then from top down, and finally from bottom up. Do not cut the tape until all the three layers of the tape are already wrapped. Wrap each layer of tape around the connector tightly.

c. Wrap each connector with three layers of PVC insulation tape, from bottom up, then from top down, and finally from bottom up. Do not cut the tape until all the three layers of the tape are already wrapped. Wrap each layer of tape around the connector tightly.

d. Bind the both ends of the tape by cable tie.

5. Connect one end of the **POE** cable to the **POE** adapter as shown in **Figure 4-38**.

Figure 4-38 Connecting a PoE adapter



DATA: connects to the network cable of a computer or a camera. PoE: connects to a **POE** cable.

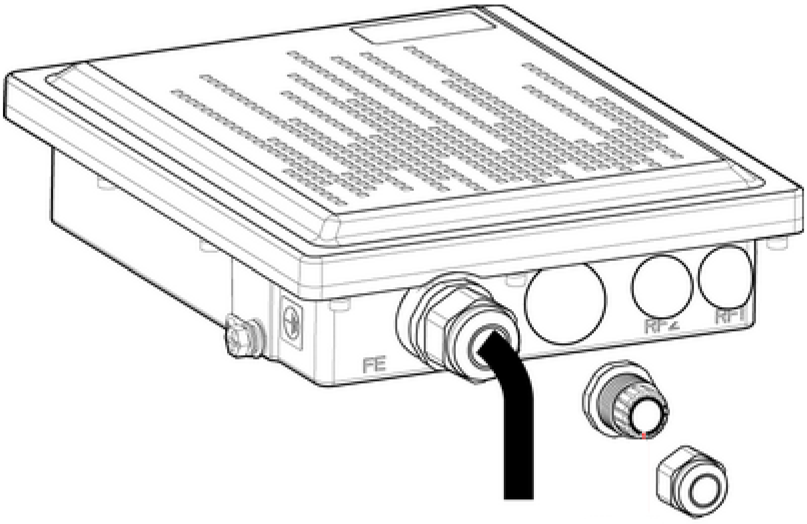
NOTE

In the outdoor, it is recommended to place the **POE** adapter in a surge protection box (provided by customer).

Step 3 **Optional:** Connect the power cable.

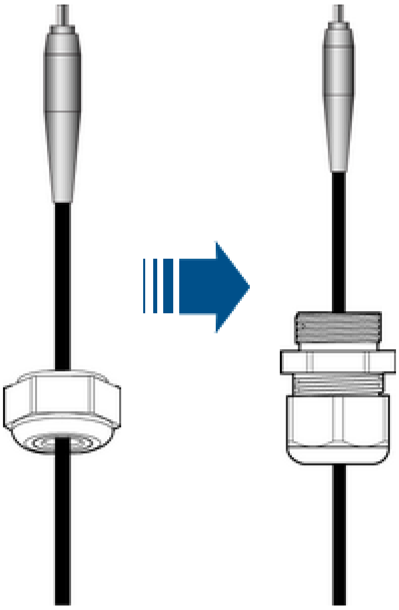
1. Screw the waterproof cover off the PWR connector, as shown in **Figure 4-39**.

Figure 4-39 Screwing the waterproof cover off the PWR connector



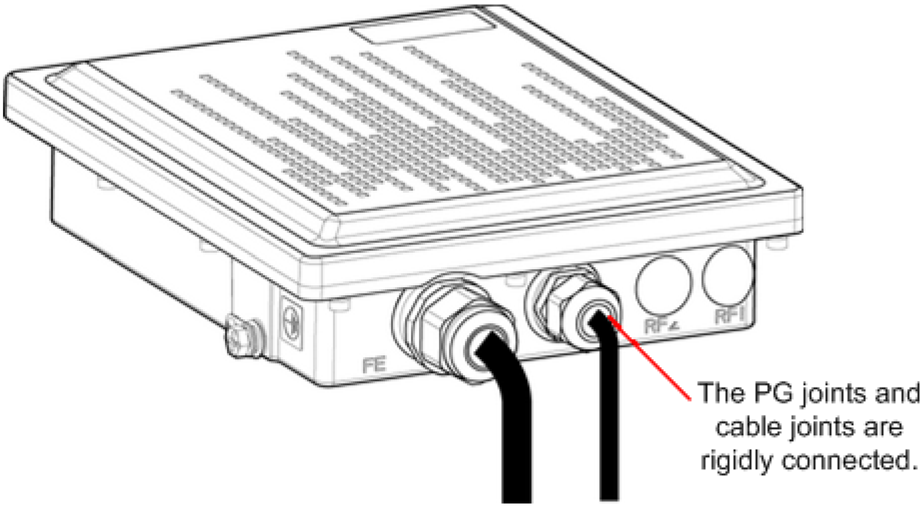
2. Pass the power cable through the PWR connector and tighten the waterproof cover, as shown in **Figure 4-40**.

Figure 4-40 Passing the power cable through the PWR connector and tightening the waterproof cover



3. Connect the power cable to the EG860 and tighten the waterproof cover, as shown in **Figure 4-41**.

Figure 4-41 Connecting the power cable to the EG860



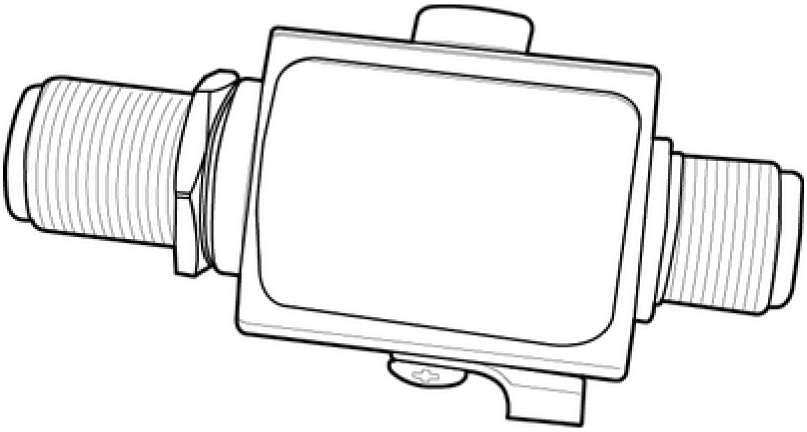
4. **Optional:** In outdoor scenarios, waterproof the connecting joints as shown in **2.4**.

Step 4 (This step is for the installation of external antenna. Please skip this step if built-in antenna is used.) Install an antenna. Connect the antenna to EG860 using a ground device (DC) for the central conductor. **Figure 4-42** shows the DC for the central conductor. The DC for the central conductor is mainly used for detecting external antenna and some surge protection.

EG860 supports single antenna and double antennas.

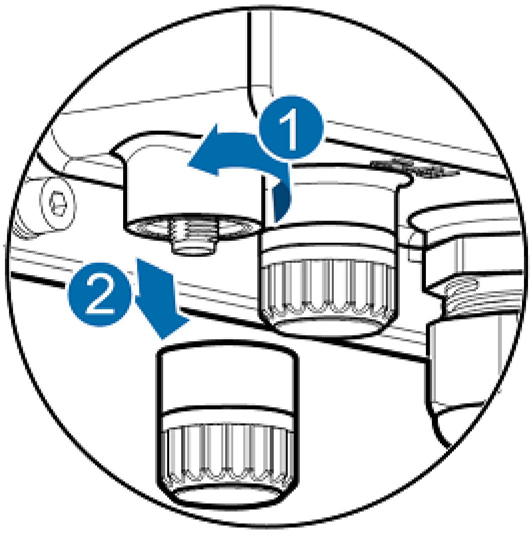
- In single antenna mode, the antenna connects with RF1 of EG860.
- In double antennas mode, the antennas respectively connects with RF1 and RF2 of EG860. The two antennas must be in the same horizontal position, with a minimal interval of 1.5 meters.

Figure 4-42 DC for the central conductor



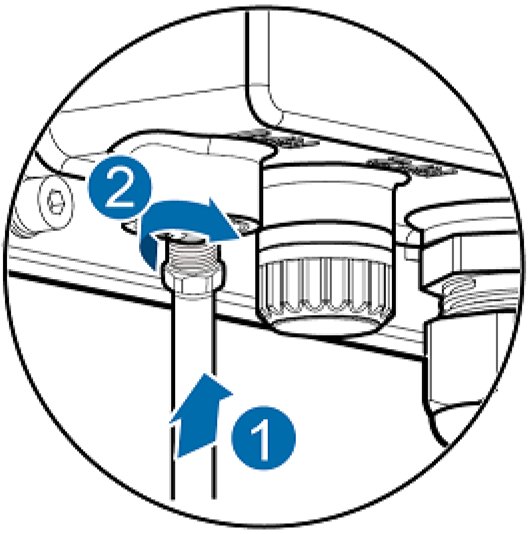
1. Loosen the antenna connector, as shown in **Figure 4-43**.

Figure 4-43 Loosening the antenna connector



2. Screw the **SMA** connector, with the torque being 10 kgf.cm, as shown in **Figure 4-44**.

Figure 4-44 Screwing the SMA connector



3. **Optional:** In outdoor scenarios, waterproof the connecting joints as shown in **2.4**.
4. Connect an external antenna through the DC for the central conductor, as shown in **Figure 4-45** and **Figure 4-46**.

Figure 4-45 Connecting an external antenna (single antenna)

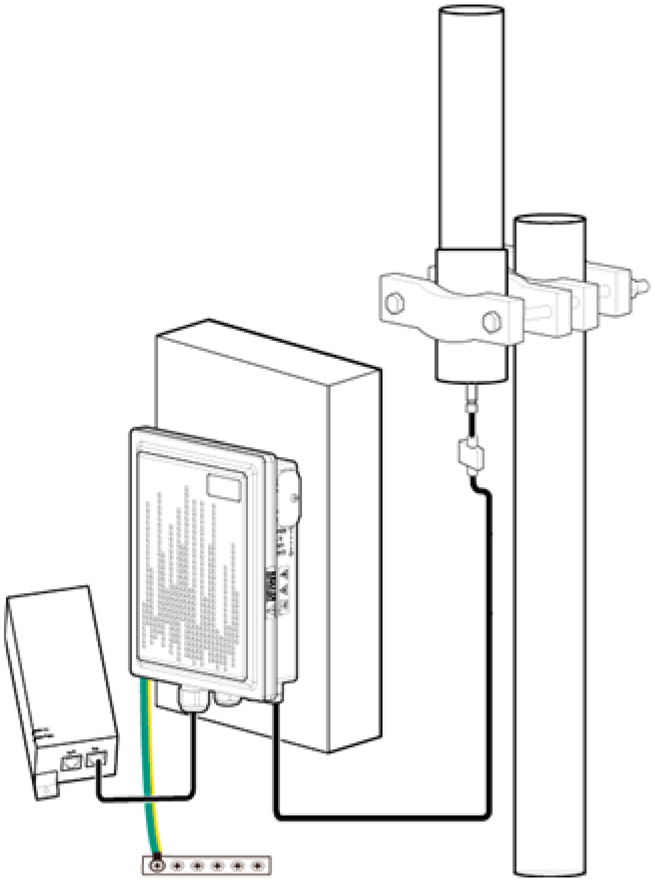
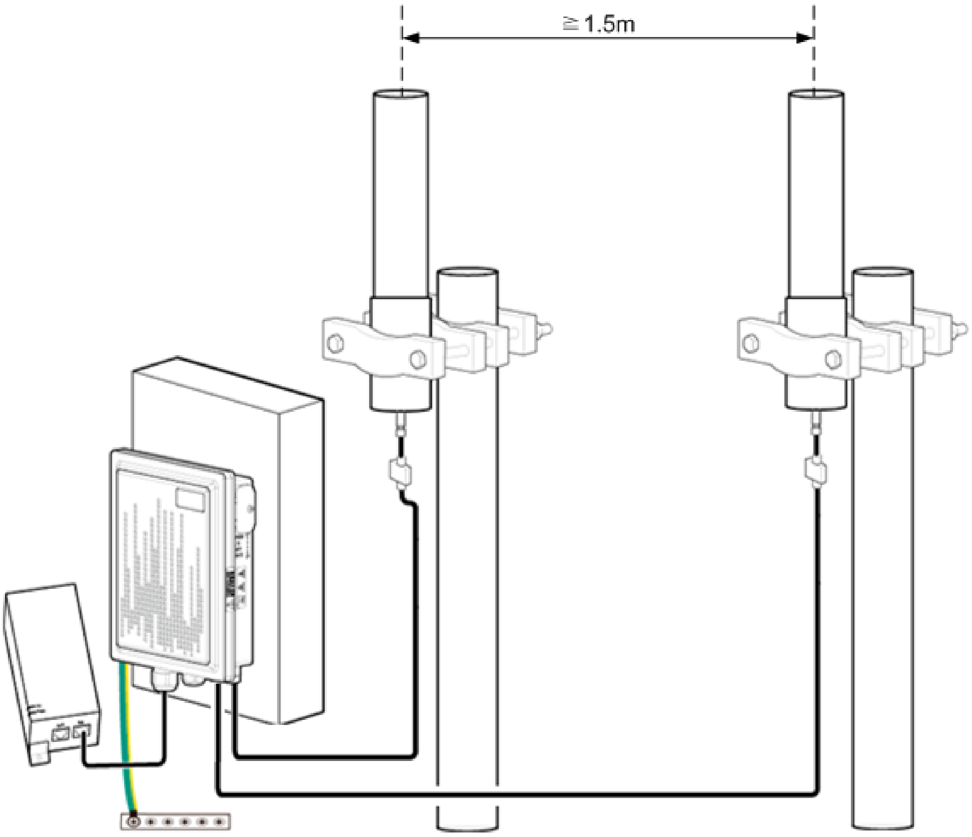


