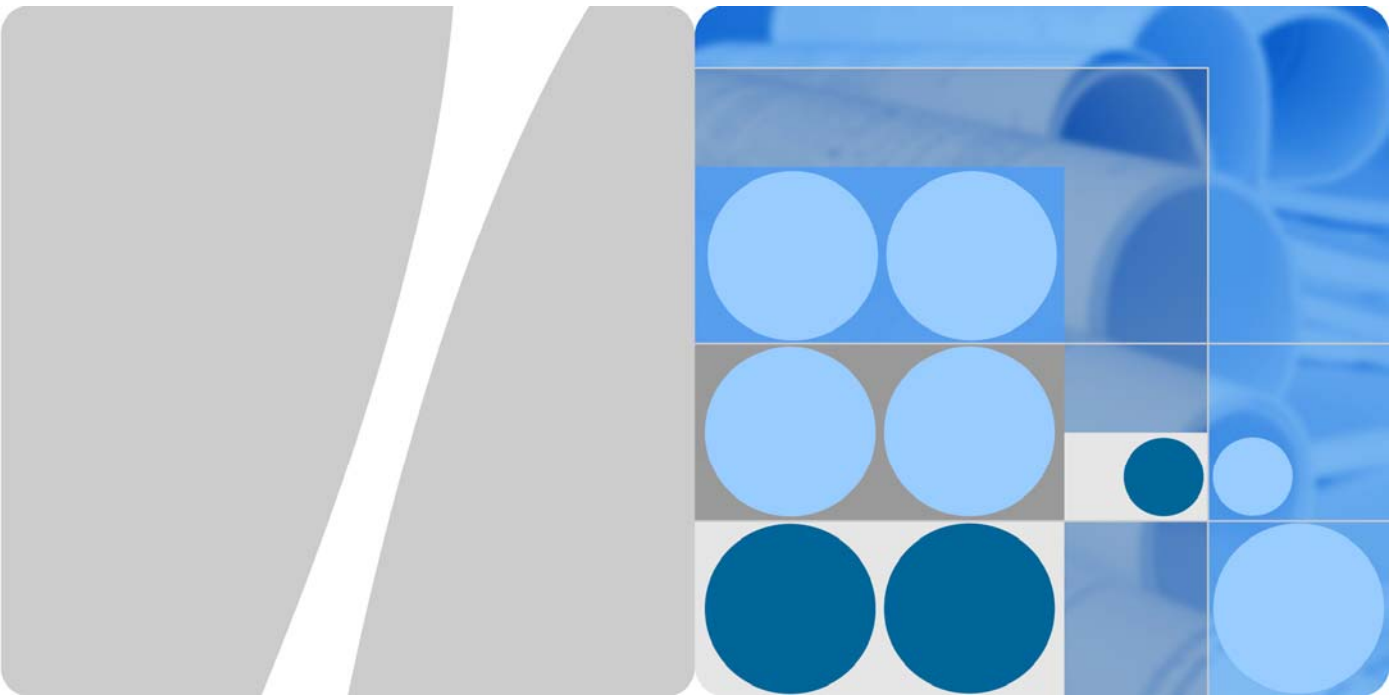


eA280 Series LTE CPE

User Guide

Issue 01

Date 2016-11-08

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, upgrade, operation and maintenance (OM) of the eA280 series customer premises equipment (LTE CPE).

Product Version

Product Name	Product Version
eA280-135	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

HUAWEI eA280 is a piece of customer premises equipment (CPE) that functions as the long term evolution (LTE) wireless gateway. It implements the conversion between LTE wireless data and wired Ethernet data and supports data backhaul. The eA280 series can be used independently and deployed outdoors.

The eA280 V100R001 CPEs support LTE Release 11/12. The eA280 provides the following functions:

- Data services

  The eA280 series use LTE broadband technologies to support high-speed broadband network access, data backhaul, and video surveillance.
- Voice services

  The eA280 provides two telephone ports to which users can connect telephones to implement basic voice functions and supplement voice functions.
- Security services

  The eA280 series support the firewall and PIN password, which protects your computers when you access the Internet.
- Firewall services

  The eA280 series support the following firewall services:
  - Firewall switch: enables or disables firewalls.
  - LAN Media access control (MAC) address filtering: prevents specified MAC addresses on a LAN from accessing the network.
  - LAN IP address filtering: prevents specified IP addresses on a LAN from accessing the network.
  - URL filtering: prevents computers from accessing certain URLs.
- Local and remote management and maintenance

The eA280 series can be locally configured in the local city to implement device management and network configuration, thereby ensuring stable operation of the device.

