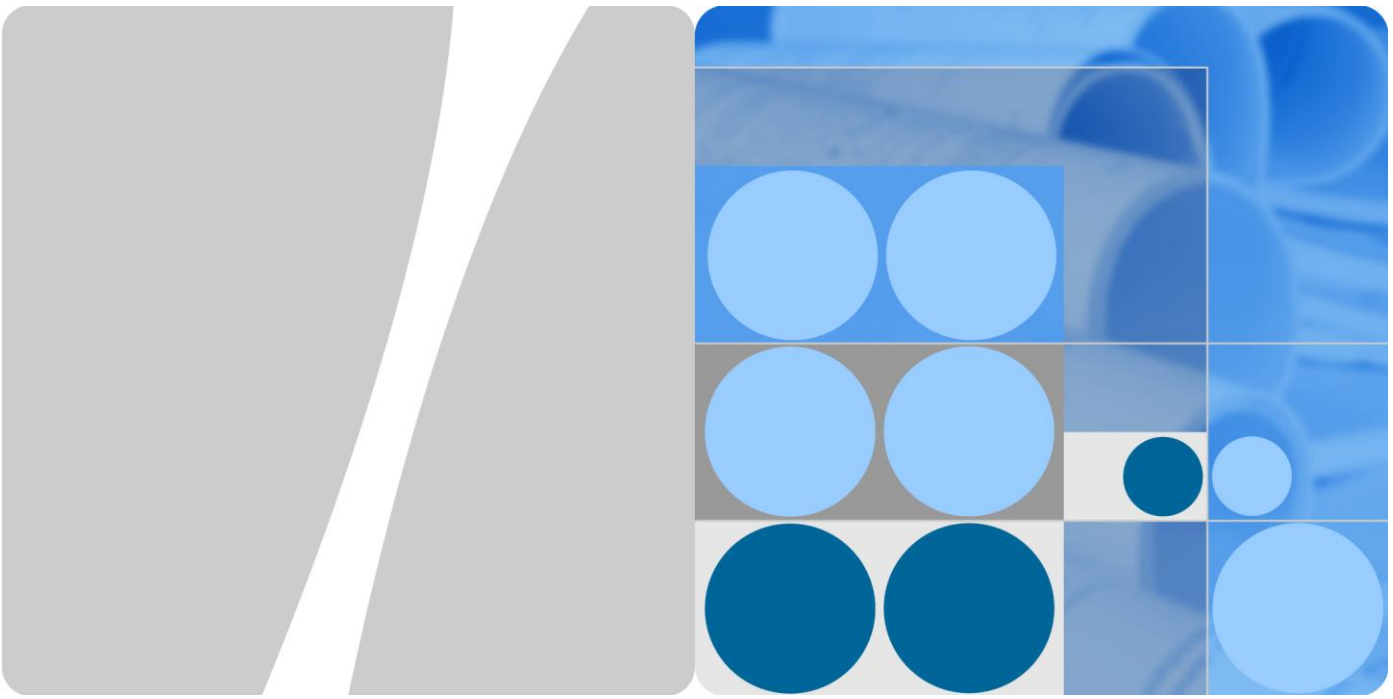


eA380 Series LTE CPE
V100R001C00
User Guide

Issue 01

Date 2017-08-31

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

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

Overview

This document describes the hardware, functions, installation, configuration, operation and maintenance (OM) of the eA380 series customer premises equipment (CPE).

Product Version

Product Name	Product Version
eA380-123	V100R001
eA380-135	V100R001

Intended Audience

This document is intended for:

- System engineers
- Product engineers
- Technical support engineers

.

Contents

1 Overview

About This Chapter

This chapter describes the functions, applications, product security and specifications of the product.

1.1 Product Introduction

The Huawei eA380 Series CPEs are the Long Term Evolution (LTE) customer premises equipments (CPEs). As a wireless gateway, the eA380 can be deployed outdoors to provide services such as data collection and video surveillance.

The eA380 Series CPEs (eA380-135, eA380-123,eA380 for short) supports LTE R11/12. The eA380 provide the following functions:

- Data services

  The eA380 series uses LTE broadband technologies to support high-speed broadband network access, data backhaul, and video surveillance.
- Small-scale local area network (LAN)

  The eA380 series can connect to external concentrators and Ethernet switches or routers to set up a LAN with multiple computers. When terminal devices on the LAN connect to the eA380 using network cables, the terminal devices can provide data services.
- Security services

  The eA380 series supports the firewall and PIN password, which protects your computers when you access the Internet.
- Firewall services

  The eA380 series supports the following firewall services:
  - Firewall enabling or disabling: enables or disables firewalls.
  - Media access control (MAC) address filtering: prevents certain MAC addresses from accessing the computers on a LAN.
  - IP address filtering: blocks certain IP addresses from accessing the local computers.
  - URL filtering: prevents computers from accessing certain URLs.
- Local and remote management and maintenance

  The eA380 support local configuration to manage devices , configure network parameters, and help ensure that the device functions properly and stably.

- Remote Management and Maintenance

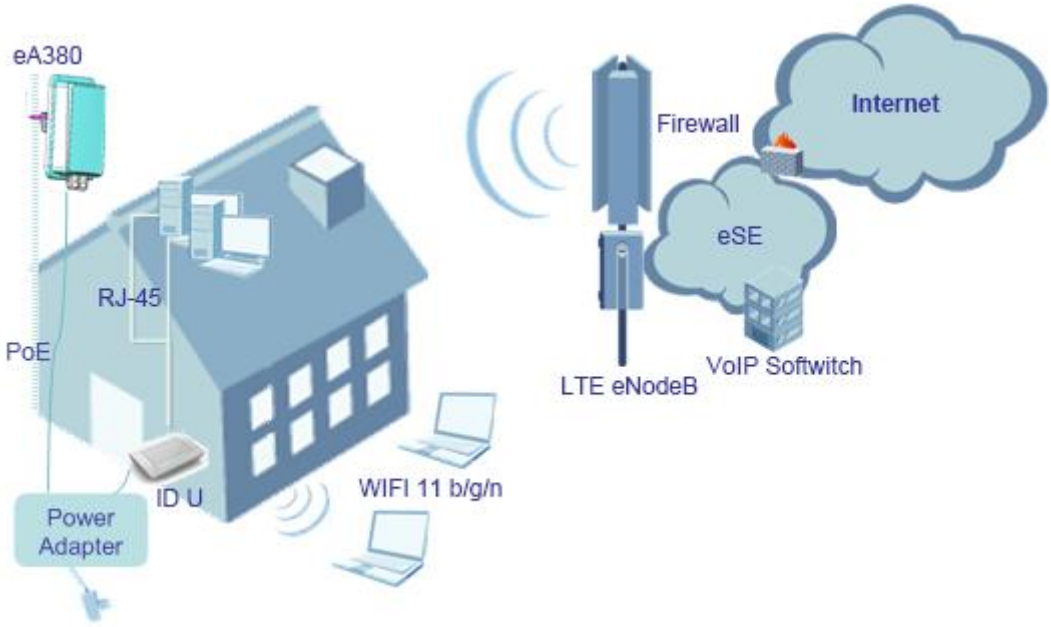
  The eA380 support remote configuration to manage devices , configure network parameters, and query the status by TR069.

1.2 Application Scenarios

The eA380 provides wireless broadband and wired Ethernet data services.

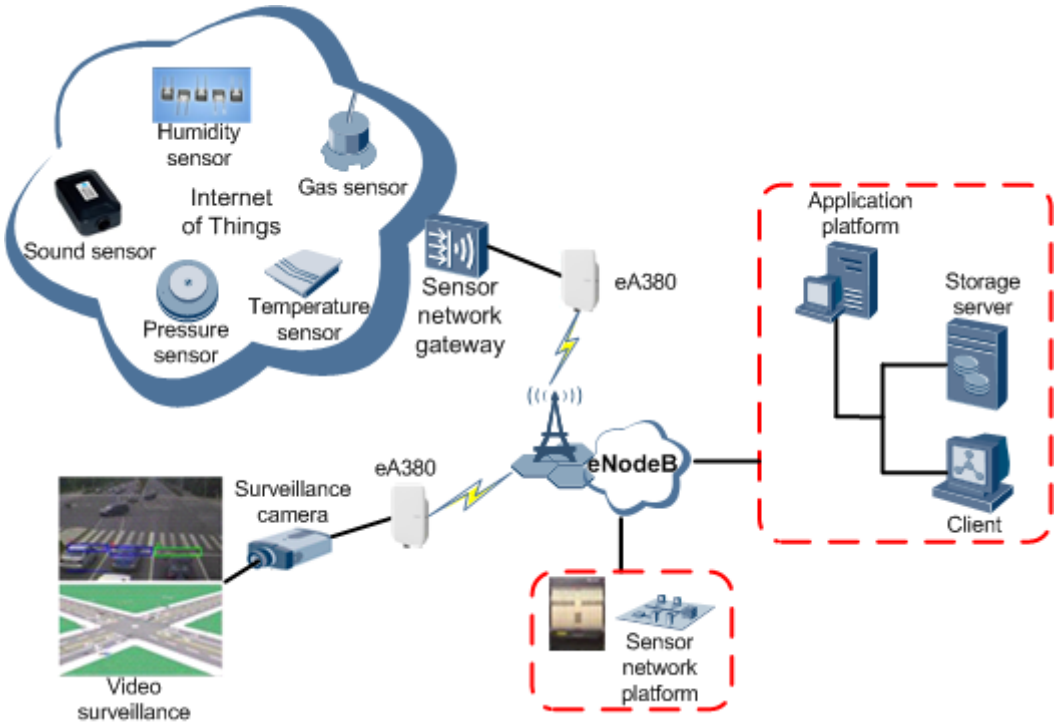
The eA380 is intended to be deployed in wISP(Wireless Internet Service Provider) network. They can also be deployed in industrial, public security and enterprise network if the performance is acceptable to the network operator.

Figure 1-1 The eA380 deployed in wISP network



The eA380 provides a variety of data services, such as LTE-TDD wireless routing and converting LTE wireless data into wired Ethernet data, and vice versa. Figure 1-2 shows an application scenario in which the eA380 is used in private industrial networks.