Figure 4-46 Connecting an external antenna (double antennas)



NOTE

- The ground device of central conductor needs to be fixed on the pole or other fixed blocks to avoid any unexpected swing. Also, waterproofing must be done at the connector of the device and RF cables.
- For details about how to install an external antenna, see the Antenna Installation Guide.

----End

4.4 Checking Installation

Check hardware and power-on status of an EG860 after installation.

Prerequisites

An EG860 has been properly mounted.

Procedure

Step 1 Check hardware installation.

Complete the items for hardware installation listed in **Table 4-2**.

Table 4-2 Checklist for hardware installation

No.	Check Item
1	The equipment position conforms to the engineering drawing and meets the space requirement. Sufficient space is reserved for equipment maintenance.
2	A **SIM** card is properly inserted.
3	The EG860 is properly mounted on a mental pole. The bracket is secure.
4	The EG860 is fixedly mounted on a wall. The holes in the bracket are aligned with those for expansion bolts and the bracket is placed against the wall securely and evenly.
5	Labels are correct, neat, and complete.

Complete the items for cable installation listed in **Table 4-3**.

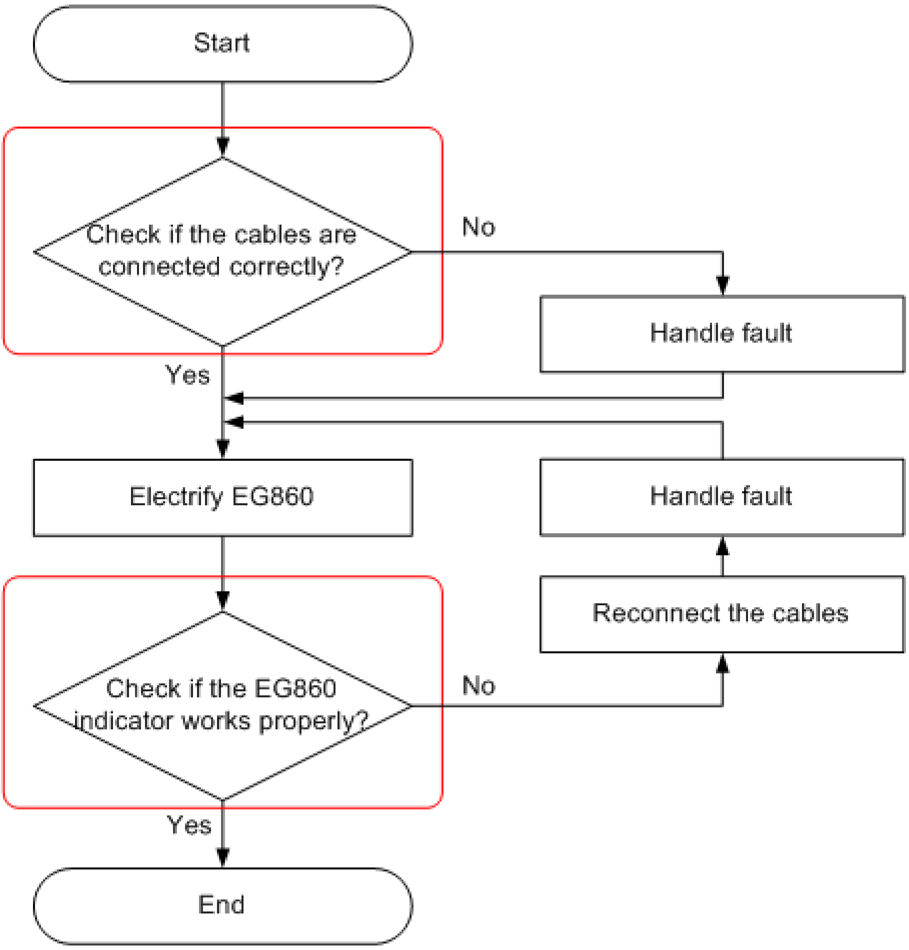
Table 4-3 Checklist for cable installation

No.	Check Item
1	The **PGND** cable is green and yellow. The NEG (-) cable is blue and the RTN (+) cable is black.
2	None of power cables or **PGND** cables is short-circuited or reversely connected.
3	The bare wires and lug handles at the wiring terminals are tightly wrapped up with **PVC** insulation tape.
4	The protection grounding of the EG860 and the surge protection grounding of the building share one group of ground conductors.
5	There are no connectors or joints on each power cable or **PGND** cable.
6	The connectors of the **POE** cable are securely connected.
7	The shield layer of the power cable is intact and the power cable is properly grounded.

No.	Check Item
8	Unused PG connectors are tightened and the protective covers of **SMA** connectors are sealed.

Step 2 Perform a power-on check by referring to **Figure 4-47**.

Figure 4-47 EG860 power-on check procedure


Start
Check if the cables are connected correctly?
No
Handle fault
Yes
Electrify EG860
Handle fault
Reconnect the cables
Check if the EG860 indicator works properly?
No
Yes
End

----End

5 Configuration

About This Chapter

Data configuration for EG860 can be performed by using WebUI or by auto-configuration.

5.1 Onsite Configuration (WebUI)
This section describes how to configure an EG860 through a web-based management interface.

5.2 Remote Configuration (Auto-configuration)
EG860 supports the auto-configuration function. Auto-configuration deployment operations can be performed to EG860 on the NMS system.

5.1 Onsite Configuration (WebUI)

This section describes how to configure an EG860 through a web-based management interface.

5.1.1 Log in to the WebUI

This section describes how to connect to EG860 by using the Web management interface.

Prerequisites

- An EG860 has been properly mounted.
- After being powered on, the EG860 operates normally based on default configuration parameters.
- EG860 has been registered to the core network.
- Internet Explorer 8.0 or later has been installed on the PC.

Procedure

Step 1 Open Internet Explorer and enter **https://192.168.1.1** in the address box.

NOTE

- A non-**IE** browser may have compatibility and security issues. After using a non-**IE** browser, log out of websites or close the browser in a timely manner.
- If you remain idle for 5 minutes after logging into the WebUI, a forced logout is executed.
- **192.168.1.1** is the default IP address of EG860. Use the new IP address to log in if the IP address of EG860 has been changed.

Step 2 On the Web management interface, input the **User name** and **Password**. The default **User name** of the system is **admin** and the **Password** is **4GCPE@TD**.

NOTE

- If you forget the password for logging in to the Web management interface, restore the EG860 factory settings in **Topology View** on the eOMC910 terminal management client.
- If you forget the password for logging in to the Web management interface and the eOMC910 cannot connect to the EG860, send the product back to the manufacturer. Keep your password secure after setting it.

Step 3 Click **Log In** to enter the Web management interface.

----End

5.1.2 Configuring Basic Data

This section describes how to configure the EG860 basic data.

Retain the default parameter settings and no more configuration is required.

To query the basic information about EG860, choose **System** > **Device information**. The information is displayed on the **Device information** tab.

To modify the **SIM** configuration parameter and **PLMN** configuration parameter, choose **System** > **SIM configuration**. The modification can be performed on the **SIM configuration** page. After the modification, restart the device to validate the new data.

5.1.3 Configuring Transmission Data

This section describes how to configure transmission data for EG860 in typical service scenarios.

Context

EG860 provides the following three transmission modes for configuration. Select a transmission mode based on the networking.

- **Routing Behind MS**

  When Routing Behind MS is applied, the uplink data will be forwarded via the available routes of EG860. The downlink data will be forwarded to EG860 according to the route set on the core network side.

- **NAT**

  NAT is to translate the **IP** address in the packet header of the **IP** data to another **IP** address.

- **GRE**

  GRE encapsulates data packets of some network-layer protocols such as **IP** and IPX. The encapsulated data packets can be transmitted over another network-layer protocol such as **IP**. GRE adopts the tunnel technology and belongs to the Layer 3 tunnel protocol of **IP**. A tunnel is a virtual point-to-point connection that provides a path for transmitting the encapsulated data packets. Data packets are encapsulated and decapsulated at the two ends of a tunnel.

- **L2TP**

  L2TP transmits PPP packets over a tunnel, allows a Layer 2 termination point and a PPP session endpoint to reside on different devices, and exchanges information using the packet switching technology, to extend the PPP model. **L2TP** combines the advantages of the L2F and PPTP protocols, and is an industry standard set by IETF.

Configuration principles for the four transmission modes are as follows:

- Four transmission modes both support one or more attached devices under an EG860. However, the operation for the Routing Behind MS transmission mode is relatively simple.
- If the network cannot traverse the public network, Routing Behind MS is recommended. If the network traverses the public network, NAT and GRE are recommended.
- When multi-cast services are required, only use GRE transmission mode.
- When Layer 2 networking transmission is used, only **L2TP** tunnel transmission can be used.
- When **L2TP** tunnel transmission is used, loopback networking must not be used. That is, two EG860s must not connect to the same switch.

Table 5-1 lists relevant NEs and devices for parameter setting in different transmission modes. For detailed configuration for other NEs and devices, see corresponding manuals.