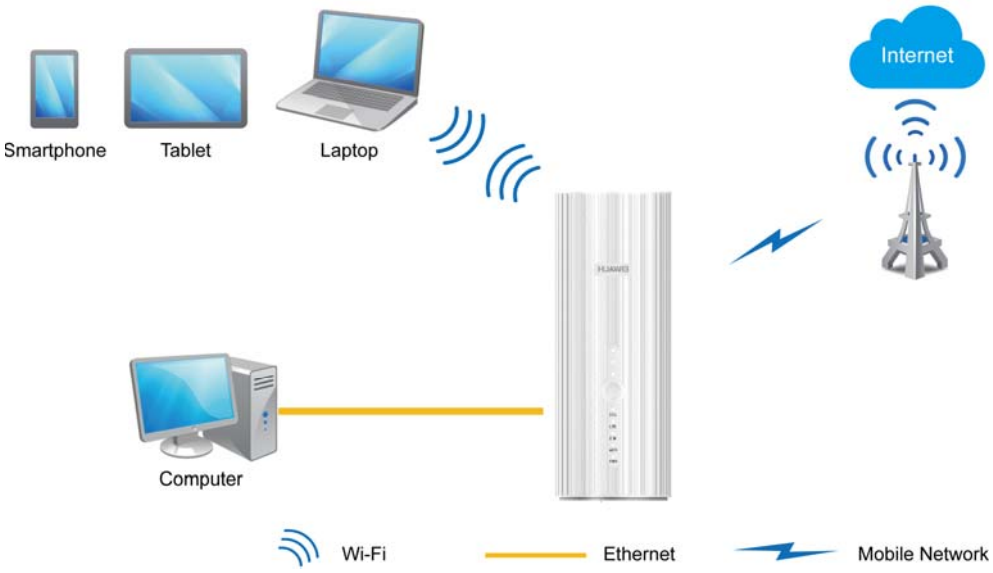
1.2 Application Scenarios

The eA280 series are mainly intended to provide users with wireless broadband data access services for wISP（Wireless Internet Service Provider） market.

The eA280 provides LTE-TDD and LTE-FDD band7 wireless routing and translating LTE wireless data into wired Ethernet data, and vice versa.

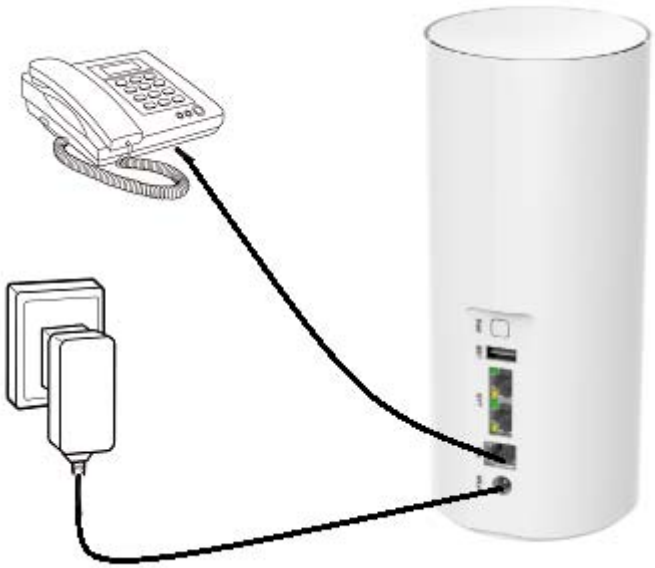
The eA280 can simultaneously set up wireless connections with 64 Wi-Fi devices (32 devices for 2.4 GHz and 32 for 5 GHz) and establish a local area network (LAN) by connecting to concentrators and switches.

Figure 1-1 eA280 connected to multiple devices



The eA280 provides one telephone interface. You can connect a telephone to achieve the basic voice capabilities.

Figure 1-2 eA280 connected to telephones (optional)



1.3 Hardware Specifications

Table 1-1 describes the technical specifications of the eA280.

Table 1-1 Technical specifications of the eA280

Item	Description
Technical standards	WAN: LTE 3GPP Release 11/12
	LAN: IEEE 802.3/802.3u
	IEEE 802.11b/g/n, 802.11a/n/ac
Working bands	eA280-135: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)) LTE TDD (3400 MHz to 3600 MHz) LTE TDD (3600 MHz to 3800 MHz)
	• 2.4 GHz (802.11b/g/n): 2.400 GHz to 2.4835 GHz • 5 GHz (802.11a/n/ac): 5.150 GHz to 5.850 GHz
External ports	One power port
	One telephone port (RJ11), one phone number
	Two LAN ports (RJ45)