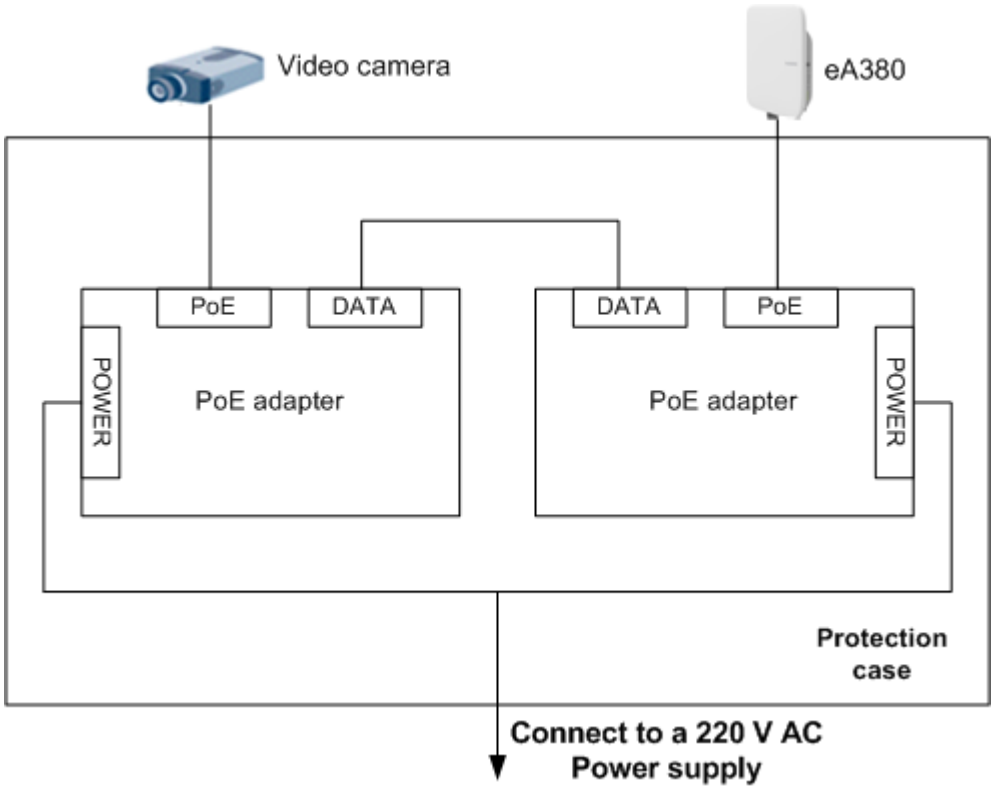
Figure 1-2 The eA380 deployed in industrial private networks



The following example describes how to use the eA380 for video monitoring.

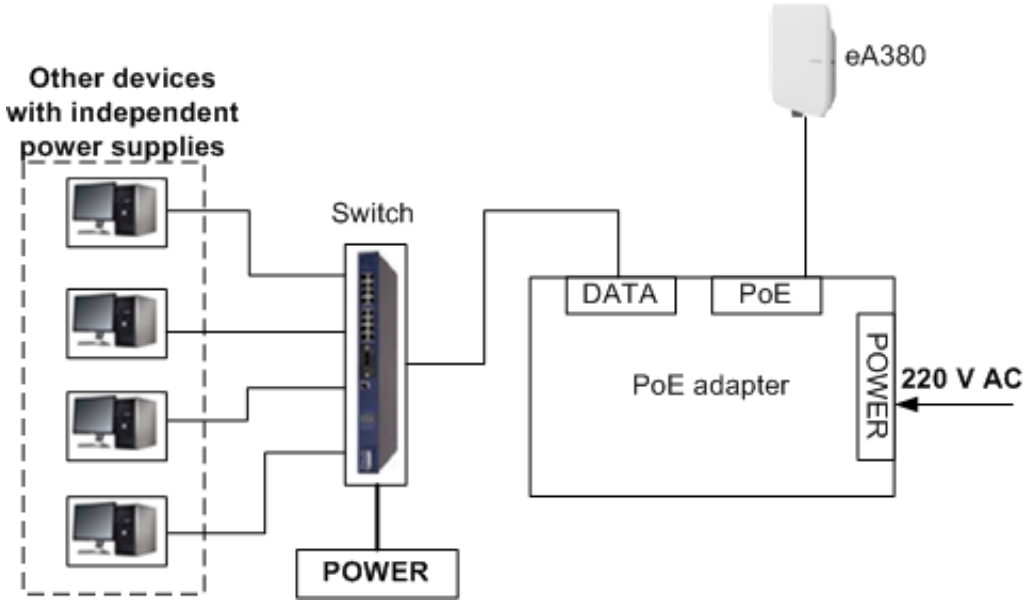
1. Use a power adapter to supply power for the eA380 or video camera, as shown in Figure 1-3.

Figure 1-3 The eA380 connected to a video camera.



2. Use a network cable to connect the eA380 to an external device. If the eA380 connects to a single device, connect the power adapter directly to the eA380. If the eA380 connects to multiple devices, connect the power adapter to a Hub or switch and then to the eA380, as shown in Figure 1-4.

Figure 1-4 The eA380 connected to multiple devices



1.3 Hardware Specifications

Table 1-1 describes the technical specifications of the eA380.

Table 1-1 Technical specifications of the eA380

Category		Description	
Technical standards		WAN: LTE 3GPP Release 11/12	
		LAN: IEEE 802.3/802.3u	
		WLAN: IEEE 802.11b/g/n	
Working frequency band	LTE	eA380-123: LTE TDD (2570 MHz to 2620 MHz) LTE TDD (2300 MHz to 2400 MHz) LTE TDD (2496 MHz to 2690 MHz) LTE FDD (2500 MHz to 2570 MHz(UL)/ 2620 MHz to 2690 MHz(DL)) eA380-135: LTE TDD (3400 MHz to 3600 MHz) LTE TDD (3600 MHz to 3800 MHz)	
	WLAN	2400 MHz to 2483.5 MHz	
External interface		• 1 Ethernet and voice interface (RJ45): 10/100/1000Base-TX Ethernet, PoE combined • 1 USB interface(for local maintenance only) • 1 SIM card slot	
LED indicator		• One POWER indicator • One LAN indicator • Three LTE signal strength indicators	
Maximum transmit power	LTE	• (23±2) dBm	
	WLAN	• (16±3) dBm	
EIRP	WiFi 2.4G	< 20 dBm	
Receiving sensitivity	LTE	eA380-123	B38/B40: • < -100 dBm/5 MHz • < -97 dBm/10 MHz • < -94 dBm/20 MHz
			B7: • < -98 dBm/5 MHz • < -95 dBm/10 MHz • < -92 dBm/20 MHz

Category		Description	
		eA380-135	B42/B43: • < -99 dBm/5 MHz • < -96 dBm/10 MHz • < -93 dBm/20 MHz
	WLAN	• 802.11b: -92 dBm@1 Mbps, -85 dBm@11 Mbps • 802.11g: -88 dBm@6 Mbps -73 dBm@54 Mbps • 802.11n: HT20: -87 dBm@MCS0 -71 dBm@MCS7 HT40: -84 dBm@MCS0 -68 dBm@MCS7	
Power consumption	when heater works (<25W) when heater off (<9W)		
Power supply	• PoE (should be powered by IEEE802.3at standard) • PoE adapter: AC 100V~240V,DC 54V/650mA		
Weight	<1.5kg (The power supply adapter is not included)		
Water and dust proof	IP65		
Temperature	• Working temperature: -40 ℃ to +55 ℃ • Storage temperature: -40 ℃ to +70 ℃		
Humidity	5% to 95%		
Installation	Mounted on poles or walls		

NOTE

Please deploy the device to make it power on in three months after received or store it under following circumstance:

- Temperature: -10℃ to 35℃
- Humidity: 30%RH to 85% RH

Thermometer and hygrometer should be used to monitor, adjust the temperature and humidity.

NOTICE

eA380-123 WLAN CH1-CH10 is unavailable when LTE works at band 40

1.4 Antenna Specifications

Table 1-2 eA380s LTE antenna specifications

Item	eA380-123	eA380–135
Band	2300 to 2400 MHz (Band 40) 2570 to 2620 MHz (Band 38) 2496 to 2690 MHz (Band 41) 2500 to 2570 MHz (Band 7 UL) 2620 to 2690 MHz (Band 7 DL)	3400 to 3600 MHz (Band 42) 3600 to 3800 MHz (Band 43)
Gain	12±1dBi	13±1dBi
Input impedance	50 ohm	
SWR	< 2	
Polarization	Dual cross polarization	
Radiation pattern	Directional antenna	

For FCC frequency range:

Frequency Range	LTE-FDD Band 7:2500-2570MHz(Tx), 2620-2690MHz(Rx) LTE-TDD Band 40: 2305-2320MHz&2345-2360MHz(Tx/Rx) LTE-TDD Band 41: 2500-2690MHz(Tx/Rx)

Table 1-3 WLAN antenna specifications

Item	Description
Frequency	2400 MHz ~ 2483 MHz
Input impedance	50 Ω
Standing wave ratio	< 3
efficiency	›50%
Gain	2dBi
Polarization	Linear polarization

1.5 Software specifications

Table 1-4 Software specifications

Item	Description
Gateway	Router: The default routing address is 0.0.0.0. The default routing table items can be generated accordingly.
	Supports Address Resolution Protocol (ARP)
	Supports domain name service (DNS)
	Supports Internet Control Message Protocol (ICMP)
	• Supports Network Address Translation (NAT) and Network Address Port Translation (NAPT). • Supports fragment message identification for normal NAT • Supports NAT traverse
	DHCP server • The default DHCP server address ranges from 192.168.1.2 to 192.168.1.254. The default gateway address is 192.168.1.1. • The default DHCP lease is 24 hours. • The DHCP server can be enabled or disabled. • The DHCP server's address pool can be configured. • The DHCP lease can be configured. • IP address status such as the hostname, Media Access Control (MAC) address, IP address, and remaining DHCP lease can be displayed. • Supports static IP address reservation • Supports DHCP relay
	Routing behind MS UE direct connect
Firewall	• Firewall switch • LAN MAC address filtering • IP address filtering • URL filtering • Security Parameter Index (SIP) ALG • Demilitarized Zone (DMZ) • Port forwarding • Service access control • NAT（Network Address Translation） • Static Route • Dynamic Route
LAN	• Auto-negotiation between 10 /100 /1000 Mbit/s • MDI/MDIX auto-sensing