Table 5-1 Transmission modes and relevant NEs and devices

Transmission Mode	Relevant NE and Device
Routing Behind MS	● EG860 ● Core network device ● Router (configured only when the 2U core network device is used and interworking between different EG860 is required) ● Video server (configured when multiple network adapters are configured) ● LAN host (configured when multiple network adapters are configured)
NAT	● EG860 ● Core network device ● Video server (configured when multiple network adapters are configured) ● LAN host (configured when multiple network adapters are configured)
GRE	● EG860 ● Core network device ● Router ● Video server (configured when multiple network adapters are configured) ● LAN host (configured when multiple network adapters are configured)
L2TP	● EG860 ● Router ● Video server (configured when multiple network adapters are configured) ● LAN host (configured when multiple network adapters are configured)

Application Scenarios

Devices attached to EG860 (such as sensor network gateways, cameras, and PCs) upload and download data through EG860. In addition, the server can also control the attached devices of EG860. **Figure 5-1** shows typical application scenarios.

Figure 5-1 Typical application scenarios of EG860

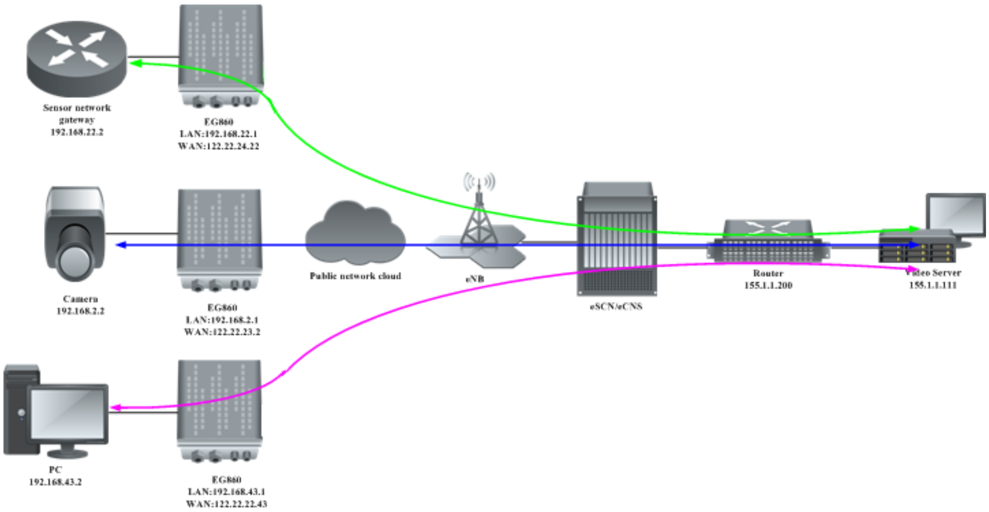

Sensor network gateway 192.168.22.2
EG860 LAN:192.168.22.1 WAN:122.22.24.22
Camera 192.168.2.2
EG860 LAN:192.168.2.1 WAN:122.22.23.2
Public network cloud
eNB
eSCN/eCNS
Router 155.1.1.200
Video Server 155.1.1.111
PC 192.168.43.2
EG860 LAN:192.168.43.1 WAN:122.22.22.43

Table 5-2 to Table 5-5 list the data plans for different transmission modes.

Table 5-2 Data plan for the Routing Behind MS transmission mode (take the attached sensor network gateway as an example)

Parameter	Example
IP address of the attached device of EG860	192.168.22.2
IP address of the LAN port on the EG860	192.168.22.1
IP address allocated by the core network to the WAN port on the EG860	122.22.24.22
IP address of the router	155.1.1.200
IP address of the video server	155.1.1.111

Table 5-3 Data plan for the NAT transmission mode (take the attached camera as an example)

Parameter	Example
IP address of the camera	192.168.2.2
IP address of the LAN port on the EG860	192.168.2.1
IP address allocated by the core network to the WAN port on the EG860	122.22.23.2
IP address of the router	155.1.1.200
IP address of the video server	155.1.1.111

Table 5-4 Data plan for the GRE transmission mode (take the attached PC as an example)

NOTE

EG860 supports both GRE single-tunnel transmission mode and GRE dual-tunnel transmission mode. The following table takes the GRE dual-tunnel transmission mode as an example.

Parameter	Example
IP address of the attached PC of EG860	192.168.43.2
IP address of the **LAN** port on the EG860	192.168.43.1
IP address allocated by the core network to the **WAN** port on the EG860	122.22.22.43
IP address of tunnel 1 on the EG860 side	43.0.0.2
IP address of tunnel 2 on the EG860 side	43.0.1.2
IP address of tunnel 1 on the router side	43.0.0.1
IP address of tunnel 2 on the router side	43.0.1.1
IP address of the core network to the router	178.1.7.7 178.1.8.7
IP address of the router to the core network	178.1.7.1 178.1.8.1
IP address of the router	155.1.1.200
IP address of the video server	155.1.1.111

Table 5-5 Data plan for the L2TP tunnel transmission mode (take the attached PC as an example)

Parameter	Example
IP address of the attached PC of EG860	192.168.43.2
IP address of the **LAN** port on the EG860	192.168.43.1
IP address allocated by the core network to the **WAN** port on the EG860	122.22.22.43
IP address of the router	155.1.1.200
IP address of the video server	155.1.1.111

Procedure

Configure the four transmission modes as follows: (the configuration data is from the data plan in **Application Scenarios**)

- Routing Behind MS

1. Choose **General Settings** > **Internet Settings**. The **Internet Settings** page is displayed.
2. In the **Internet Settings** page, set **Routing Behind MS** to **Enable**. The **Enable Routing Behind MS needs disenabling the natport function or clear the natport and the Internet will be reconnectted, continue or no?** dialog box is displayed. Click **OK**.
3. **Optional:** In the **Internet Settings** page, set **Quick Forward** to **Enable**.
4. In the **Internet Settings** page, click **Submit**.

- NAT

  When the NAT transmission mode is used, **Port Mapping** should be configured on the EG860 side so that the server can control the devices attached to EG860. If upload and download services are performed only on the EG860 side, configuring **Port Mapping** is not required.

1. Choose **General Settings** > **Internet Settings**. The **Internet Settings** page is displayed.
2. In the **Internet Settings** page, set **NAT** to **Enable**. **NAT Type** is **NAPT** by default.
3. **Optional:** In the **Internet Settings** page, set **Quick Forward** to **Enable**.
4. In the **Internet Settings** page, click **Submit**.
5. Choose **NAT Settings** > **Port Mapping**. The **Port Mapping** page is displayed.
6. In the **Port Mapping** page, configure **Port Mapping** based on the plan. For detailed configuration methods, see **7.4 NAT Settings**.

Table 5-6 Examples for port mapping configuration (configuring three tunnels)

Parameter	Example 1	Example 2	Example 3	Description
Type	Custom	Custom	Custom	When the value of **Type** is **Custom**, other parameters needed to be filled in manually. Set according to the plan.
Protocol	TCP/UDP	TCP/UDP	UDP	The Protocol used for port mapping
Remote Host	–	–	–	**IP** address of remote host
Remote Port Range	1-8079	8080	8081-65535	The port number of remote host

Parameter	Example 1	Example 2	Example 3	Description
Local Host	192.168.2.2	192.168.2.2	192.168.2.2	**IP** address of the camera
Local Port	-	80	-	The port number of local host
Status	Enable	Enable	Enable	Status of port mapping

- GRE

1. Choose **General Settings** > **Internet Settings**. The **Internet Settings** page is displayed.
2. In the **Internet Settings** page, configure data for **Tunnel**.

   Tunnel1 is a tunnel for downlink data. **Tunnel2** is a tunnel for uplink data. The configuration rules are as follows:

   - The **Peer IP** of **Tunnel1** cannot be the same with that of **Tunnel2**.
   - The **Tunnel IP** of **Tunnel1** cannot be in the same network segment with that of **Tunnel2**. The subnet mask is 255.255.255.0.

Table 5-7 Examples for GRE tunnel configuration

Parameter		Parameter Value	Description
Tunnel1	Peer IP	178.1.7.1	**IP** address of the router to the core network
	Tunnel IP	43.0.0.2	**IP** address of tunnel 1 on the EG860 side
Tunnel2	Peer IP	178.1.8.1	**IP** address of the router to the core network
	Tunnel IP	43.0.1.2	**IP** address of tunnel 2 on the EG860 side

3. In the **Internet Settings** page, click **Submit**.
4. Choose **General Settings** > **Routing**, the **Routing** page is displayed.
5. In the **Routing** page, configure **Static Routes** based on the plan. For detailed configuration methods, see **7.2.8 Routing**.

Table 5-8 Examples for static route configuration

Parameter	Parameter Value	Description
Destination IP	155.1.1.111	IP address of the video server
Subnet Mask	255.255.255.255	The subnet mask 255.255.255.255 indicates that the destination of routes is only one host.
Gateway IP	43.0.1.2	IP address of tunnel 2 on the EG860 side

- L2TP

1. Choose **General Settings** > **L2TP Settings**. The **L2TP** interface is displayed.
2. On the **L2TP Config** interface, set related parameters.
3. Click **Commit**.

Table 5-9 Example for L2TP configuration

Parameter	Parameter Value	Description
L2TP Tunnel	Enable	If this parameter is set to **Enable**, the L2TP transmission mode is enabled.
Peer Ip Addr	155.1.1.200	IP address of the router
User	admin	Authentication user name of the L2TP tunnel transmission mode. The user name must be the same as that configured on the router.
Password	TD4GCPE	Authentication password of the L2TP tunnel transmission mode. The password must be the same as that configured on the router.
Add to bridge	Enable	If this parameter is set to **Enable**, a BCP interface is added to the bridge to implement ETH over PPP over L2TPv2.

5.1.4 Configuring Dedicates Bearers

This section describes how to configure dedicated bearers.

To ensure the service performance, configure dedicated bearers based on specific service and planning.

For data configuration on the EG860 side, see **7.2.9 Dedicated Context**.

For data configuration on the side of other NEs, see the *QoS Feature Manual*.

5.2 Remote Configuration (Auto-configuration)

EG860 supports the auto-configuration function. Auto-configuration deployment operations can be performed to EG860 on the NMS system.

Prerequisites

- An EG860 has been properly mounted.
- After being powered on, the EG860 operates normally based on default configuration parameters.
- The EG860 is registered to the network and can be managed by the eOMC910.

Context

NOTE

Security control must be implemented because uncertainties exist in the environments where remote terminals are located. Users are advised to provide remote access as required. Locally accessing EG860 has fewer risks.

Procedure

The flowchart of remotely auto-configurable commissioning for EG860 using the eOMC910 is shown as **Figure 5-2**. See **Table 5-10** for details.

Figure 5-2 Flowchart for Auto-configurable Commissioning

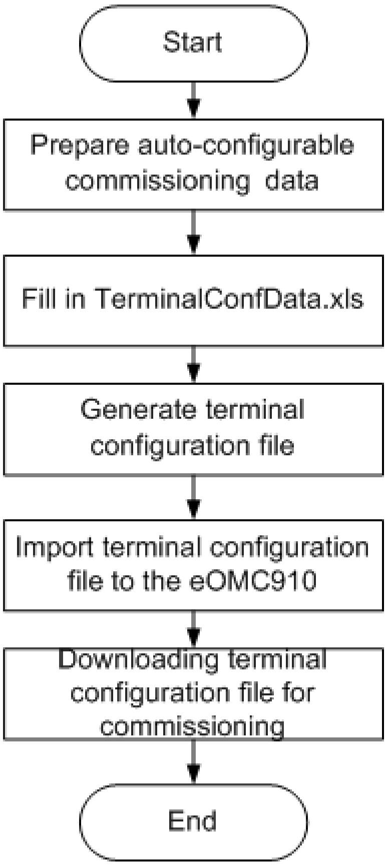

Start
Prepare auto-configurable commissioning data
Fill in TerminalConfData.xls
Generate terminal configuration file
Import terminal configuration file to the eOMC910
Downloading terminal configuration file for commissioning
End

Table 5-10 Description of the Auto-configurable Commissioning Steps

No.	Steps	Description
1	Prepare auto-configurable commissioning data	-
2	Fill in **TerminalConfData.xls**	Obtain complete directory of configuration file from the EG860 software package, which contains the **TerminalConfData.xls** sheet and other files. Fill **TerminalConfData.xls** based on the actual service scenario.