Item	Description		
	One USB 2.0 slave port (for local maintenance only)		
	One micro SIM card port		
Buttons	One PWR button		
	One WPS button		
	One reset button		
LED indicators	One PWR indicator		
	One Wi-Fi indicator		
	One SIM indicator		
	One LTE indicator		
	One STA indicator		
	Three signal strength indicators		
Maximum transmit power	LTE	LTE: conform to power class 3 definition	
	WLAN	802.11b	(16±3) @11 Mbps
		802.11g	(16±3) @6 Mbps (16±3) @54 Mbps
		802.11n	(16±3) @2.4G MCS0 (16±3) @2.4G MCS7
		802.11a/n/ac high band	(16±3)@MCS0 (16±3) @MCS7 (16±3) @MCS9
		802.11a/n/ac low band	(16±3) @MCS0 (16±3) @MCS7 (16±3) @MCS9
Receiving sensitivity	LTE	LTE: confirm to 3GPP requirements	
	WLAN	802.11b	-92 dBm@1 Mbps -85 dBm@11 Mbps
		802.11g	-88 dBm@6 Mbps -73 dBm@54 Mbps
		802.11n HT20 (2.4 GHz)	-87 dBm@MCS0 -71 dBm@MCS7
		802.11n HT40 (2.4 GHz)	-84 dBm@MCS0 -68 dBm@MCS7
		802.11n HT20 (5 GHz)	-88 dBm@MCS0 -68 dBm@MCS7

Item	Description		
		802.11n HT40 (5 GHz)	-85 dBm@MCS0 -64 dBm@MCS7
		802.11ac 20M (5 GHz)	-87 dBm@MCS0 -68 dBm@MCS7
		802.11ac 40M (5 GHz)	-83 dBm@MCS0 -66 dBm@MCS7 -59 dBm@MCS9
		802.11ac 80M (5 GHz)	-80 dBm@MCS0 -63 dBm@MCS7
		802.11ac 80M (5 GHz)	-56 dBm@MCS9
Power consumption	< 12 W		
Power supply	AC: 100 V to 240 V		
	DC: 12 V/2 A		
Dimensions (D x H)	95 mm x 210 mm		
Weight	About 530 g (power adapter excluded)		
Temperature	Working temperature: 0°C to +40°C		
	Storage temperature: –20°C to +70°C		
Humidity	5% to 95% RH		

NOTE

You are advised to deploy the device and power on it in three months after it is received or store it under following circumstance:

- Temperature: –10°C to 35°C
- Humidity: 30% RH to 85% RH

Storage environment should be equipped with temperature and humidity equipment and dehumidification equipment to monitor and adjust the temperature and humidity.

NOTICE

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

1.4 Antenna Specifications

Table 1-2 Specifications of the LTE main antenna

Item	Description
Frequency range	2300 MHz to 3800 MHz
Input impedance	50 Ω
Standing wave ratio (SWR)	< 2
Efficiency	> 50%
Gain	3 dBi
Polarization type	Linear polarization
Direction	Omni-directional

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 2.4 GHz antenna specifications

Item	Description
Frequency	2.400 GHz to 2.4835 GHz
Input impedance	50 Ω
Standing wave ratio	< 3
H side gain	2 dBi
Efficiency	> 60%
Polarization	Linear polarization

Table 1-4 WLAN 5 GHz antenna specifications

Item	Description
Frequency	5150 MHz to 5850MHz
Input impedance	50 Ω
Standing wave ratio	< 3
H side gain	2 dBi
Efficiency	> 60%
Polarization	Linear polarization

1.5 Software Specifications

Table 1-5 describes the software specifications of the eA280.

Table 1-5 Software specifications

Item	Description	
Gateway	Supports the default route, namely, the route with the IP address **0.0.0.0**.	
	Supports the Address Resolution Protocol (ARP).	
	Supports the Internet Control Message Protocol (ICMP).	
	Supports the domain name service (DNS).	
	NAT	Supports network address translation (NAT) and Network Address and Port Translation (NAPT), which complies with RFC2663, RFC3022, and RFC3027.
	DHCP server	• The default IP address of the DHCP server 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. • Enables and disables the DHCP server. • Configures DHCP server address pools. • Sets the lease time. • Supports static IP address reserving. • Supports DHCP relay.
	Routing Behind MS	Supports routing Behind MS
	UE direct connect	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	