Item	Description
	• Compatible with IEEE 802.3/802.3u • If you connect to multiple hosts via Hub or switch, the number of host devices sold under LTE CPE should not exceed 32
frequency lock	Support frequency, cell lock two ways
WLAN	SSID broadcast and hiding is supported.
	WLAN 2.4 GHz (802.11b/g/n) is supported.
	WPS is supported.
	Authentication: • Open System authentication • Shared Key authentication • 64/128-digit WEP encryption • 256-digit WPA-PSK/ WPA2-PSK encryption • AES ciphering algorithm TKIP and AES ciphering algorithm synchronously
	MAC address authentication: • Up to 10 MAC address items. • Support MAC address whitelist • Support MAC address blacklist
	Ratio adjustment: • Automatically • Manually
	STA management: • Supports limit of access users (up to 32 users) • Support STA status query
Upgrade	Supports TR-069 upgrade and local upgrade and online upgrade
SIM	Supports PIN management and SIM card authentication soft SIM
Dial-up connection	Supports automatic and manual connection
Importing and exporting configuration	Encrypt and back up the current configuration, and then restore from a backup configuration

1.6 Product Security

eA380 security includes network security and application security. Application security includes wireless security and OM security.

1.6.1 Network Security

eA380 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 eA380, the OM TCP applications can use SSL. HTTP over SSL is generally called HTTPS. HTTPS is used for connections between the NMS/WebUI and eA380. 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.

1.6.2 Application Security

eA380 application security includes wireless security and OM security.

Wireless Security

eA380 wireless security includes authentication, air-interface data encryption, and integrity protection.

OM Security

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

User Authentication and Access Control

User authentication and access control are implemented for users to be served by the eA380. 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.

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.

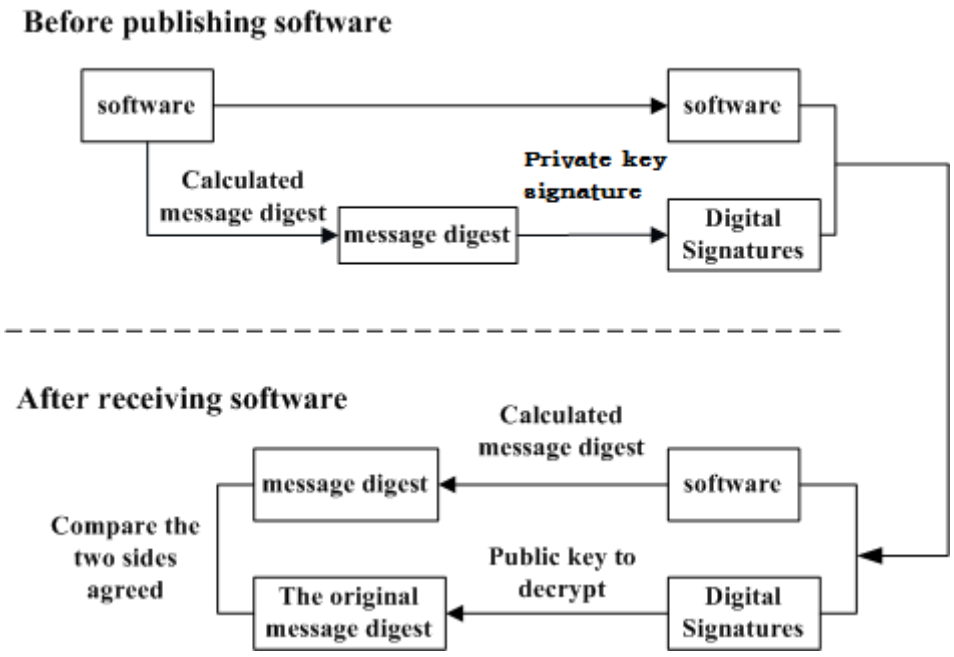
Software integrity protection helps detect viruses or malicious tampering in a timely manner, preventing insecure or virus-infected software from running on the device.

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 1-5 illustrates the principles of a software digital signature.

Figure 1-5 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.

1.7 Device Ports

1.7.1 Web Port

You can log in to the CPE WebUI over HTTPS to manage the LTE CPE, including configuring and querying settings, exporting running logs, querying device logs, importing and exporting the configuration, restarting and updating the LTE CPE, and restoring the LTE CPE to its default settings. For details, see the WebUI online help.

- The default WebUI login user name and password are **admin** and **admin**, respectively.

- You can change the login password on the WebUI.
- Internet Explorer 9.0 and a later version is recommended, because Internet Explorer 6.0 uses the SSL 3.0 protocol that contains vulnerabilities.

To improve security, change the default password at your first login and regularly change the password. It is recommended that users do not set an empty password or a simple password.

- A password must meet the following rules:

  A password consists of 8 to 15 characters.

  A password contains at least two types of characters of the following:

  - Lowercase letter
  - Uppercase letter
  - Digit
  - Special characters, including the space character and the following: ! # $ ( ) * - . / = @ [ ] ^ _ ` { } ~ |

  A password cannot be the user name or the reverse order of the user name.

  A password cannot contain more than two consecutive characters that are the same (for example, **111** is not allowed.)

- By default, the function to remotely log in to the CPE WebUI over HTTPS is disabled. The remote WebUI functions the same as the local WebUI.

NOTICE

- The maximum number of WebUI login attempts is three. After three login failures, the WebUI login page is locked and will be unlocked after one minutes. The lockingduration is incremented by one minute each time the WebUI login page is locked later.
- When the WebUI login password is forgotten, contact the device agent or maintenance center to restore factory defaults; refer to the AT command manual to restore factory defaults by yourself; or contact the device operator to reset the password through TR-069.
- The WebUI supports remote (LTE wireless link) and local (Ethernet interface or Wi-Fi link) login. Please configure ACL rights based on scenarios to control remote and local WebUI login. Opening unnecessary login interfaces may increase network attack risks or lead to unauthorized login. You can use the ACL service to enable or disable remote or local WebUI login. For details, see the section "Service Control List" in the online help of the device WebUI.
- If you do not perform any operation within 5 minutes after logging in to the WebUI, the system automatically logs you out.
- You are advised to change the password timely after first login and regularly change the password to improve network security.
- Personnel in the central office may remotely log in to the LTE CPE WebUI for CPE management and upgrade using HTTPS.
- CPEs support HTTPS and are compatible with HTTP. HTTP is not a relatively secure protocol.

1.7.2 USB Port

In normal cases, the USB port works in slave mode. In slave mode, the USB port will be mapped to a computer UI after the Huawei-provided chip driver is installed on the computer. This UI is locked by default. You can run other AT commands and write data to the SoftSim card only after running the unlock command. After the serial port mapped by the USB is connected successfully, run the unlock command.

The commands for unlocking the computer UI port and changing the unlock password are as follows:

- **at^PCPORT="*pwd*",1**: Enable the computer UI.

  pwd indicates the unlock password.
- **at^PCPORT="*pwd*",0**: Disable the computer UI.

  pwd indicates the unlock password.
- **at^PORTPWD="*oldPwd*","*newPwd*", "*newPwdConf*"**: Change the unlock password of the computer UI.

  Here, *oldPwd* indicates the current password, and *newPwd* the new password, and *newPwdConf* the confirm password. *newPwd* must be the same as *newPwdConf*; otherwise, the password cannot be changed.

  - The default unlock password is $Zls123Q.
  - To improve security, change the default USB unlock password at your first login and regularly change the password. It is recommended that users do not set an empty password or a simple password.
- A password must meet the following rules:

  A password consists of at least eight characters.

  A password contains at least three types of characters of the following:

  - Lowercase letter
  - Uppercase letter
  - Digit
  - Special characters, including the space character and the following: ! # $ ( ) * - . / = @ [ ] ^ _ ` { } ~ |

  The password cannot be the user name or the reverse order of the user name.

  A password cannot contain more than two consecutive characters that are the same (for example, **111** is not allowed.)

When the PC UI is unlocked, you can run commands to unlock other USB ports or AT commands to map the ports in the following table.

Port Mapping Name on the Computer	Port Usage	Port Number
HUAWEI Mobile Connect - PC UI Interface	Used to run AT commands.	18 (the actual computer port prevails)

- To learn more about AT commands, Please contact Huawei. The chipset driver supporting the USB interface is the host driver that supports Huawei Balong V7R1. If you need it, contact Huawei.

NOTICE

- The maximum number of unlock the USB port attempts is five. After five attempt failures, users cannot input any key. Users have to restart the device.
- The maximum number of attempts of locking the USB port is five. After five attempt failures, users cannot input any key. Users have to restart the device.
- The maximum number of password change attempts is five. After five attempt failures, the USB ports will be locked.
- After USB ports are unlocked, the USB ports do not support logout upon timeout and do not exit the unlock state even if the ports are removed. In this context, perform the operation in a secure environment and restart the device, or run commands to lock the USB ports.
- You are advised to change the password timely after first login and regularly change the password to improve network security.

1.7.3 TR-069 Port

Personnel in the central office can manage the LTE CPE remotely using TR-069.

- The management functions include device configuration, configuration query, running log exporting, and device updating.
- The account used for connections between the LTE CPE and central office TR-069 management equipment is managed by personnel in the central office. The default account name and passwords are **admin** and **Changeme123**, respectively.
- You can also change the password for connections between the LTE CPE and central office TR-069 management equipment. A password must meet the following rules:

  A password consists of 6 to 15 characters.

  A password contains at least two types of characters of the following:

  - Lowercase letter
  - Uppercase letter
  - Digit
  - Special characters, including the space character and the following: ! # $ ( ) * - . / = @ [ ] ^ _ ` { } ~ |

  The password cannot be the user name or the reverse order of the user name.