No.	Steps	Description
3	Generate terminal configuration file	Use eOMC910's Auto ConfigData Building tool to generate a terminal configuration file. See **Addendum** of *eOMC910 Terminal Management Client User Guide* in *eOMC910 Product Documentation* for details. NOTE If the matching EG860 is V200R003C00 version, after the terminal configuration file is generated by Auto ConfigData Building tool, use the **self opening station configuration file integrity check** tool to generate the verified terminal configuration file. For the detailed operations, please see the description of the Cover page in **TerminalConfigData.xls**.
4	Import terminal configuration file to the eOMC910	See **Commissioning Configurations** of *eOMC910 Terminal Management Client User Guide* in *eOMC910 Product Documentation* for details. NOTE After downloading the terminal configuration file, the EG860 user password will be set to the default password.
5	Downloading terminal configuration file for commissioning	

6 Maintenance

About This Chapter

This chapter describes how to maintain an EG860.

6.1 Preparations for Site Maintenance
Before maintaining an EG860, familiarize yourself with the site information, choose a maintenance task, and arrange tools and spare parts.

6.2 Powering on/off an EG860
Perform the following operations to power on or power off an EG860.

6.1 Preparations for Site Maintenance

Before maintaining an EG860, familiarize yourself with the site information, choose a maintenance task, and arrange tools and spare parts.

Learning Site Information

Learn the following information about the site before going onsite:

- Uncleared faults and alarms of the site
- Hardware configurations on the site
- Natural environment
- Spare parts

Choosing a Maintenance Task

Choose a proper maintenance task from the following items:

- Maintain the EG860 equipment room.
- Maintain power supply and grounding systems of an EG860.
- Maintain an EG860.

Arranging Tools and Spare Parts

Arrange necessary tools and spare parts for maintaining an EG860.

The following lists commonly used maintenance tools.

- Devices for frequency tests: include a frequency meter, a spectrum analyzer, connectors and cables.
- Power meter: is frequently used to measure and analyze the output power of an EG860.
- SiteMaster: is frequently used for antenna and feeder tests in terms of standing wave ratio, return loss, cable insertion loss, and fault location.
- Other devices:
  - Multimeter
  - Web **NMS**
  - Spare parts

6.2 Powering on/off an EG860

Perform the following operations to power on or power off an EG860.

Procedure

- Power on an EG860.
  1. Switch on the power supply connected to the EG860.

2. Check the status of the PWR indicator on the front panel. **Table 6-1** provides the status explanation for the PWR indicator.

Table 6-1 Status explanation for the PWR indicator

Status	Description
On	The power supply is functional.
Off	The power supply is abnormal. Troubleshoot as follows: ● Verify that the power cable is properly connected. ● Remove and connect the power cable, and then switch on the power supply. ● Contact technical support engineers of the equipment provider if the preceding operations do not work.

- Power off an EG860.

  Remove the power cable to power off the EG860 in the cases of special scenarios such as device replacement and intended outages and emergencies that the EG860 generates electric sparks or smoke.

----End

7 Reference

About This Chapter

This chapter describes how to use the Web network management system (NMS).

7.1 Status
This section describes how to check Internet, local area network (LAN), and wireless local area network (WLAN) status through the Status menu on the Web NMS.

7.2 General Settings
The Web NMS offers the General Settings menu to configure the subscriber identity module (SIM), Internet, Dynamic Host Configuration Protocol (DHCP), and wireless local area network (WLAN).

7.3 Security Settings
The Web NMS offers the Security Settings menu to configure Firewall General, MAC Filtering, and IP Filtering.

7.4 NAT Settings
Network Address Translation (NAT) settings, or port mapping settings, is necessary if a PC server is enabled and used by a WLAN, to allow port redirection for access from the WLAN to the server.

7.5 QoS Management
This section describes how to set QoS parameters on the **QoS Management** page.

7.6 VPN
This section describes how to configure VPN connections, and use the data service encryption function.

7.7 System
The Web NMS offer the System menu to view and configure parameters such as Device Information, Reset, Backup & Recovery, and Upgrade.

7.8 Logout
The login user interface is displayed upon a logout of the Web NMS.

7.1 Status

This section describes how to check Internet, local area network (LAN), and wireless local area network (WLAN) status through the Status menu on the Web NMS.

7.1.1 Internet

This page presents Internet connection status and traffic statistics.

Background Information

For the precise data about traffic statistics and online duration, contact related carriers.

Status

In Status, view the following information:

- **SIM card status**: displays the current status of the **SIM** card.
- **Network mode**: displays the network mechanism. If **--** is displayed in **Network mode**, no router is connected to the Internet.
- **Connection status**: displays the status of the current network.
- **IP** and **MAC**: respectively displays the **IP** address and the **MAC** address of the EG860.

Statistics

In **Statistics**, view the following information:

- **Received**: displays the number of received packets.
- **Sent**: displays the number of sent packets.
- **Total Volume**: displays the total number of received or sent bytes.
- **Packets**: displays the total number of received and sent packets.
- **Errors**: displays the number of error packets.
- **Discarded**: displays the number of discarded packets.

NOTE

Traffic statistics data are lost upon power-off of an EG860 but traffic is measured the next time the equipment is powered on.

7.1.2 LAN

This page presents local area network (LAN) connection status and traffic statistics.

Status

In **Status**, view the following information:

- **IP** and **MAC**: respectively displays the **IP** address and the **MAC** address of the EG860.
- **DHCP server**: displays the status of the **DHCP** server configured on a router.

- **LAN1**: display **LAN** port status.

Statistics

In **Statistics**, view the following information:

- **Received**: displays the number of received packets.
- **Sent**: displays the number of sent packets.
- **Total Volume**: displays the total number of received or sent bytes.
- **Packets**: displays the total number of received and sent packets.
- **Errors**: displays the number of error packets.
- **Discarded**: displays the number of discarded packets.

NOTE

Traffic statistics data are lost upon power-off of an EG860 but traffic is measured the next time the equipment is powered on.

7.1.3 WLAN

This page presents wireless local area network (WLAN) connection status and traffic statistics. A router provides four WLAN ports.

Status

In **Status**, view the following information:

- **SSID**: displays the name of the **WLAN Wi-Fi** access point.
- **IP** and **MAC**: respectively displays the **IP** address and the **MAC** address of EG860.
- **Broadcast**: displays **SSID** broadcast status of a **WLAN** port.
- **Wireless encryption**: displays the encryption mode of a **WLAN** port.

Statistics

In **Statistics**, view the following information:

- **Received**: displays the number of received packets.
- **Sent**: displays the number of sent packets.
- **Total Volume**: displays the total number of received or sent bytes.
- **Packets**: displays the total number of received and sent packets.
- **Errors**: displays the number of error packets.
- **Discarded**: displays the number of discarded packets.

NOTE

Traffic statistics data are lost upon power-off of an EG860 but traffic is measured the next time the equipment is powered on.

7.2 General Settings

The Web NMS offers the General Settings menu to configure the subscriber identity module (SIM), Internet, Dynamic Host Configuration Protocol (DHCP), and wireless local area network (WLAN).

7.2.1 SIM Card Settings

The personal identification number (PIN) of a subscriber identity module (SIM) card can be properly configured to prevent unauthorized access to a router.

Context

- The PIN management is only applicable to the physical SIM card but not to the virtual SIM card.
- In case of using the physical SIM card, the router cannot provide network service if the **PIN** check fails.

Procedure

Step 1 Choose **General Settings** > **SIM Card Settings**. The **SIM Card Settings** page is displayed.

Step 2 Set **PIN verification** to **Enable** or **Disable** as required.

When **PIN verification** is changed from **Enable** to **Disable**, or from **Disable** to **Enable**, the **PIN** value must be input in the **Input PIN** column.

Step 3 Set **Save my PIN** to **Enable** if required. If this parameter is set to **Enable**, the PIN is checked automatically each time a user accesses the network through the WAN port.

Step 4 Click **Submit**.

Step 5 Change the PIN as required.

1. Set **PIN verification** to **Enable**.
2. Set **Modification** to **Enable**.
3. Enter the old PIN in **PIN**.
4. Enter the new PIN in **New PIN**.
5. Enter the new PIN again in **Confirm PIN**.
6. Click **Submit**.

----End

7.2.2 Internet Settings

Different carriers have different access point name (APN) settings. If the APN parameters are incorrectly set, Internet service is inaccessible.

Context

- Communicate with the carrier before configuring the **APN**.

- When **Connection mode** is **Always on**, modify parameters on the page and click **Submit**, the number will be redialed.
- When **Connection mode** is **Manual**, modify parameters on the page and click **Submit**, and click **Connect** after the configuration takes effect.

Procedure

Step 1 Choose **General Settings** > **Internet Settings**. The **Internet Settings** page is displayed.

Step 2 Configure the parameters in **Data Connect**.

If **Data Connect** is **Connected**, the Internet is accessible.

1. Configure **Data APN**.

   If **Data APN** is set to **Auto APN**, the APN dynamically selects a network mode.

2. Configure the **Connection mode**.

   The related parameters are as follows:

   - **Always on**: indicates that a router is automatically connected to the Internet and always on. The **Connection mode** is set to **Always on** by default.
   - **Manual**: indicates that a router is manually connected to the network after it is powered on or disconnected due to network faults.

3. **Optional:** Set **NAT** to **Enable**. **NAT Type** is **NAPT** by default.

   ⚠ **NOTICE**

   If **NAT** is set to **Enable**, **Routing Behind MS** cannot be set to **Enable**.

4. If **DNS** is set to **Enable**, you must add the IP address of the DNS.
5. **Optional:** Set **Routing Behind MS** to **Enable**. The **Enable Routing Behind MS needs disenabling the natport function or clear the natport and the Internet will be reconnectted, continue or no?** dialog box is displayed. Click **OK**.
6. Set **Quick Forward** to **Enable**.
7. **Tunnel1** is a tunnel for multicast data. **Tunnel2** is a tunnel for unicast data. The configuration rules are as follows:

   - The **Peer IP** of **Tunnel1** cannot be the same with that of **Tunnel2**.
   - The **Tunnel IP** of **Tunnel1** cannot be in the same network segment with that of **Tunnel2**. The subnet mask is 255.255.255.0.

NOTE

- The GRE tunnel and quick forward cannot be configured at the same time.
- It is suggested not to configure GRE tunnel and routing behind MS at the same time.
- The WAN port will be restarted and services will be interrupted for seconds during routing behind MS and tunnel configuration.

Step 3 Click **APN Profile** to add the APN.

- An APN indicates an Internet access point provided by a carrier. Different carriers have different APN settings.

- If the APN in use does not match the operator, Internet services will be unavailable.
- The APN in use cannot be deleted.
- The default APN cannot be edited or deleted.

Step 4 Click **Edit APN Profile** and configure **APN**, **Dialed Number**, **User Name**, and **Password**.

Step 5 Click **Submit**.

----End

7.2.3 DHCP Settings

A Dynamic Host Configuration Protocol (DHCP) server manages all the equipment and assigns IP addresses to them within a LAN or WLAN.

Context

After changing parameter values of a **DHCP** server, perform the following operations:

- Log in to the EG860 again using the new IP address because the EG860 needs to be restarted.
- Check port mapping status.

Procedure

Step 1 Choose **General Settings** > **DHCP Settings**. The **DHCP Settings** page is displayed.

Step 2 In **LAN Host Settings**, configure **IP address**, **Subnet mask**, and **DHCP server**.

Configure related network parameters on the router.

Step 3 In **DHCP Settings**, configure **Start IP address**, **End IP address**, and **Lease time**.

The related parameters are as follows:

- Configure **Start IP address** and **End IP address** in the same network segment with **IP address** in **LAN Host Settings**.
- Set **Lease time** to values ranging from 1 min to 10080 min.

Click **Connected Devices**, the **Connected Devices** page is displayed. The **Devices List** displays the active devices connected to the EG860 through the LAN and WLAN.

Step 4 Click **Set Up List** and configure **Reserved Address List**.

If the **MAC** address of equipment is a static **IP** address, the **DHCP** server will always assign the same **IP** address to the equipment. The related parameters are as follows:

- Configure **MAC Address** and **IP Address** as required.
- **Status** indicates validity of all the preceding configurations. **Done** indicates that all the configurations are valid. **Waiting** indicates that the configurations will take effect upon restart.

Step 5 Click **Submit**.

----End

7.2.4 WLAN Settings

Wi-Fi equipment can connect to the Internet within the range of a WLAN.

Context

When **WLAN** parameters are modified, the **Wi-Fi** equipment needs to restart and the **WLAN** will be disconnected for about 30s.

Procedure

Step 1 Choose **General Settings** > **WLAN Settings**. The **WLAN Settings** page is displayed.

Step 2 Configure the parameters in **General Settings**.

The parameters in **General Settings** are basic control parameters for **WLAN** ports. The configurations are valid only when the **WLAN** is enabled. The related parameters are as follows:

- Set **WLAN Status** to **Enable** and configure the **Wi-Fi** function. **WLAN Status** is set to **Enable** by default.
- **Mode** can be set to **802.11b/g**, **802.11b**, **802.11g**, **802.11n**, or **802.11b/g/n**.
- **Channel** value range: **1-13**. If this parameter is set to **Auto**, the system automatically selects a channel with the lowest interference.
- **802.11n bandwidth** can be set to **20 MHz** or **20/40 MHz**.
- **Rate** is set to **Auto** by default.
- **Transmit power** can be set to **5%**, **30%**, **60%**, **80%**, **90%**, or **100%**. **90%** is recommended.
- If **QoS** is set to **Enable**, the QoS function is enabled for the WLAN.

Step 3 Configure the parameters in **Interface Profile**.

The related parameters are as follows:

- **Auto SSID name** is set to **Enable**, **SSID** is not manually set, and **SSID** is recommended to set it to **WLAN-SN**.
- **SSID** indicates a **WLAN** port, that is, the name of the user that accesses the WLAN.
- Set **Maximum number of connected devices** to a value from **1-32**.
- If **Hide SSID broadcast** is set to **Enable**, the **WLAN** port will not be scanned.
- If **AP isolation** is set to **Enable**, **Wi-Fi** equipment cannot interact.
- **Security** can be set to **NONE**, **WPA-PSK**, **WPA2-PSK**, or **WPA-PSK+WPA2-PSK**. **WPA2-PSK** is recommended.
- **WPA-PSK** is the password to access the WLAN, and consists of 8 to 63 ASCII characters or 8 to 64 hexadecimal characters. The value is **WLAN1-TDLTE** by default, and can be changed as required.
- **WPA encryption** can be set to **AES**, **TKIP**, or **TKIP+AES**. **AES** is recommended.

Step 4 Click **Submit**.

----End

7.2.5 WLAN Multi-SSID

WLAN Multi-SSID allows four channels for Wi-Fi LAN access at different speeds based on customer and application requirements.

Context

If **WLAN** Multi-SSID parameters are modified, **Wi-Fi** equipment needs to restart. The **WLAN** will be disconnected for about 30s.

Procedure

Step 1 Choose **General Settings** > **WLAN Multi-SSID**. The **WLAN Multi-SSID** page is displayed.

Step 2 Configure the parameters in **SSID List**.

When several **WLAN** ports are activated, corresponding channels can be provided for **Wi-Fi** access. The related parameters are as follows:

- **Auto SSID name** is set to **Enable**, **SSID** is not manually set, and **SSID** is recommended to set it to **WLAN-SN**.
- **SSID** indicates a **WLAN** port.
- Set **Maximum Number of Connected Devices** to values ranging from 1 to 32.
- If **Hide SSID broadcast** is **Enable**, the **WLAN** port will not be scanned.
- If **AP isolation** is **Enable**, **Wi-Fi** equipment cannot interact.
- **Security** can be set to **NONE**, **WPA-PSK**, **WPA2-PSK**, or **WPA-PSK+WPA2-PSK**. **WPA2-PSK** is recommended.
- **WPA-PSK** consists of 8 to 63 ASCII characters or 8 to 64 hexadecimal characters.
- **WPA encryption** can be set to **AES**, **TKIP**, or **TKIP+AES**. **AES** is recommended.

Step 3 Click **Submit**.

----End

7.2.6 WLAN Access Restrictions

WLAN access restriction management determines the Wi-Fi equipment that can access to a Wi-Fi LAN based on MAC addresses.

Context

When **WLAN** access restriction management parameters are modified, **Wi-Fi** equipment must be initialized. The **WLAN** will be disconnected for about 30s.

Procedure

Step 1 Choose **WLAN Access Restrictions** > **WLAN Access Restrictions**. The **WLAN Access Restrictions** page is displayed.

Step 2 Configure parameters in **WLAN MAC Control**.

The related parameters are as follows:

- **SSIDN**s can be configured with different rules of access restrictions.
- If **SSID1 MAC Access** is set to **Blacklist** and the **MAC** address list is empty, all the **Wi-Fi** equipment has access to the Internet within the **WLAN**.
- If **SSID1 MAC Access** is set to **Whitelist** and the **MAC** address list is empty, no **Wi-Fi** equipment has access to the Internet within the **WLAN**.

Step 3 Click **Set Up List** and configure **WLAN MAC List**.

Access restrictions for **Wi-Fi** devices are based on **MAC** addresses. If the **MAC** address of **Wi-Fi** equipment is changed, the previous filter rules become invalid. The related parameters are as follows:

- Configure **MAC** as required.
- If **For SSIDn** is **Enable**, the **MAC** filter rules are valid for **SSID**.

Step 4 Click **Submit**.

----End

7.2.7 Internet MTU

Set the maximum transmission unit (MTU) on an Internet port in **Internet MTU**.

Context

- A larger **MTU** presents a higher probability of Internet access failures.
- A packet larger than the **MTU** needs to be divided, which reduces transmission efficiency.

Procedure

Step 1 Choose **General Settings** > **Internet MTU**. The **Internet MTU** page is displayed.

Step 2 Configure the parameter in **Internet MTU Settings**.

Internet MTU: indicates the maximum length of the packets sent at an Internet port. The parameter ranges from 576 bytes to 1500 bytes. The recommended value is 1440 bytes. An **MTU** larger than 1500 bytes needs to be divided, which reduces transmission efficiency.

Step 3 Click **Submit**.

----End

7.2.8 Routing

If routers are cascaded within a LAN, a static route is required to allow network access for computers connected to the routers.

Context

Routers only work when connections are available.

Procedure

Step 1 Choose **General Settings** > **Routing**. The **Routing** page is displayed.

Step 2 Click **Add Item** to configure **Static Routes**.

Static routes function similarly with dynamic routes except that static routes are manually created and always valid, and have higher priority than the dynamic routes.

Step 3 Click **Submit**.

----End

7.2.9 Dedicated Context

This page describes how to configure a dedicated channel.

Procedure

Step 1 Choose **General Settings** > **Dedicated Context**. The **Dedicated Context** page is displayed.

Step 2 Click **Add** to configure parameters in **Dedicated Context**.

The related parameters are as follows:

- **CID**: indicates the channel identifier.
- **QCI**: indicates the **QoS** class identifier as shown in **Table 7-1**.

Table 7-1 QCIs

QCI	Resource Type	Priority	Data Packet Delay	Packet Loss Rate	Typical Service
1	GBR	2	100ms	10^{-2}	Session voice
2		4	150ms	10^{-3}	Session video (live broadcast)
3		3	50ms	10^{-3}	Real-time gaming
4		5	300ms	10^{-6}	Non-session video (buffer stream)
5	Non-GBR	1	100ms	10^{-6}	**IMS** signaling
6		6	300ms	10^{-6}	Voice (buffer stream) and **TCP**-based services such as Internet surfing, email, chatting, file transfer, point-to-point (PTP) file sharing, and line-by-line scan video.
7		7	100ms	10^{-3}	Voice and video (broadcast stream) and interactive game
8		8	300ms	10^{-6}	Voice (buffer stream) and **TCP**-based services such as Internet surfing, email, chatting, file transfer, point-to-point (PTP) file sharing, and line-by-line scan video.
9		9			

- Configure **DLGBR**, **ULGBR**, **DLMBR**, and **ULMBR** as required.

Step 3 Click **Edit** to configure the parameters in **TFT**.

The related parameters are as follows:

- **IP address**: indicates the **IPv4** address. Packets can be transmitted this **IP** address by using dedicated bearers.
- **MASK**: indicates the subnet mask.
- **Packet Filter Id**: indicates the identifier of packet filter.
- **Precedence**: indicates the priority of the relative packet filter.
- **Protocol Id**: ranges from 0 to 255 and is configured as required.
- **Local port** and **Remote port**: range from 0 to 65535 and are configured as required.
- **CID**: indicates the channel identifier.

Step 4 Click **Submit**.

----End

Example

Table 7-2 provides the typical **QoS** parameter settings for EG860.

Table 7-2 Typical QoS parameter settings for EG860

Service Type	CID	QCI	DLGBR (kbit/s)	ULGBR (kbit/s)	DLMBR (kbit/s)	ULMBR (kbit/s)
High-definition camera	2	4	1024	2688	10240	10240
Standard-definition camera	3	4	1024	1152	10240	10240
Checkpoint	4	6	-	-	-	-

7.2.10 IGMP Management

This page presents how to configure Internet Group Management Protocol (IGMP).

Context

The multicast mode includes the dynamic multicast mode and static multicast mode. In dynamic multicast mode, the query interval depends on the number of NEs. The more the NEs, the longer the query interval. A maximum of 32 records can be configured to static multicast.

Procedure

Step 1 Choose **General Settings** > **IGMP Management**. The **IGMP Management** page is displayed.

Step 2 Configure **IGMP Management**.

IGMP Proxy can be set to **Enable** as required.

Step 3 Set **IGMP mode** to **Dynamic IGMP** or **Static IGMP**.

NOTE

Configure the multicast source and multicast group if **IGMP mode** is set to **Static IGMP**.

Step 4 Set **Query interval time** to a value within the range from 10 to 256, the unit is second.

Step 5 Click **Submit**.

----End

7.2.11 L2TP Settings

This section describes how to set related parameters of the L2TP transmission mode on the **L2TP Settings** interface.

Context

- **L2TP** implements Layer 2 **VPN**.
- After **L2TP** parameters are modified successfully, the **L2TP** tunnel is re-established, and services are interrupted.
- You are not advised to use the **L2TP** tunnel and fast forwarding function at the same time.
- **L2TP** does not support tunnel authentication. Before enabling **L2TP**, disable the tunnel authentication mode on the peer router.