  A password cannot contain more than two consecutive characters that are the same (for example, **111** is not allowed.)

NOTE

- It is recommended that you change the password for connections between the LTE CPE and central office TR-069 management equipment at regular intervals.
- Ensure that the settings for the LTE CPE and central office TR-069 management equipment are the same. Otherwise, the LTE CPE cannot be managed by the central office TR-069 management equipment.

- MD5 digest authentication is used for connections between the LTE CPE and central office TR-069 management equipment, and the authentication complies with TR-069 Amendment 4.
- When TR-069 network management is enabled, each registration of the LTE CPE will generate about 70 KB of data traffic, each periodic reporting will generate about 20 KB of data traffic, and the data traffic generated by each update depends on the update package size. An update package is generally smaller than 100 MB, and updates are triggered by the central office management equipment.
- When TR-069 network management is enabled, the LTE CPE regularly connects to the central office management equipment, and the connection cycle complies with TR-069 Amendment 4.
- The LTE CPE supports the reporting of the following alarms:
  - High temperature alarm
  - Low temperature alarm
  - Weak signal alarm
  - Lower device disconnection alarm
  - Local login alarm
  - Lower devices have more than 32 alarms.
  - LAN uplink exception alarm

NOTICE

- Digest authentication prevents the account and password used for connections between the LTE CPE and central office TR-069 management equipment from being cracked. The number of attempts is five. After five attempt failures, wait five minutes and receive new connection authentication requests.
- The central office TR-069 management equipment will use the SN as the unique identifier for device management.
- Change the default password at your first login. To improve security, regularly change the password after negotiation with NMS engineers.

2 Hardware

About This Chapter

This chapter describes the hardware and cables of the eA380s.

2.1 eA380 Hardware

This section describes the appearance, ports, and indicators of the eA380.

2.1.1 Appearance

Figure 2-1 shows the appearance of the eA380.

Figure 2-1 eA380 appearance

2.1.2 Panel

The panel of the eA380 provides the Power over Ethernet (PoE) port, SIM card maintenance window, and indicator.

Figure 2-2 shows the panel of the eA380.

Figure 2-2 Panel of the eA380

Table 2-1 lists the ports of the eA380.

Table 2-1 Ports on the eA380

Name	Description
PoE	PoE port
SIM card maintenance window	Consists of the SIM card slot and USB port. • A SIM card is inserted into the SIM card slot. • The USB port is used for internal commissioning.

2.1.3 Indicator

The eA380 indicators are located in the SIM card maintenance window and are used to indicate the running status of the eA380.

The four indicators from top to bottom are POWER, WLINK, and Signal lights (3), as shown in Figure 2-3.

Figure 2-3 eA380 Indicators

Table 2-2 describes the indicators of the eA380.

Table 2-2 Indicators of the eA380

Identifier	Status	Color	Description
POWER	On	Red	The power supply is normal.
	Off	Gray	No power is supplied.
LAN	Steady on	Green	The eA380 is successfully registered to the network.
	Off	Gray	The product fails to register to the network.
	4Hz flashing	Green	The network port has data transmission
Signal lights (3) **NOTE** The identification		Green	Strong signal.
		Green	Medium signal.

Identifier	Status	Color	Description
of the lights on the panel is , the number of signal divisions is determined by combining RSRP and RSSI.		Green	Weak signal.
		Gray	no signal.

2.2 eA380 Cables

2.2.1 PoE Network Cable

The power over Ethernet (PoE) network cable is an unshielded network cable that is used to connect the PoE port of the eA380. The PoE network cable connects to an RJ45 connector at both ends. The appearance of the cable is shown in Figure 2-4.

Figure 2-4 Network Cable

Background Information

The PoE network cable transmits data signals to the eA380 and provides DC power for the equipment.

Technical Specifications

Table 2-3 lists the technical specifications of the PoE network cable.

Table 2-3 Technical specifications of the PoE network cable

Name	Description
Color	Black
Outer diameter	6.8 mm
Working temperature range	–40 ℃ to 75 ℃

Name	Description
The actual maximum operating voltage	54V
The actual maximum operating current	650mA

2.3 Mounting Parts

Describes the mounting parts that need to be used when installing the CPE, as described below：

Figure 2-5 Installing the adapter board

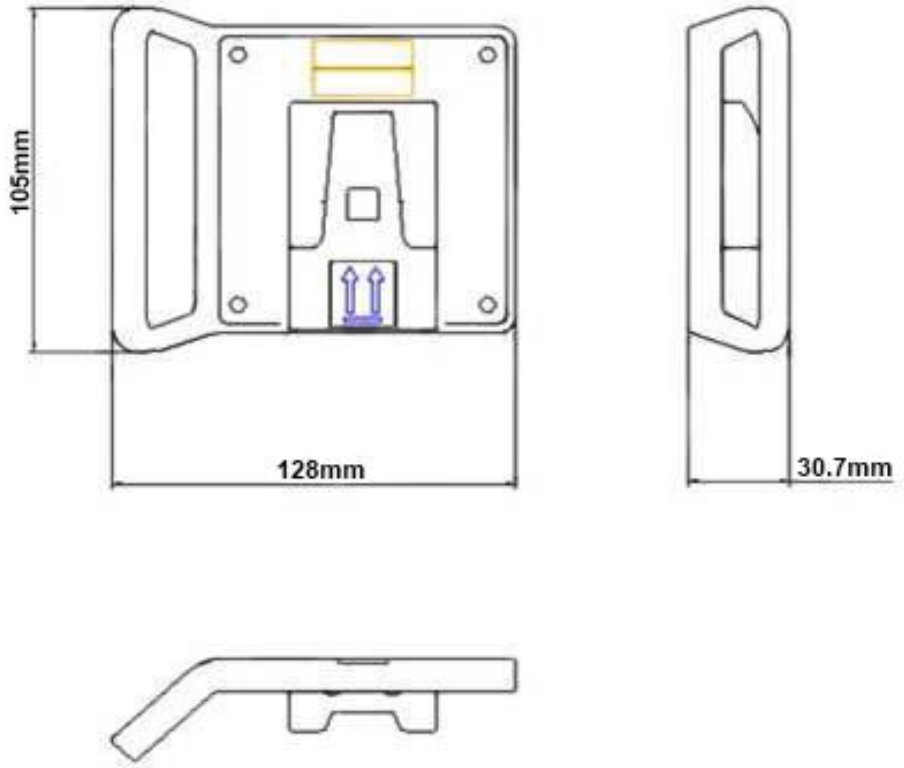


Figure 2-6 Pole mounting

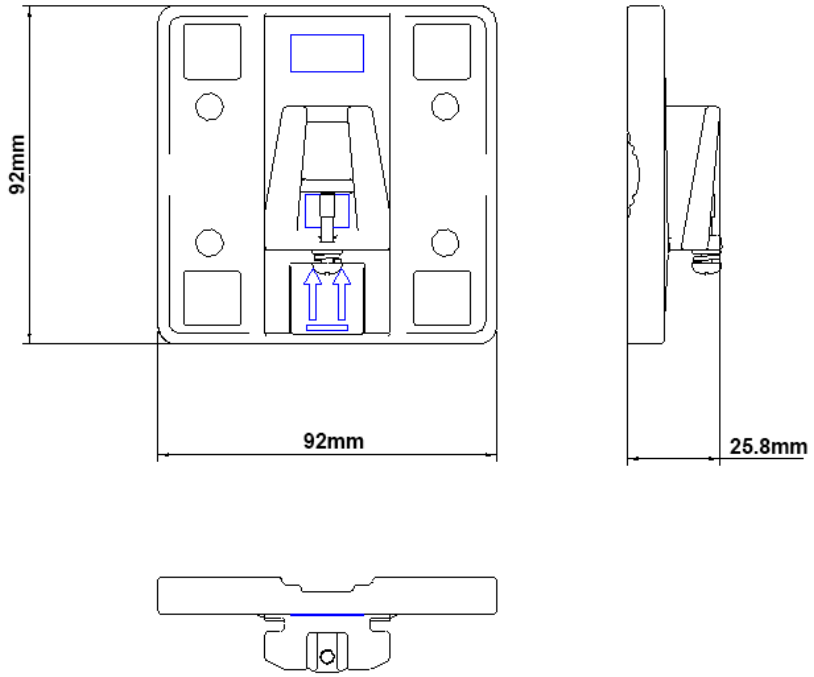
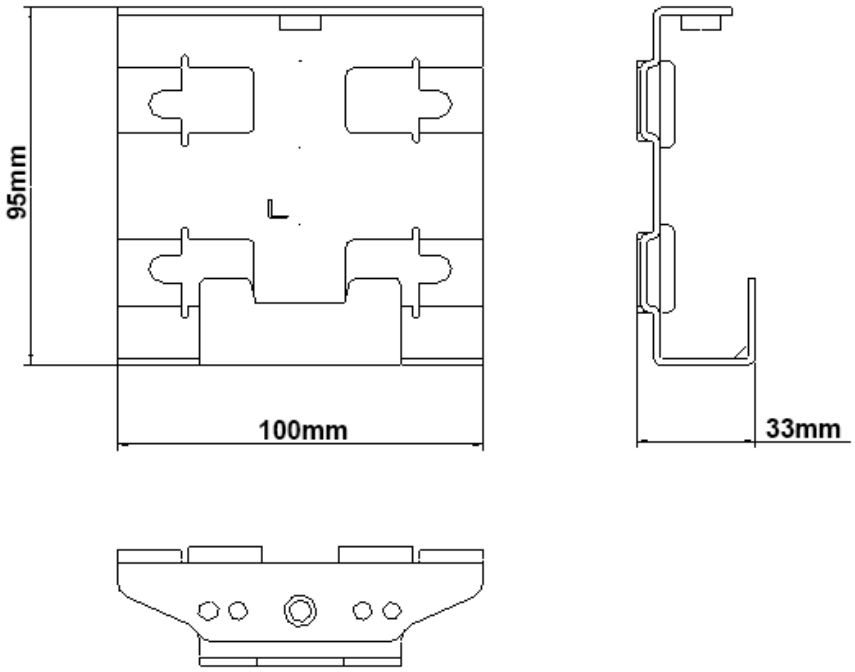


Figure 2-7 Wall mount ing (No Adjusted)



3 Installation

About This Chapter

This section describes how to install the eA380s.