Procedure

Step 1 Choose **General Settings** > **L2TP Settings**. The **L2TP Settings** interface is displayed.

Step 2 If **L2TP Tunnel** is set to **Enable**, the **L2TP** transmission mode is enabled.

Step 3 Set **Peer Ip Addr** to the **IP** address of the L2TP server, that is, the **IP** address of the peer router.

Step 4 Set **User** and **Password** to the PPP authentication user name and password. The user name and password must be the same as those configured on the peer router.

Step 5 Set **Add to bridge** to **Enable**. BCP is added to the bridge to implement ETH over PPP over L2TPv2.

Step 6 Click **Commit**.

----End

7.2.12 FTP Settings

This section describes how to enable or disable an FTP port on the **FTP Settings** interface.

Procedure

Step 1 Choose **General Settings** > **FTP Settings**. The **FTP Settings** interface is displayed.

Step 2 If **FTP port** is set to **Enable**, the FTP port is enabled.

NOTE

The **FTP port** needs to be enabled when using V100R200C00 eOMC910 to manage V200R003C00 EG860 for configuration delivery, log import/export, and upgrading.

Step 3 Click **Submit**.

----End

7.2.13 Security access Settings

This section describes how to enable or disable the two-way authentication with eOMC910 on the **Security access Settings** interface.

Procedure

Step 1 Choose **General Settings** > **Security access Settings**. The **Security access Settings** interface is displayed.

Step 2 If **two-way authentication** is set to **Enable**, the two-way authentication with eOMC910 is enabled.

NOTE

The **two-way authentication** needs to be disabled when using V200R003C00 EG860 to connect to V100R200C00 eOMC910.

Step 3 Click **Submit**.

----End

7.3 Security Settings

The Web NMS offers the Security Settings menu to configure Firewall General, MAC Filtering, and IP Filtering.

7.3.1 Firewall General

This section describes how to configure firewall level and filter rules. The filter rules work only if the firewall is enabled.

Context

When default filter rules are used, data is transmitted unidirectionally from a **LAN** to a **WAN**.

The firewall filter mechanism is as follows:

- MAC Address Filter

  Only the filter rule for MAC address needs to be configured.

- IP Address Filter

  Only the filter rule for IP address needs to be configured.

- MAC Address Filter + IP Address Filter

  The filter rule for both MAC address and IP address need to be configured. Make sure the MAC address and IP address correspond to each other.

Procedure

Step 1 Choose **Security Settings** > **Firewall General**. The **Firewall General** page is displayed.

Step 2 Configure the parameters in **Firewall Level**.

The related parameters are as follows:

- **Current firewall level**: indicates the validity level of the firewall. To configure validity rules, set the current firewall level to **Custom**.
- **Firewall level**: can be set to existing levels or customized.

Step 3 Click **Submit**.

----End

7.3.2 MAC Filtering

MAC filtering prioritizes IP filtering. Packets that are not filtered at the MAC layer will be filtered at the IP layer.

Procedure

Step 1 Choose **Security Settings** > **MAC Filtering**. The **MAC Filtering** page is displayed.

Step 2 Click **Add Item** to configure the parameters in **MAC Whitelist**.

The related parameters are as follows:

- **Current MAC filtering status**: indicates the validity mode of MAC filtering.
- **MAC filtering mode**: indicates the filtering mode of a MAC address list. This parameter is described as follows:
  - If **MAC filtering mode** is set to **Blacklist**, the MAC addresses in the blacklist have no access rights to the network.
  - If **MAC filtering mode** is set to **Whitelist**, the MAC addresses in the whitelist have access rights to the network.
  - A maximum of 16 records can be configured for **Blacklist** and **Whitelist** respectively.

Step 3 Click **Submit**.

----End

Example

Table 7-3 provides the typical whitelist parameter settings for MAC address filter.

Table 7-3 Typical whitelist parameter settings

Index	MAC
1	00:1E:10:1F:04:05
2	00:E0:4C:98:58:98
3	D4:BE:D9:AF:F3:80

Index	MAC
4	44:19:B7:11:0A:9C
5	5C:F3:FC:2D:27:9F
6	D4:6E:5C:70:8F:66

NOTE

- 00:1E:10:1F:04:05 is the **MAC** address allocated by the core network to the **WAN** port on theEG860
- 00:E0:4C:98:58:98 is the **MAC** address of **PC** for EG860 local maintenance
- D4:BE:D9:AF:F3:80 is the service **MAC** address of the eOMC910
- 44:19:B7:11:0A:9C is the **MAC** address of the attached camera of EG860
- 5C:F3:FC:2D:27:9F is the **MAC** address of the Dispatcher
- D4:6E:5C:70:8F:66 is the **MAC** address of the WebUI for EG860

The above **MAC** addresses are for reference only. Please configure them according to the actual networking plan.

7.3.3 IP Filtering

A router determines whether to transfer a packet based on its source IP address, destination IP address, source port ID, destination port ID, and protocol type.

Procedure

Step 1 Choose **Security Settings** > **IP Filtering**. The **IP Filtering** page is displayed.

Step 2 Click **Add Item** to configure the parameters in **IP Whitelist**.

The related parameters are as follows:

- **IP filtering mode**: If this parameter is set to **Blacklist**, the **IP** addresses in the blacklist have no access rights to the network. If this parameter is set to **Whitelist**, the **IP** addresses in the whitelist have access rights to the network.
- **Application name**: indicates an application rule template for **IP** filtering. You can select a customized template for quick configurations.

Step 3 Click **Submit**.

----End

Example

Table 7-4 provides the typical whitelist parameter settings for **IP** address filter.

Table 7-4 Typical whitelist parameter settings

Index	Application name	Source Address Range	Destination Address Range
1	Custom	192.168.71.5	192.168.71.10

Index	Application name	Source Address Range	Destination Address Range
2	Custom	122.22.22.71	191.162.1.3
3	Custom	191.162.1.3	122.22.22.71
4	Custom	192.168.71.1	184.1.5.10
5	Custom	184.1.5.10	192.168.71.1

NOTE

- 192.168.71.5 is the **IP** address of **PC** for EG860 local maintenance
- 192.168.71.1 is the **IP** address of the attached camera of EG860
- 192.168.71.10 is the **IP** address for logging into the EG860 WebUI
- 122.22.22.71 is the **IP** address allocated by the core network to the **WAN** port on theEG860
- 191.162.1.3 is the service **IP** address of the eOMC910
- 184.1.5.10 is the **IP** address of the Dispatcher

The above **IP** addresses are for reference only. Please configure them according to the actual networking plan.

7.4 NAT Settings

Network Address Translation (NAT) settings, or port mapping settings, is necessary if a PC server is enabled and used by a WLAN, to allow port redirection for access from the WLAN to the server.

Procedure

Step 1 Choose **NAT Settings** > **Port Mapping**. The **Port Mapping** page is displayed.

Step 2 Click **Add Item** to configure the parameters in **Port Mapping**.

The related parameters are as follows:

- **Type**: indicates the type of the preset port mapping template. It is a configuration wizard. When the value of **Type** is **Custom**, other parameters needed to be filled in manually. Set according to the plan. When setting as other types, the default configuration is applied.
- **Protocol**: indicates the Protocol used for port mapping.
- **Remote Host**: indicates that only the authorized **IP** addresses are allowed to access the **WLAN**.
- **Remote Port Range**: indicates the port number of remote host. It must be a single number or a range within the range from 1 to 65535.
- **Local Host**: indicates the **IP** address of the server within the **LAN**.
- **Local Port**: indicates the port number of local host. It must be a single number or a range within the range from 1 to 65535.When this parameter is null, by default, the **Local Port** and **Remote Port Range** are the same. For example, the value of **Remote Port Range** is **23**, the value of **Local Port** is also**23**.

Step 3 Click **Submit**.

----End

7.5 QoS Management

This section describes how to set QoS parameters on the **QoS Management** page.

Context

EG860 supports QoS on multiple concurrent services to guarantee CPU resources for high-priority services. EG860 supports traffic filtering based on the source/destination IP addresses, source/destination port IDs, DSCP, and protocol types, to perform QoS on specified services.

QoS configurations are valid only for egress queues. On a WAN, QoS configurations are valid for uplink data; on a LAN, QoS configurations are valid for downlink data.

Procedure

Step 1 Choose **QoS Management** > **QoS Global**. The **QoS Global** interface is displayed.

Step 2 Set parameters in **Global Settings**.

The related parameters are as follows:

- **Global**: enables or disables QoS globally.
- **WAN total Bandwidth**: specifies the total uplink bandwidth. If this parameter is set to **0**, the uplink bandwidth is not limited.
- **LAN total Bandwidth**: specifies the total downlink bandwidth. If this parameter is set to **0**, the downlink bandwidth is not limited.
- **Queue type**: supports only **HTB** currently.

Step 3 Set **Queue type**.

A maximum of eight service queues are supported.

The related parameters are as follows:

- **Queue name**: specifies the service type name. The value can be customized.
- **Interface type**: specifies the service interface type. On a WAN, QoS configurations are valid for uplink data; on a LAN, QoS configurations are valid for downlink data.
- **Priority**: The value range is **1-8**. **1** specifies the highest priority, and its default priority is **8**.
- **Bandwidth**: The total bandwidth of services with the same interface type must not exceed the global bandwidth of the corresponding interface type.
- **Enable**: After a rule is matched with a service, use this parameter to enable the rule.

Step 4 Click **Edit** to set parameters in **Filter rule**.

Each rule must match a service. A service can match a maximum of 32 rules.

The related parameters are as follows:

- **Queue index**: specifies the service that a rule matches.

- **Rule priority**: The value range is **1-32**. **Rule priority** must be unique for each rule.
- **Protocol number**: specifies the protocol used by a rule. Common protocol numbers include 1 (ICMP), 2 (IGMP), 6 (TCP), 17 (UDP), and 47 (GRE). If a rule is used to match a GRE tunnel, the protocol number is 47, and the matching port is invalid.
- **DSCP**: specifies that a rule is matched using the DSCP. The value range is **0-63**.
- **Source IP**: The input format is **start IP address/mask bits**, for example **192.168.32.0/24**.
- **Destination IP**: The input format is **start IP address/mask bits**, for example **192.168.32.0/24**.
- **Source port**: The value range is **0-65535**.
- **Destination port**: The value range is **0-65535**.

Step 5 Click **Submit**.

----End

7.6 VPN

This section describes how to configure VPN connections, and use the data service encryption function.

Procedure

Step 1 Choose **VPN** > **VPN**. The **VPN** interface is displayed.

Step 2 Click **New**, and set **VPN** connection parameters.

The related parameters are as follows:

- **VPN connection**: If this parameter is set to **Enable**, the encryption rule is enabled.
- **VPN name**: indicates the name of an encryption rule. The name must be unique.
- **Remote IP address**: indicates the **IP** address of the peer device on the **VPN**.
- **Key mode**: includes **Manual** and **Auto** modes.

  If the **Manual** mode is used, the following parameters must be set:

  - **Protocol**: includes **AH** and **ESP** protocols.
  - **Manual authentication algorithm**: includes **hmac_md5** and **hmac-sha1** algorithms.
  - **Manual authentication key**: If **Manual authentication algorithm** is **hmac_md5**, **Manual authentication key** must contain 16 characters; if **Manual authentication algorithm** is **hmac-sha1**, **Manual authentication key** must contain 20 characters.
  - **Manual encryption algorithm**: If **Protocol** is set to **ESP**, this parameter can be set to **3des-cbc** or **des-cbc**.
  - **Manual encryption key**: required if **Protocol** is set to **ESP**.