3.1 Site Preparations

This section describes how to prepare a site before eA380 installation.

Select a site and space for installing an eA380 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 eA380, 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:

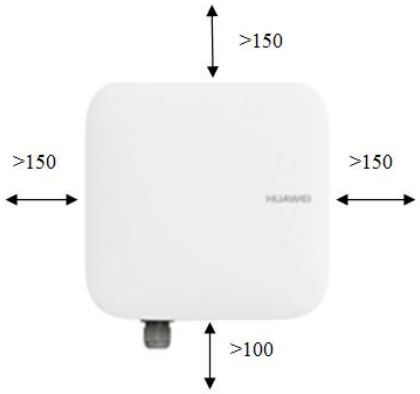
- Keep the site away from high temperature, dusty location, poisonous gases, explosive objects, and unstable voltages.
- Keep the site away from any electric substation, industrial boiler, and heating boiler.
- Keep the site away from any radar station, large-power radio transmitting station, and other interference sources. The field strength of interference sources cannot exceed that of unwanted radiation that an eA380 can shield.
- Keep an outdoor eA380 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 eA380 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 eA380 site higher than the second floor in a building. Alternatively, mount an eA380 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 3-1.

Figure 3-1 Space requirements for installing an eA380 (unit: mm)



Requirements for Operating Environment

For details about operating environment requirements, see1.3 Hardware Specifications.

3.2 Installation Preparation

Before you install the eA380, unpack and inspect the equipment delivered to the site and prepare the related tools.

Prerequisites

Perform the following operations to inspect the goods delivered to the site:

1. Unpack the equipment, count the total number of items based on the packing list attached to each packing case, and check whether each packing case is intact.
2. Check whether the models and quantities are consistent with those specified on the **Packing List**.
3. Record the serial number of the LTE CPE (From the CPE box on the two labels in the S / N bar code torn off, posted on the record book).

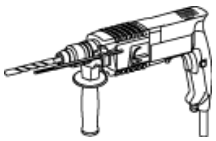
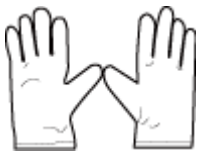
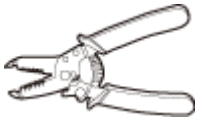
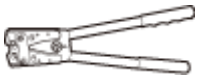
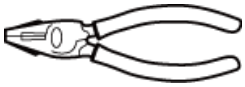
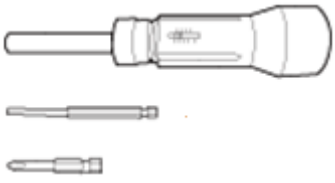
Precautions

- Power on a LTE CPE within 24 hours after unpacking it. If you power off a LTE CPE for maintenance, restore power to the LTE CPE within 24 hours. Keep the LTE CPE dry in humid environment.
- To avoid direct lightning, LTE CPEs 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.
- In outdoor environments, LTE CPEs may be vulnerable to the following attacks: interception, power removal, and physical damages. Please ensure the security of installation locations.
- Ensure that there are no obstacles facing the LTE CPE, and enable the LTE CPE to face the base station.

Installation Tools

Table 3-1 lists the tools used for installing the eA380.

Table 3-1 Installation tools

 Hammer drill	 ESD gloves	 Vacuum cleaner
 Heat gun	 Phillips screwdriver (M3–M6)	 Flat-head screwdriver (M3–M6)
 Claw hammer	 Utility knife	 Wire stripper
 Power cable crimping tool	 Cable cutter	 Adjustable wrench (open end ≥32 mm)
 Vise	 Hex key (M5,M6)	 Phillips torque screwdriver

 Measuring tape	 Multimeter	 Marker (diameter ≤ 10 mm)

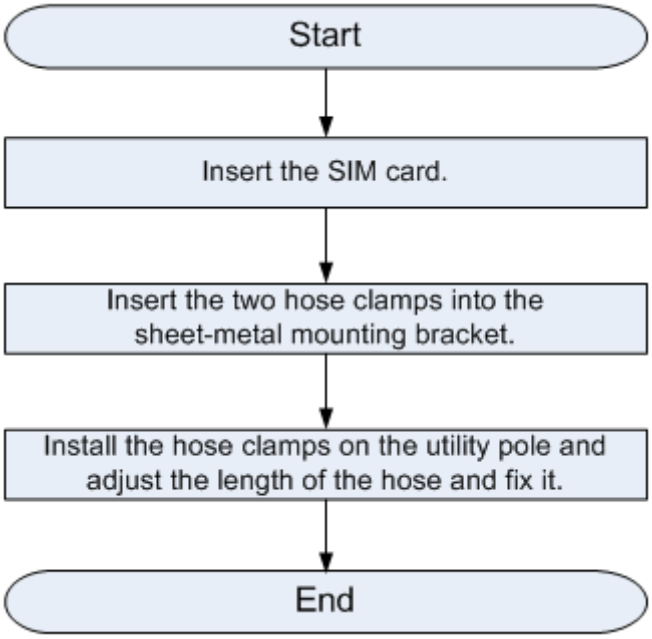
3.3 Installation Procedure

3.3.1 Mounting on a Utility Pole

Context

Figure 3-2 shows the flowchart for mounting the eA380 on a utility pole without an angle adjusting component.

Figure 3-2 Flowchart for mounting the eA380 on a utility pole without an angle adjusting component



Procedure

Step 1 Open the SIM card maintenance window of the eA380 and insert the SIM card. as shown in 0.

Figure 3-3

NOTICE

- When you install the SIM card maintenance window, insert the protrusion into the caging slot to ensure that the SIM card maintenance window is waterproof. Do not fasten the screws until the SIM card maintenance window has been correctly installed.
- When fastening the SIM card cover, press the rubber washer into the slot to avoid that it is exposed. Do not twist the rubber drop-proof chain.

Step 2 Insert the hose clamp to the wall-mounting frame, as shown in Figure 3-4.

Figure 3-4 Inserting the hose clamp to the wall-mounting frame

NOTE

Insert the end of the hose clamp that does not contain a screw into the square hole on top of the wall-mounting frame on the back of the unit. When half of the hose clamp passes through the square hole, slightly kink the protruding part and insert it into the other square hole on the front of the unit.

Step 3 Install the hose clamp with the wall-mounting frame on the utility pole, and use a M6 hex key to rotate the screw on the hose clamp to adjust the length of the hose clamp until it is correctly connected, as shown in Figure 3-5.

NOTICE

If the hose clamp is too long, cut off the extra part. Apply anti-rust oil to the cut in case it gets rusty.

Figure 3-5 Adjusting the length of the hose clamp

Step 4 The installation is complete. as shown in Figure 3-6.

Figure 3-6 The installation is complete

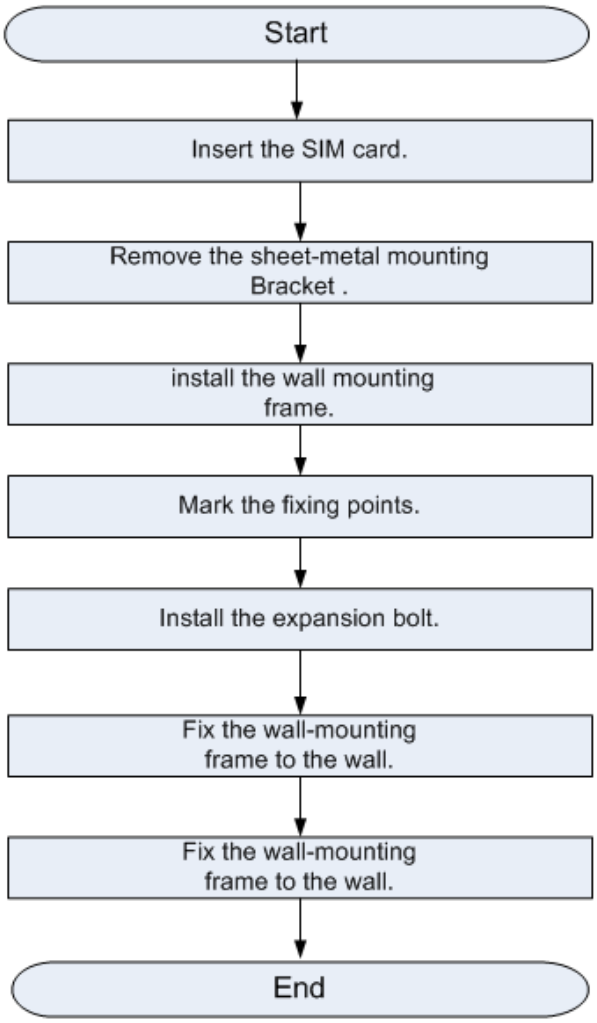
----End

3.3.2 Mounting on the Wall

Context

Figure 3-7 shows the flowchart for mounting the LTE CPE on the wall.

Figure 3-7 Wall-mounting flowchart



Procedure

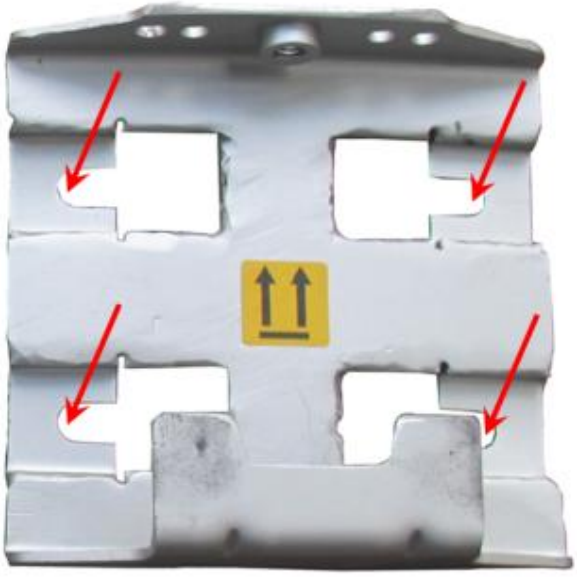
Step 1 Open the SIM card maintenance window of the eA380 and insert the SIM card.

Step 2 Remove the sheet-metal mounting Bracket and install the wall mounting frame ,as shown in Figure 3-8.

Figure 3-8 Remove the sheet-metal mounting Bracket and install the wall mounting frame

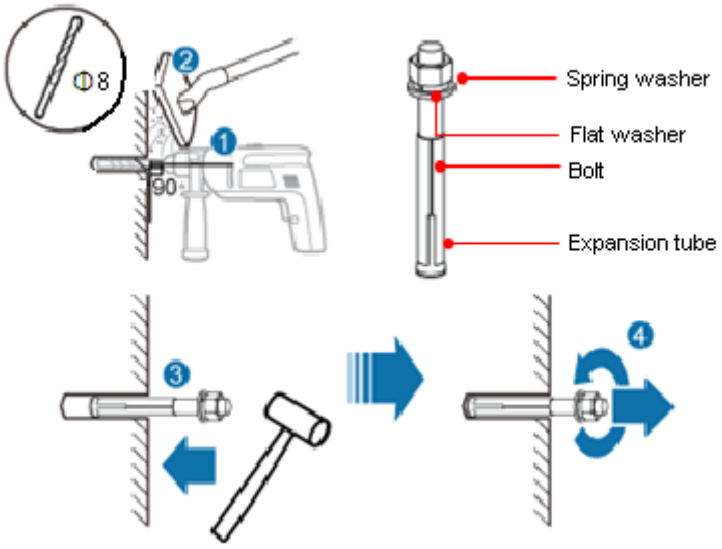
Step 3 Hold the wall-mounting frame tightly against the wall, use a level to adjust the horizontal position, and mark the fixing points with a marker, as shown in Figure 3-9.

Figure 3-9 Marking the fixing points



Step 4 Use a drill with 8 mm drill bit to drill holes in the fixing points. Then remove the dust from the holes and install the expansion bolts, as shown in Figure 3-10.

Figure 3-10 Installing the expansion bolt



Step 5 Align the four fixing points with the bolts on the wall and tighten the expansion bolt's screw nut to fix the wall-mounting frame, as shown in Figure 3-11.

Figure 3-11 Fixing the wall-mounting frame

Step 6 Fix eA380 to the wall-mount frame using the dovetail groove, as shown in Figure 3-12.

Figure 3-12 Fixing the LTE CPE

Step 7 Tighten the wall-mounting frame's screw.

----End

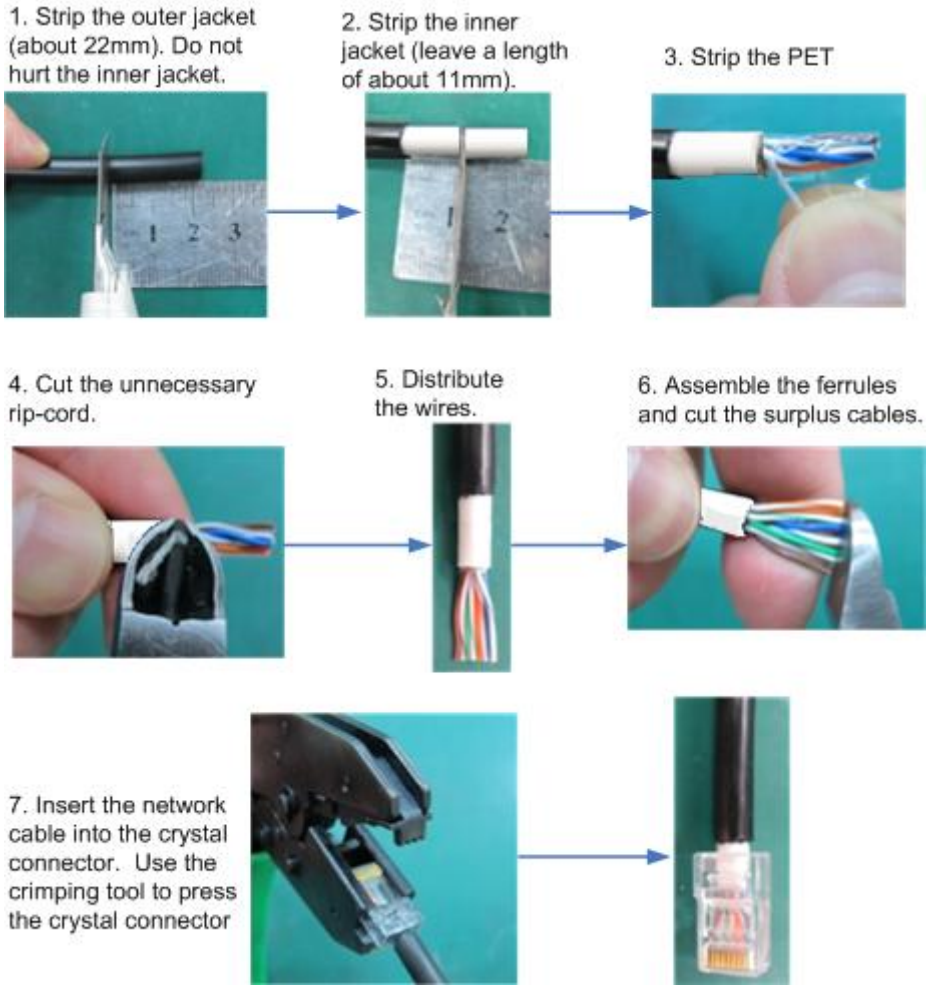
3.3.3 Cable Connection

This section describes the procedure for connecting the eA380 cables.

Procedure

Step 1 Make the crystal connector to PoE network cable, as shown in Figure 3-13.

Figure 3-13 Make crystal connector



NOTE

When making PoE network cables, follow the international standard EIA/TIA568A or EIA/TIA568A to arrange the cables. Make sure that the two ends of each network cable use the same standard.

Step 2 Connect the PoE network cable.

1. Disassemble the PG-head screw cap and air-proof block on the PoE port, and pass the network cable through them, as shown in Figure 3-14.

Figure 3-14 Passing the network cable through the PG-head screw cap and air-proof block

2. Connect the network cable to the network adapter, and manually rotate the screw cap to ensure that the lock block adheres to the network cable, as shown in Figure 3-15.

Figure 3-15 Installing the PG-head screw cap and air-proof block

Step 3 Connect the PoE adapter.

Connect the splitter with the adapter, as shown in Figure 3-16.

Figure 3-16 Connecting the PoE adapter

1. DATA port: connects to the computer network cable.	2. PoE port: connects to the PoE network cable.

----End

3.4 Installation Check

After you install the eA380, perform a hardware installation check and a power-on check.

Prerequisites

The eA380 hardware has been installed.

Procedure

Step 1 Check whether the eA380 hardware is correctly installed.

When performing the hardware check for the eA380, check the items listed in Table 3-2 in order.

Table 3-2 Hardware installation check of the eA380

No.	Check Item
1	The installation position must strictly comply with the design drawings, meet the installation space requirements, and reserve space for maintenance.
2	When the eA380 is mounted on a metal utility pole, the fixture must be firmly installed, and the LTE CPE must be attached.
3	When the eA380 is mounted on the wall, the installation hole on the fixture must be aligned with the one on the expansion bolt. In addition, the fixture must be tightly and firmly attached to the wall and must not wobble when you shake it.

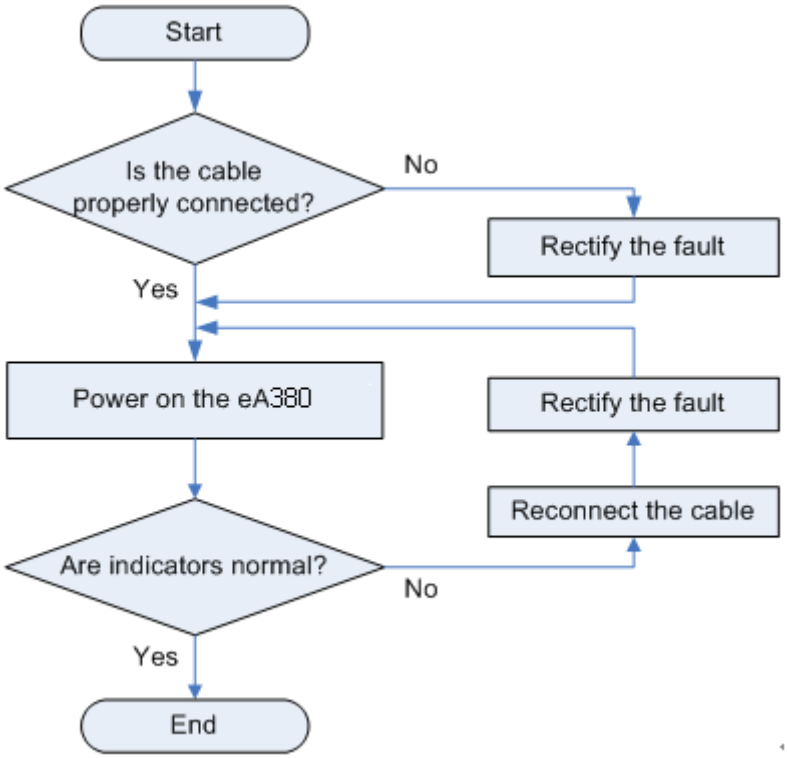
When checking the cable connections of the eA380, check the items listed in Table 3-3 in order.

Table 3-3 Cable connection check of the eA380

No.	Check Item
1	No cable is short-circuited or inversely connected.
2	The connector of the PoE network cable must be appropriately connected. The waterproof connector of PoE must be tightened.

Step 2 Perform the power-on check, as shown in Figure 3-17.

Figure 3-17 Power-on check of the eA380



The items listed in Table 3-4 must be checked during eA380 indicator check.

Table 3-4 Indicator check

No.	Check Item
1	When the eA380 powers on, the power indicator is on.
2	When the eA380 powers on, The signal strength indicator is on.

NOTE
If the signal strength indicator is off, no signals are available. If an indicator is steady green, the signal strength is weak. If this occurs, check whether the power supply is normal.

----End

4 Configuration Introduction

About This Chapter

This chapter describes the configuration Introduction of the eA380s.