    If **Manual encryption algorithm** is **3des-cbc**, **Manual encryption key** must contain 24 characters. The 24 characters are divided into three groups, and must meet the following requirements: the three groups must be different from each other; the characters in each group must not be completely the same; each group must contain valid ASCII code; the characters must not be only digits or letters.

If **Manual encryption algorithm** is **des-cbc**, **Manual encryption key** must contain 8 characters.

- **IPsec mode**: includes **Transmission** and **Tunnel**.
- **Data source**: required if **IPsec mode** is **Tunnel**.
- **Subnet mask of data source**: required if **IPsec mode** is **Tunnel**.
- **Data destination**: required if **IPsec mode** is **Tunnel**.
- **Subnet mask of data destination**: required if **IPsec mode** is **Tunnel**.
- **Local port**: in **Transmission** mode, indicates the port used by the VPN; in **Tunnel** mode, indicates the data start port.
- **Remote port**: in **Transmission** mode, indicates the port used by the VPN; in **Tunnel** mode, indicates the data end port.
- **Manual SPI**: must be a hexadecimal character in the range of **0x100-0xffffffff**.

If the **Auto** mode is used, the following parameters must be set:

- **Protocol**: includes **AH** and **ESP** protocols.
- **IPsec mode**: includes **Transmission** and **Tunnel**.
- **Data source**: required if **IPsec mode** is **Tunnel**.
- **Subnet mask of data source**: required if **IPsec mode** is **Tunnel**.
- **Data destination**: required if **IPsec mode** is **Tunnel**.
- **Subnet mask of data destination**: required if **IPsec mode** is **Tunnel**.
- **Local port**: in **Transmission** mode, indicates the port used by the VPN; in **Tunnel** mode, indicates the data start port.
- **Remote port**: in **Transmission** mode, indicates the port used by the VPN; in **Tunnel** mode, indicates the data end port.
- **Mode**: includes **Aggressive** and **Main** modes.
- **Identification Type**: If **Mode** is **Aggressive**, this parameter can be set to **IP Type** or **Name Type**.
- **Local Identifier**: required if **Identification Type** is **Name Type**.
- **NAT-T state**: indicates whether NAT traversal is enabled, and can be set to **Enable**, **Disable**, or **Force**.
- **Phase 1 encryption algorithm**: includes **3des**, **des**, **aes**, and **All**. **All** indicates that all the 3des, des, and aes algorithms are supported.
- **Phase 1 authentication algorithm**: includes **md5**, **sha1**, and **All**. **All** indicates that both md5 and sha1 algorithms are supported.
- **Phase 1 DH group**: indicates the length of the phase 1 DH group, and can be set to **768bit**, **1024bit**, **1536bit**, **2048bit**, or **4096bit**.
- **Phase 1 life cycle**: value range: **60-86400**; default value: **3600**; unit: second
- **Phase 2 encryption algorithm**: includes **3des** and **des**.
- **Phase 2 authentication algorithm**: includes **hmac_md5** and **hmac_sha1**.
- **Phase 2 DH group**: indicates the length of the phase 2 DH group, and can be set to **768bit**, **1024bit**, **1536bit**, **2048bit**, **4096bit**, or **null**.
- **Phase 2 life cycle**: value range: **60-86400**; default value: **3600**; unit: second

- **Authentication mode**: includes **Pre-shared key** and **Certificate** modes. If **Authentication mode** is **Certificate**, the common certificate, private certificate, and peer common certificate must be uploaded.
- **Pre-shared key**: required if **Authentication mode** is **Pre-shared key**, and contains 1 to 32 characters.

Step 3 Click **Submit**.

----End

7.7 System

The Web NMS offer the System menu to view and configure parameters such as Device Information, Reset, Backup & Recovery, and Upgrade.

7.7.1 Device Information

This section presents basic information that distinguishes a router.

Device information

In **Device information**, view the following information:

- **Name**: displays the name of the device.
- **SN**: displays the serial number of the device.
- **Hardware version**: displays the hardware version number of the device.
- **Software version**: displays the software version number of the device.
- **Modem hardware Version**: displays the hardware version number of the modem.
- **Modem software Version**: displays the software version number of the modem.

7.7.2 Reset

Reset is used to restart a router and recover factory defaults.

Context

If the webpage is not automatically refreshed within 60s, enter the login address manually.

Procedure

Step 1 Choose **System** > **Reset**. The **Reset** page is displayed.

Step 2 **Optional:** To restart the router, click **Reboot**.

Step 3 **Optional:** To recover factory defaults, click **Restore**.
Recovering factory defaults will delete all the configuration parameters.

----End

7.7.3 Backup & Recovery

Backup & Recovery allows backup and recovery of user configuration files.

Context

A router will restart after configuration files are recovered. Do not switch off the power supply during the recovery.

Procedure

Step 1 Choose **System** > **Backup & Recovery**. The **Backup & Recovery** page is displayed.

Step 2 **Optional:** To download configuration files, click **Backup**.

Step 3 **Optional:** When the router is faulty, recover the configuration files as follows:

1. Click **Browse** to upload the configuration files.
2. Click **Recover** to recover the configuration files.

----End

7.7.4 Upgrade

Upgrade allows a local upgrade of a router.

Context

- EG860 can be upgraded on the local web or remote eOMC910. This manual describes how to upgrade EG860 on the local web. For details about how to upgrade EG860 on the remote eOMC910, see the *eOMC910 Terminal Management Client User Guide* in *eOMC910 Product Documentation*.

  NOTE

  Security control must be implemented because uncertainties exist in the environments where remote terminals are located. Users are advised to provide remote upgrade as required.

- Download the latest version of files before upgrading the router.
- The router will restart after a upgrade. Do not cut off the power supply during the upgrade.

Procedure

Step 1 Choose **System** > **Upgrade**. The **Upgrade** page is displayed.

Step 2 Click **Browse...** to upload files.

Step 3 Click **Upgrade** to upgrade the router.

----End

7.7.5 Password Change

This section describes how to change the password for logging in to the WebUI and the password for connecting with eOMC910 on the **Password Change** page.

Context

- The new password must meet password complexity requirements.
- The new password must not be one of the 3 passwords that are recently used.

- Keep your password secure.

Procedure

Step 1 Choose **System** > **Password Change**. The **Password Change** page is displayed.

Step 2 Change the password in **Password Change**.

NOTICE

The password of the **acs** user must be changed on both the eOMC910 and the Web management interface.

Step 3 Click **Submit**.

----End

7.7.6 Password Complexity

This section describes how to query and set the password complexity on the **Password Complexity** interface.

Context

You can query and set the password complexity. After the settings take effect, the new password must meet the complexity requirements when you change the password.

The complexity requirements are as follows:

- The password must contain 8 to 32 characters.
- The password must contain at least two character types and must not contain three or more than three consecutively same characters.

  The character types include:
  - Lowercase letters
  - Uppercase letters
  - Digits
  - Special characters `~!@#$%^&*()-_=+\|[{}];:'",<.>/?, and space
- The password must not contain the account name or its reversion.

  For example, if the user name is **TD4GCPE**, the password must not be **TD4GCPE** or **EPCG4DT**.

Procedure

Step 1 Choose **System** > **Password Complexity**. The **Password Complexity** interface is displayed.

Step 2 Set the password complexity rules in **Config Password Complexity**.

Step 3 Click **Submit**.

----End

7.7.7 Password security Settings

This section describes how to set password security policies on the **Password security Settings** interface.

Procedure

Step 1 Choose **System** > **Password security Settings**. The **Password security Settings** interface is displayed.

Step 2 Set password security policies on the **Password security Settings** interface.

The related parameters are as follows:

- **Login Fail count**: indicates the maximum login attempts to the WebUI. Value range: **1-10**.
- **Login Lock time**: indicates the account lockout duration if the number of login attempts exceeds the specified value. Value range: **60-3600s**.
- **Change password count**: indicates the maximum password change attempts. If the number of change attempts exceeds the specified value, the user must log in to the system again. Value range: **1-10**.

Step 3 Click **Submit**.

----End

7.7.8 Date & Time

Date and time information is lost each time a router is powered off. It is recommended to enable the synchronization with network time function.

Procedure

Step 1 Choose **System** > **Date & Time**. The **Date & Time** page is displayed.

Step 2 Click **Manually set with local time** or **Synchronize with network time** to set time and date as required.

For detailed information about the parameters, see the online help on the right of the Web management interface.

Step 3 Click **Submit**.

----End

7.7.9 Diagnosis

Ping and Traceroute helps you quickly detect network connection status and the system check allows one-click self-check. Main/Neighbor Cell displays current main/neighbor cell information in real time. Chip temperature shows the current temperature of device internal environment. Tcpdump provides packet capture at ports. Tmsi provides Tmsi information query. Up/Down Throughup displays current throughput in real time. Work Frequency displays the current working frequency. Packet Stat displays the number of packets received/transmitted at a port. WAN ICMP controls whether to discard the ICMP packets received at the WAN port.

Procedure

Step 1 Choose **System** > **Diagnosis**. The **Diagnosis** page is displayed.

Step 2 Configure **Method** as required.

- If **Method** is set to **Ping**, you can ping **Destination IP address or domain** to help diagnose network faults.

  The related parameters are as follows:

  - **Destination IP address or domain**: indicates the destination IP address or domain name.
  - **Packet size**: indicates the number of transmitted bytes and ranges from 1 bytes to 9,000 bytes.
  - **Timeout**: indicates the timeout period for each response and ranges from 1s to 10s.
  - **Do not Fragment**: Set this parameter to **Enable** or not as required.
- If **Method** is set to **Traceroute**, you can use the Traceroute function to test **Destination IP address or domain** to help diagnose network faults.

  The related parameters are as follows:

  - **Destination IP address or domain**: indicates the destination IP address or domain name.
  - **Maximum hops**: indicates the maximum number of hops tested by traceroute and ranges from 1 to 100.
  - **Timeout**: indicates the timeout period for each response and ranges from 2s to 10s.
- If **Method** is set to **System check**, check the equipment status and output the result.
- If **Method** is set to **Main/Neighbor Cell**, current main/neighbor cell information will be displayed in the result.
- If **Method** is set to **Chip temperature**, the ambient temperature inside the equipment will be displayed in the result.
- If **Method** is set to **Tcpdump**, the system automatically selects the size of the packets captured at the port based on the number of ports where packet capture is performed. The fewer the selected ports, the longer the period of packet capture.

  NOTE

  Packet capture lasts less than 10 minutes. After packet capturing is completed, click **Export** to save the packet capturing file.
- If **Method** is set to **Tmsi**, click **Query** to query the current TMSI parameters of the data card.
- If **Method** is set to **Up/Down Throughput**, current throughput information will be displayed in the result.
- If **Method** is set to **Work Frequency**, the locked working frequency is displayed. "0" indicates that no frequency is locked.
- If **Method** is set to **Packet Stats**, and **Packet Stats** is set to **Enable**, the number of received/transmitted packets is collected.
- If **Method** is set to **WAN ICMP**, and **WAN ICMP** is set to **Enable**, the WAN ICMP function is switched on.

----End

7.7.10 Log

User operations and equipment abnormalities are recorded in logs.

Procedure

Step 1 Choose **System** > **Log**. The **Log** page is displayed.

Step 2 Export logs.

1. Set **Log level**.

   The following options are provided to help troubleshoot:

   - Information: records information of the system, including login information, upgrade information, and reset information.
   - Warning: indicates problems that may affect operating of the system. If the problem is not handled in time, it may cause severe problems.
   - Error: indicates the errors that may result in faults on equipment.
2. **Optional:** Click **Clear** to clear the logs.
3. Click **Export** to export the logs.