4.1 Log in to the WebUI

Prerequisites

- The deployment on the network side is complete.
- The computer has been connected to the eA380.
- The installation of the eA380 is complete.
- The eA380 starts correctly based on default parameters during power-on.

Procedure

Step 1 Start the IE browser, enter **https://192.168.1.1** in the address bar, and press **Enter**. Connect the eA380 from the near end using the Web management page.

NOTE
Use Internet Explorer 9.0 or a later version.

Step 2 Log in to the web management page with **User name** set to default value **admin** and **Password** set to default value **admin**.

Step 3 Access **Password Modification** and modify **New Password**.

NOTE
Use the default values of other parameters. To change the default settings, please refer to the *LTE CPE Online help*.

----End

4.2 NAT /Routing Behind MS Settings

Prerequisites

Install Service engine and LTE CPE and commission them so that they are ready to be connected.

Configure the NAT Settings on Service engine.

Background Information

NAT and Routing Behind MS are mutually exclusive features. On the LTE CPE's web interface, select **NAT Enable** under **NAT Settings** and click **Apply** to enable **NAT Enable** or deselect **NAT Enable** under **NAT Settings**, and then click **Apply** to enable Routing Behind MS.

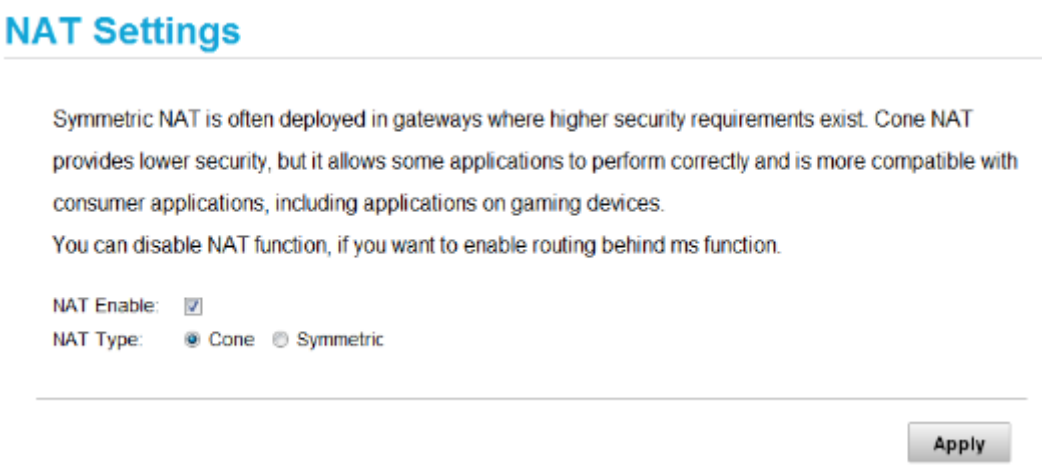
Procedure

Step 1 Log in to the WebUI.

For details, see section 4.1 "Log in to the WebUI."

Step 2 Choose **Settings** > **Security** > **NAT Settings**. Deselect **NAT Enable** under NAT Settings and click **Apply** to enable Routing Behind MS.

Figure 4-1 Enabling NAT



----End

4.3 Profile Management

Step 1 Log in to the WebUI.

For details, see section 4.1 "Log in to the WebUI."

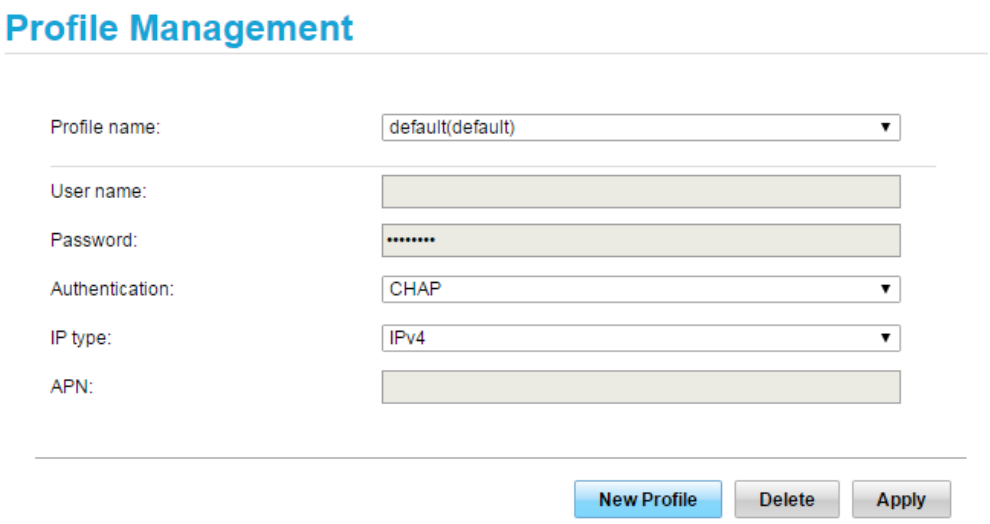
Step 2 Choose **Settings** > **Dial-up** > **Profile Management**.

Step 1 Click **New Profile**. On the displayed page, set **Profile name**, **User name**, **Password**, **Authentication,IP type** and **APN** as required.

- An APN indicates an Internet access point provided by an enterprise. Different enterprises have different APN settings.
- If the current APN does not match the enterprise, the data network service is unavailable.
- APNs in use cannot be deleted.
- The default APN cannot be deleted or edited.
- An APN cannot start with *rac*, *lac*, or *rnc*, or end with *.gprs*.

Step 2 Click **Apply**.

Figure 4-2 Profile management



4.4 TR-069 Setting

TR-069 is a standard for communication between CPEs and the auto-configuration server (ACS). If your service provider uses the TR-069 automatic service provision function, the ACS automatically provides the LTE CPE parameters. If you set the ACS parameters on both the LTE CPE and ACS, the network parameters on the LTE CPE are automatically set using the TR-069 function, and you do not need to set other parameters on the LTE CPE.

NOTICE

In some cases, remote upgrade will be required for service update by ACS. No services are available in upgrade process.

TR069 based LTE CPE upgrades, which are performed by network operators, cannot be canceled by LTE CPE users.

General info: ACS in carrier network will use SN(serial number) of the device as a unique identity for management and maintenances (including upgrade) operations. By TR069 protocol, the carrier can add, delete, and modify the device configurations for management and maintenances (including upgrade) only.

The TR069 function allows network operators to obtain operation logs, system logs, and configuration files, and cannot be canceled by LTE CPE users or inform users.

To configure the LTE CPE to implement the TR-069 function, perform the following steps:

Step 1 Choose **System** > **TR-069 Settings**.

Step 2 To enable the LTE CPE to send inform packets to the ACS at predefined intervals, set **Periodic inform** to **Enable**.

Step 3 If you set **Periodic inform** to **Enable**, set **Periodic inform interval**.

Step 4 In the **ACS URL** box, enter the ACS URL address.

If you want to disable ACS function, please set ACS URL to loopback address 127.0.0.1.

Step 5 Enter **ACS user name** and **ACS password** for LTE CPE authentication.

To use the LTE CPE to access the ACS, you must provide a user name and password for authentication. The user name and the password must be the same as those defined on the ACS.

Step 6 Enter **Connection request user name** and **Connection request password** for ACS authentication.

To use the ACS to access the LTE CPE, you must provide a user name and password for authentication. The user name and the password must be the same as those defined on the ACS.

Step 7 Click **Submit**.

TR069 operators can change LTE CPE passwords and upgrade LTE CPEs without LTE CPE users' knowledge through the eSight. To prohibit such upgrade behavior, stop the TR069 function on the device's WebUI.

----End

4.5 Security Settings

4.5.1 Firewall Settings

These sections describe how to enable the firewall function and filtering functions. IP address filtering, MAC address filtering, and domain name filtering are supported only after the firewall is enabled.

To enable the firewall, perform the following steps:

Step 1 Log in to the WebUI.

For details, see section 4.1 "Log in to the WebUI."

Step 2 Choose **Settings > Security > Firewall**. On the displayed page, select **Enable firewall**.

Step 3 Click **Apply**.

----End

4.5.2 LAN IP Address Filtering

Step 1 Log in to the WebUI.

For details, see section 4.1 "Log in to the WebUI."

Step 2 Choose **Settings** > **Security** > **Firewall**. On the displayed page, select **Enable IP address filter**.

Step 3 Choose **Settings** > **Security** > **LAN IP Filter**.

Step 4 Click **Add**.

In the **LAN IPAddress** text box, type the original IP address segment you want to filter.

In the **LAN Port** text box, type the original port address segment you want to filter.

In the **WLAN IPAddress** text box, type the destination IP address segment you want to filter.

In the **WAN Port** text box, type the destination port address segment you want to filter.

Set **Protocol**.

Step 5 Click **Apply**.

----End

4.5.3 MAC Address Filtering

Step 1 Log in to the WebUI.

For details, see section 4.1 "Log in to the WebUI."

Step 2 Choose **Settings** > **Security** > **Firewall**. On the displayed page, select **Enable MAC filter**.

Step 3 Choose **Settings** > **Security** > **MAC Filter**.

Set an MAC address filtering mode from the filtering mode drop-down list box.

Disable: disables MAC address filtering

Allow: allows a client to connect to your device if the client's MAC address is in the MAC address list

Deny: denies a client's access to your device if the client's MAC address is in the MAC address list

----End

4.5.4 Domain Name Filtering

Step 1 Log in to the WebUI.

For details, see section 4.1 "Log in to the WebUI."

Step 2 Choose **Settings** > **Security** > **Firewall**. On the displayed page, select **Enable domain name filter**.

Step 3 Choose **Settings** > **Security** > **Domain Name Filter**.

----End

.

5 Update Introduction

About This Chapter

This chapter describes three methods of updating the eA380 software. If a new version is detected, the system informs users to upgrade the software.

5.1 Local Update

Prerequisites:

- The LTE CPE is powered on and you have successfully logged in to the WebUI.
- A commercial software release for the LTE CPE is obtained.

Procedure:

Step 1 On the WebUI, choose **Update** > **Local Update**.