Step 3 Set **Modem log setting** to **offline log** or **Online log**.

NOTE

Set **Modem log setting** to **Online log** when connecting Histudio.

Step 4 Export serial port logs.

Click **Collect**, and click **Export** after collecting serial port logs successfully. If you conduct any other operation before exporting logs, the **Export** button becomes unavailable, and you need to recollect the logs.

1. Click **Collect** to collect the serial port logs.
2. Click **Export** to export the serial port logs.

   NOTE

   Personal information is anonymized to protect user privacy.
3. Click **Clear** to clear the serial port logs.

----End

7.7.11 Device Switch

Set hardware device switches in **Device Switch**.

Procedure

Step 1 Choose **System** > **Device Switch**. The **Device Switch** page is displayed.

Step 2 Set **Heat status** to **Enable** or not as required.

NOTE

Only when **Heat status** is set to **Enable**, and the temperature is -10℃ or below, will the heating film activate to heat EG860. Otherwise, the heating film will not be activate to heat.

Step 3 Set **WAN Antenna**. Set **Antenna status** based on the actual product.

The EM350-D61 data card supports only **Outer Antenna**. The EM350-C71 data card supports **Outer Antenna**, **Inner Antenna**, and **Outer Antenna Prefer**.

Step 4 Set **WIFI antenna**. **MIMO** is used in 802.11n mode, so set **Antenna status** to **Double WIFI antenna**.

Step 5 **Optional:** Set **Wan auto reset**.

This parameter is valid only if **General Settings** > **Internet Settings** > **Connection mode** is set to auto.

Step 6 Click **Submit**.

----End

7.7.12 Bandinfo Number Configuration

This section describes how to check Localbandinfo and check and configure Airbandinfo on the **Bandinfo Number Configuration** page.

Procedure

Step 1 Choose **System** > **BandInfo**. The **Bandinfo Number Configuration** page is displayed.

Step 2 Configure **AirBandInfo**.

A minimum of one record and a maximum of eight records can be configured for AirBandInfo based on the following requirements:

1. Set each parameter to a value within the corresponding range.
2. Uniquely set **AirBand ID**. The ranges from Earfcn_Low to Earfcn_High of different cells cannot overlap.
3. The range from Freq_Low to Freq_High of AirBand must be a subset of that of Localband.
4. one AirBand corresponds to one LocalBand or multiple AirBands correspond to one LocalBand.

----End

7.7.13 Work Frequency

This section describes how to set the working frequency of a modem on the **Work Frequency** interface.

Context

After the working frequency is changed, the modem is restarted.

Procedure

Step 1 Choose **System** > **Work Frequency**. The **Frequency Settings** interface is displayed.

Step 2 Set **BandID**. The value range is **0-63**. **0** indicates that the frequency is not locked.

Step 3 Set **Frequency**. The value range is **0-65535**. **0** indicates that the frequency is not locked.

Step 4 Click **Submit**.

----End

7.7.14 SIM Configuration

This section describes how to modify virtual SIM card and PLMN configurations on the **SIM configuration** page.

Context

- After modifying **SIM** configurations and **PLMN** configurations, power off and restart Modem to validate the modification.
- You can change the SIM card number in **SIM configuration**. After **PLMN configurable parameter** is configured, the SIM card number is generated automatically.
- You can set one or multiple parameters at a time.

Procedure

Step 1 Choose **System** > **SIM configuration**. The **SIM configuration** page is displayed.

Step 2 **Optional:** Configure parameters in **SIM configuration** to change the SIM card number.

The related parameters are as follows:

- **MNC_Length** can be set to **2** or **3**. The default value is **3**.
- **SIM** is a 15-bit number in decimal.
- **Authen_Arith** can be set to **0** or **1**. **0** indicates the Millenge algorithm and **1** indicates the Test algorithm. Only **0** (Millenge) is supported at present.
- **Op_Value** is a 32-bit number in hexadecimal (128bit). The default value is 0.
- **K_Value** is a 32-bit number in hexadecimal (128bit).

Step 3 **Optional:** Configure **PLMN configurable parameter** to generate the SIM card number. Set **PLMN** as required.

Step 4 Click **commit**.

----End

7.7.15 Alarm Configuration

This section describes how to configure alarm information.

Context

The basic information of EG860 alarms is as follows:

Alarm Name	Alarm ID	Alarm Type	Alarm Severity
the Alarm Configuration of Lan state	50001	Communication alarm	Critical

Alarm Name	Alarm ID	Alarm Type	Alarm Severity
the Alarm Configuration of High Temperature	50002	Environment alarm	Major
the Alarm Configuration of RadioSignal Weak	50003	Quality of Service (QoS) alarm	Major

Procedure

Step 1 Choose **System** > **Alarm Configuration**. The **Alarm Configuration** page is displayed.

Step 2 Configure **the Alarm Configuration of Lan state**, **the Alarm Configuration of High Temperature**, and **the Alarm Configuration of RadioSignal Weak**.

An example is provided as follows:

Alarm Name	AlarmRaiseSmoothPeriod	AlarmCeaseSmoothPeriod	AlarmReportTh	AlarmResumeTh
the Alarm Configuration of Lan state	10	10	None	None
the Alarm Configuration of High Temperature	6	6	75	65
the Alarm Configuration of RadioSignal Weak	6	6	-123	-118

- **AlarmRaiseSmoothPeriod** indicates the number of times for alarm generation and **AlarmCeaseSmoothPeriod** indicates the number of times for alarm clearing. Configure these parameters as required. The value range of **AlarmRaiseSmoothPeriod** and **AlarmCeaseSmoothPeriod** are **1~100**.
- Configure **AlarmReportTh** and **AlarmResumeTh** as required.
- **ResumeTh**: **0** indicates that no alarm is reported and **1** indicates that alarms are reported.
- **AlarmMaskFlag**: **0** indicates that alarms are not masked and **1** indicates that alarms are masked.
- In **the Alarm Configuration of High Temperature**, the value range of **AlarmReportTh** and **AlarmResumeTh** are **20 ℃~80 ℃**, set **AlarmReportTh** and **AlarmResumeTh** with a difference of more than 10 ℃.

- In **the Alarm Configuration of RadioSignal Weak**, the value range of **AlarmReportTh** and **AlarmResumeTh** are **-150 dBm~-50 dBm**, set **AlarmReportTh** and **AlarmResumeTh** with a difference of more than 5 dB.

Step 3 Click **Submit**.

----End

7.8 Logout

The login user interface is displayed upon a logout of the Web NMS.

Procedure

Step 1 Click **Logout**.

Step 2 In the displayed **Are you sure you want to log out** dialog box, click **OK**.

----End

8 Alarm Reference

About This Chapter

This chapter describes possible alarms related to EG860, and how to handle them.

8.1 ALM-50001 Lan state
This alarm is reported when the LAN port of an EG860 is faulty and the link between the EG860 and the device connected to it is unavailable.

8.2 ALM-50002 High Temperature
This alarm is reported when the temperature of an EG860 exceeds a preset threshold.

8.3 ALM 50003-RadioSignal Weak
This alarm is reported when the signals received by an EG860 are weak.

8.1 ALM-50001 Lan state

This alarm is reported when the LAN port of an EG860 is faulty and the link between the EG860 and the device connected to it is unavailable.

Attribute

Alarm ID	Alarm Severity	Alarm Type
50001	Critical	Fault

Parameters

None

Impact on the System

Alarm Severity	Alarm Impact
Critical	The link between the EG860 and the device (such as a **PC** or a camera) connected to it is unavailable, and the device fails to connect to the network.

System Actions

None

Possible Causes

Cause Category	Possible Cause
Environment	The network cable connection between the EG860 and the device connected to it is faulty.
Equipment	A connection fault occurs on the device connected to the EG860.

Procedure

Check the network cable connection between the EG860 and the device connected to it.

Related Information

None

8.2 ALM-50002 High Temperature

This alarm is reported when the temperature of an EG860 exceeds a preset threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
50002	Major	Fault

Parameters

None

Impact on the System

Alarm Severity	Alarm Impact
Major	Hardware may be damaged, and the EG860 fails to work properly, and services may be interrupted.

System Actions

None

Possible Causes

Cause Category	Possible Cause
Environment	The ambient temperature is excessively high and heat dissipation of the EG860 is poor.
Configuration	The alarm threshold is set to an inappropriate value.

Procedure

- Check whether any heat sources or devices that affect ambient temperature exist.
- Query the alarm threshold.

Related Information

None

8.3 ALM 50003-RadioSignal Weak

This alarm is reported when the signals received by an EG860 are weak.

Attribute

Alarm ID	Alarm Severity	Alarm Type
50003	Major	Fault

Parameters

None

Impact on the System

Alarm Severity	Alarm Impact
Major	Air interface signals received by the EG860 are weak and services may be affected.

System Actions

None

Possible Causes

Cause Category	Possible Cause
Environment	The **RF** feeder connection of the EG860 is faulty.
Configuration	The signals of the cell in which the EG860 resides are weak.

Procedure

- Check whether the **RF** feeder connection of the EG860 is normal.
- Check the signal strength in the cell in which the EG860 resides. To perform this check, log in to the **WebUI** and choose **System** > **Diagnosis**.

Related Information

None

9 Glossary

This table provides the related glossary for reference.

Glossary	Full Name
AAC	Advanced Audio Coding
AP	Access Point
APN	Access Point Name
CE	Conformite Europeenne
DC	Direct Current
DHCP	Dynamic Host Configuration Protocol
DMO	Direct Mode Operation
EEC	European Economic Community
ESD	Electrostatic Discharge
FE	Fast Ethernet
FTP	File Transfer Protocol
FTPS	File Transfer Protocol over SSL
GPS	Global Positioning System
ID	Identifier
IE	Internet Explorer
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IP	Internet Protocol

Glossary	Full Name
IPv4	Internet Protocol version 4
L2TP	Layer Two Tunneling Protocol
LAN	Local Area Network
LTE	Long Term Evolution
MAC	Media Access Control
MIMO	Multiple Input Multiple Output
MP3	MPEG audio layer-3
MPLS	Multiprotocol Label Switching
MS	Mobile Station
MSTP	Multi-Service Transmission Platform
MTU	Max Transmission Unit
NMS	Network Management System
OTA	Over the Air
PC	Personal Computer
PCB	Printed Circuit Board
PCC	Policy and Charging Control
PIN	Personal Identification Number
PLMN	Public Land Mobile Network
PGND	Protection Ground
POE	Power Over Ethernet
PTT	Push To Talk
PVC	Polyvinyl Chloride
QoS	Quality of Service
RF	Radio Frequency
RoHS	Restriction of the Use of Certain Hazardous Substances
RSRP	Reference Signal Received Power
SAR	Specific Absorption Rate
SDH	Synchronous Digital Hierarchy
SDP	Session Description Protocol

Glossary	Full Name
SELV	Safety Extra-low Voltage
SFTP	Secure File Transfer Protocol
SIM	Subscriber Identity Module
SMA	Sub-Miniature-A Connector
SSID	Service Set Identifier
TCP	Transmission Control Protocol
TFT	Thin Film Transistor
TMO	Trunking Mode Operation
TMSI	Temporary Mobile Subscriber Identity
TNV	Telecommunication Network Voltage
USB	Universal Serial Bus
VPN	Virtual Private Network
WAN	Wide Area Network
WebUI	Web User Interface
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WMA	Windows Media Audio
WPS	Wi-Fi Protected Setup