Step 2 On the displayed **Local Update** page, click **Browse…** and upload the file.

Step 3 Click Update to complete the LTE CPE upgrade.

----End

5.2 Online Update

Prerequisites:

The LTE CPE is powered on and you have successfully logged in to the WebUI.

Procedure:

Step 1 On the WebUI, choose **Update** > **Online Update**.

Step 2 On the **Configuration and Updates** page, set **Server IP**, **Server port**, and **Server virtual directory**. Then, click **Apply**.

Step 3 Click **Check for Updates** to view the information of the version after the upgrade.

Step 4 Click **Update Now** to complete the LTE CPE upgrade.

----End

5.3 TR069 eSight Update

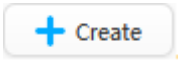
5.3.1 Firmware Version

Prerequisites:

- You have logged in to the client.
- You have obtained the latest firmware version file of the LTE CPEs.
- You have been assigned the operation rights.

Procedure:

Step 1 Choose **Resources** > **eLTE Device** > **Device Software Management** > **version management Management** from the main menu.

Step 2 Click 

that is displayed, upload the version file and set version parameters..

a. Click  following the **Firmware version file** and select the version file.

b. **Optional**: Click  following the **Signature file** and select the signature file.

c. Set **default firmware version**.

If the default firmware version of the product model exists on eSight and you have enabled **default firmware version**, a confirm dialog box is displayed. To make the current firmware version become the new default firmware version, click **Yes**.

d. Set **Remark**.

e. Click **OK**.

Step 3 Click **OK** in the dialog box that is displayed.

If the **Version Information Confirm** window is displayed during the upload, confirm and modify **Device Model**, and set **Hardware Version** and **Version** as required. When the parameters are verified, click **OK**.

----end

5.3.2 Upgrade Management

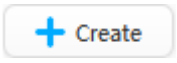
Prerequisites:

- You have logged in to the eSight client.

- The firmware version files for CPEs have been created on eSight.
- You have been assigned the operation rights.

Procedure:

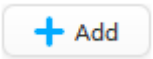
Step 1 Choose **Resources** > **eLTE Device** > **Device Software Management** > **CPE upgrade management** from the main menu.

Step 2 Click 

to create a task.

a. Set **Task Name** in **Task Set**.
b. Set **Scheduled Task**.
   - If you set **Scheduled Task** to **ON**, set **Scheduled Time** manually.
   - If you set **Scheduled Task** to **OFF**, eSight performs the upgrade task immediately.
c. Set **Same Version Upgrade**.
   - If you set to **OFF**, eSight will not perform the upgrade task when the target version is the same as the current version of the LTE CPE.
   - If you set to **ON**, eSight performs the upgrade task when the target version is the same as the current version of the LTE CPE.

Step 3 Select devices.

d. Click 

and select a managed object on the page that is displayed.
e. Click **OK**.

Device models and version are automatically displayed in the **Select File** area.

Step 4 Set **Target Version/File** in the list under the **Select File**.

Step 5 Click **OK**.

----end

6 Maintenance

About This Chapter

This chapter describes the maintenance preparation and fault diagnosis methods for the eA380.

6.1 Maintenance Preparation

Before performing site maintenance for the eA380, learn about the sit information, select required maintenance items, and prepare related tools.

Learning About the Site Information

Gather the following site information before going to the eA380 site to perform maintenance.

- Persisting faults and alarms
- Hardware configuration
- Natural environment

Selecting Maintenance Items

Select suitable maintenance items based on the eA380 site conditions.

Maintenance items must include the following aspects:

- Natural environment of the eA380 site
- Power of the eA380
- eA380

6.2 Fault Diagnosis

When the LTE CPE does not run properly, use the tools on the Web management page to perform initial diagnosis.

Prerequisites

- The network deployment is complete.
- The installation of the eA380 is complete.
- The eA380 starts appropriately based on default parameters after power-on.

Procedure

- When the LTE CPE fails to access the Internet, run the **Ping** function to quickly check the network connection status.

3. Start the IE browser, enter **https://192.168.1.1** in the address bar, and press **Enter**. Log in to the Web management page, and enter **User name** and **Password**.

NOTE
Use Internet Explorer 9 (IE9) or a later version.

4. Choose **Settings > TR-069 Management> Diagnosis** to open the **Diagnosis** page.
5. Set **Diagnosis Method** to **Ping**.
6. Enter the domain name in the **Destination IP address/domain name** box.
7. Click **Apply**.
8. Wait until the operation is performed. The command output is displayed in the **Result** box.

NOTE
Timeout indicates the timeout period of each reply, and ranges from 1 to 10 seconds.

- When the LTE CPE does not run properly, the **System Check** can be used to preliminarily identify the problem.
- Start the IE browser, enter **https://192.168.1.1** in the address bar, and press **Enter**. Then enter the correct password and click **Log In**.

NOTE
Use Internet Explorer 9 (IE9) or a later version.

9. Choose **Settings > TR-069 Management> Diagnosis** to open the **Diagnosis** page.
10. Set **Diagnosis Method** to **System Check**.
11. Click **Check**.
12. Wait until the system check is performed. Click **Export** to export the detailed information to the computer. If necessary, send the detailed information to maintenance personnel.

----End

7 FAQ

7.1 What Do I Do If the Web UI Fails to Be Opened?

Problem Description:

I cannot visit the Web management page of eA380 through browser.

Solution:

Step 1 Check whether the LTE CPE is powered on.

Step 2 Check whether the cables are not properly connected.

Step 3 Check whether the IP address is entered correctly.

Step 4 If there is no problem after the above checks, try to restart the LTE CPE from the near end.

Step 5 If the problem persists, please contact Huawei technical engineer.

----End

7.2 What Do I Do When Power Indicator Is Not Working?

Problem Description:

Power indicator is not working

Solution:

Step 1 Check whether the PoE cable is correctly connected to the power. The power supply is provided if the Power indicator presents red light.

Step 2 Check whether the PoE power adapter meets the product specifications.

NOTE

The LTE CPE is powered by the PoE adapter as the power adapter.

- The minimum input voltage: 100 V
- The maximum input voltage: 240 V
- Rate output voltage or current: 54 V or 650 mA
- Output voltage accuracy:5%
- Input or output cable connector: C8/RJ45-GE

----End

7.3 What Do I Do When the Data Service Is not Provided?

Problem Description:

Data service is not provided

Solution:

Step 1 Check whether the LTE CPE is powered. If the Power indicator presents red light, the power supply is provided.

Step 2 Check whether the SIM card is correctly installed.

Step 3 Confirm whether the LTE CPE is connected to the network. Check whether the LANI indicator is steady or blinking.

Step 4 If the problem persists, contact local service provider.

----End

8 Privacy and Security

8.1 Privacy Policy

To better understand how we protect your personal information, please see the privacy policy at http://consumer.huawei.com/privacy-policy.

The device will use the SN as the unique identifier for device management.

The device provides the log function to records device running and operation information, excluding any information related to individuals, including the IMEI, IMSI, call record (in voice scenarios), account, and password.

The device provides TR-069-based network management function. To disable this function, see the TR-069-related section in the online help.

8.2 Security Maintenance

Software components used by this device may report vulnerabilities. This device will use the software upgrade mode to fix these issues. You can obtain specific software packages from the device agent.

8.3 Performing Default Security Configuration

After a WebUI login, users can check the online help to perform default security configuration.

- Change the WebUI login password, keep it secure, and regularly change it subsequently.
- Verify that the TR-069 port password meets complexity requirements.
- Set the WiFi encryption method to WPA2-PSK/AES. Ensure WiFi password meets the complexity requirements. Change your password periodically.
- The firewall switch is turned on by default.
- Configure the service list control function based on product application scenarios. If HTTPS and ICMP access requests on the WAN side do not exist, disable WAN access.
- Set multicast upgrade disabled according to ***AT Commands for the eA380's USB Port.doc*** before deployment.

- Change the USB port password, keep it secure (before installation), and regularly change it subsequently (optional).

NOTE

The USB port provides maintenance and repair functions and allows you to set device parameters. Please keep the password secure to prevent device parameters from being modified or exposed.

9 Acronyms and Abbreviations

This section lists the acronyms and abbreviations related to the eA380.

Table 9-1 List of acronyms and abbreviations

Acronym/Abbreviation	Full Name
3GPP	3rd Generation Partnership Project
ARP	Address Resolution Protocol
CPE	Customer Premises Equipment
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
ICMP	Internet Control Message Protocol
IP	Internet Protocol
GRE	Generic Routing Encapsulation
LTE	Long Term Evolution
MAC	Media Access Control
MDI	Medium Dependent Interface
NAPT	Network Address Port Translation
NAT	Network Address Translation
RTU	Remote Terminal Unit
PoE	Power over Ethernet
SPI	Security Parameter Index
SIM	Subscriber Identity Module
TR069	Technical Report 069
URL	Uniform Resource Location

Acronym/Abbreviation	Full Name
WAN	Wide Area Network

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment and it also complies with Part 15 of the FCC RF Rules. This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 40 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provide with antenna installation instructions and consider removing the no-collocation statement.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Caution!

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

ISEDC RSS warning

This device com plies with ISEDC licence-exempt RSS standard (s). Operation is subject to the following two conditions: (1)this device m ay not cause interference, and (2) this device must accept any inte rference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'ISEDC applicables aux appareils radio exempts de licence.

L'exploitation est autorisée aux deux conditions suivantes:

(1) l'appareil ne doit pas produire de brouillage, et

(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

ISEDC Radiation Exposure Statement:

This equip ment com plies with ISEDC RF radiation exposure limits set forth for an uncontrolled environm ent. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Rapport d'exposition de la radiation d' ISEDC :

Cet équip ement est co nforme aux lim ites d'exposition d'ation de radi de l'ISEDC rf déterminées pour un environnem ent non cont rôlé. Cet ém etteur ne doit pas être Co-placé ou fonctionnant dans la conjonction avec aucune autre antenne ou émetteur.

This equipment should be installed and operated with minimum distance 40cm between the radiator& your body.

Cet équipement doit être installé et utiliséavec une distance minimale de 40cm entre leradiateur & votre corps.