Item	Description	
LAN	• Auto-negotiation between 10 /100 /1000 Mbit/s • MDI/MDIX auto-sensing • 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	
VoIP	Supports G.729, G.711a, and G.711u.	
	Supports SIP (RFC3261).	
	Supports SDP (RFC2327).	
	Supports DNS.	
	Supports DTMF.	
	Supports SIP ALG.	
Upgrade	Supports TR-069 upgrade and local upgrade and online upgrade.	
SIM	Supports PIN management and SIM card authentication. Supports soft SIM cards.	
Frequency Lock	Support frequency, cell lock in two ways.	
Dial-up connection	Supports automatic and manual connection.	
Importing and exporting configuration	Encrypts and backs up the current configuration, and then restores from a backup configuration.	
WLAN	Broadcasts and hides service set identifiers (SSIDs).	
	Complies with WLAN 2.4 GHz IEEE 802.11b/g/n and 5 GHz 802.11a/n/ac	
	Supports WPS.	
	Authentication	Supports Open System authentication.
		Supports encryption using wired equivalent privacy (WEP), Wi-Fi protected access pre-shared key (WPA-PSK), and WPA2-PSK keys.
		Supports the Advanced Encryption Standard (AES) encryption algorithm.
		Supports the TKIP and AES hybrid encryption algorithm.
	MAC address authentication	Supports the MAC address authentication white list.
		Supports the MAC address authentication blacklist.
		Supports a maximum of 10 MAC address entries.

Item	Description	
	Supports automatic transmission rate adjustment.	
	Station management	Supports station status queries.
		Supports a maximum of 32 connected stations at 2.4 GHz. Supports a maximum of 32 connected stations at 5 GHz.

1.6 Product Security

eA280 security includes network security and application security. Application security includes wireless security and OM security.

1.6.1 Network Security

eA280 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 eA280, the OM TCP applications can use SSL. HTTP over SSL is generally called HTTPS. HTTPS is used for connections between the NMS/WebUI and eA280. 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

eA280 application security includes wireless security and OM security.

Wireless Security

eA280 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 eA280. 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.

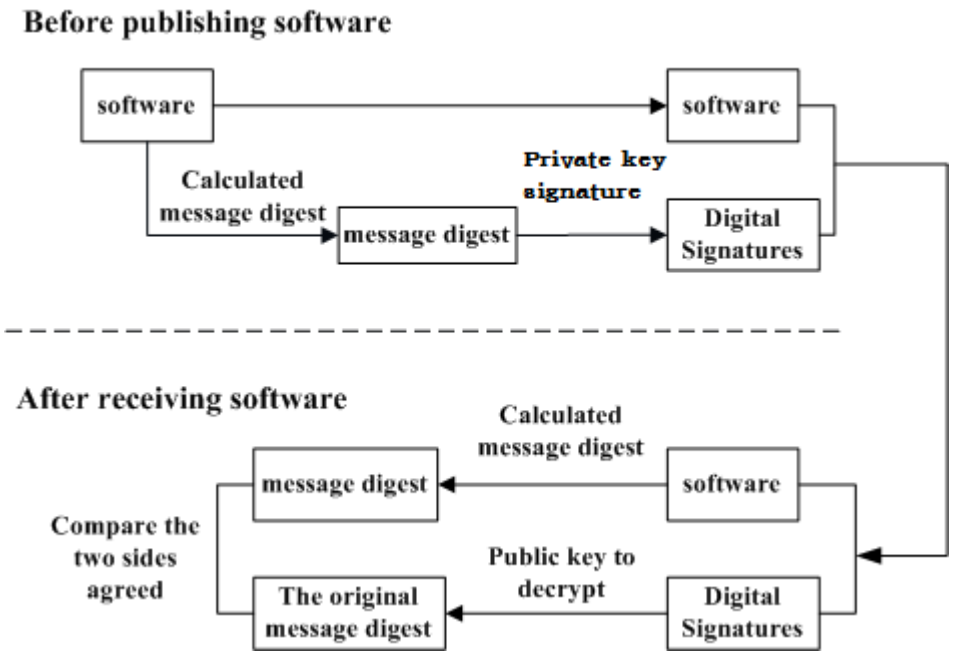
Software integrity protection helps detect viruses or malicious tampering in a timely manner, preventing insecure or virus-infected software from running on the device.

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 1-3 illustrates the principles of a software digital signature.

Figure 1-3 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.

1.7 Device Ports

1.7.1 Web Port

You can log in to the LTE 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.

NOTE

- 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 soft SIM 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**: enables the computer UI.

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

  pwd indicates the unlock password.
- **at^PORTPWD=*"oldPwd","newPwd", "newPwdConf"***: changes 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.

NOTE

- 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. It is recommended that users do not set an empty password or a simple password.
- 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 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.

1.7.4 Voice Interface

The product provides the optional Voice over IP (VoIP) function that complies with the RFC2617 protocol. The communication between the SIP client and SIP server is authenticated using MD5 digest.

2 Hardware

About This Chapter

This chapter describes the hardware and cables of the eA280s.

2.1 eA280 Hardware

This section describes the appearance, ports, and indicators of the eA280.

Appearance

Figure 2-1 shows the appearance of the eA280.

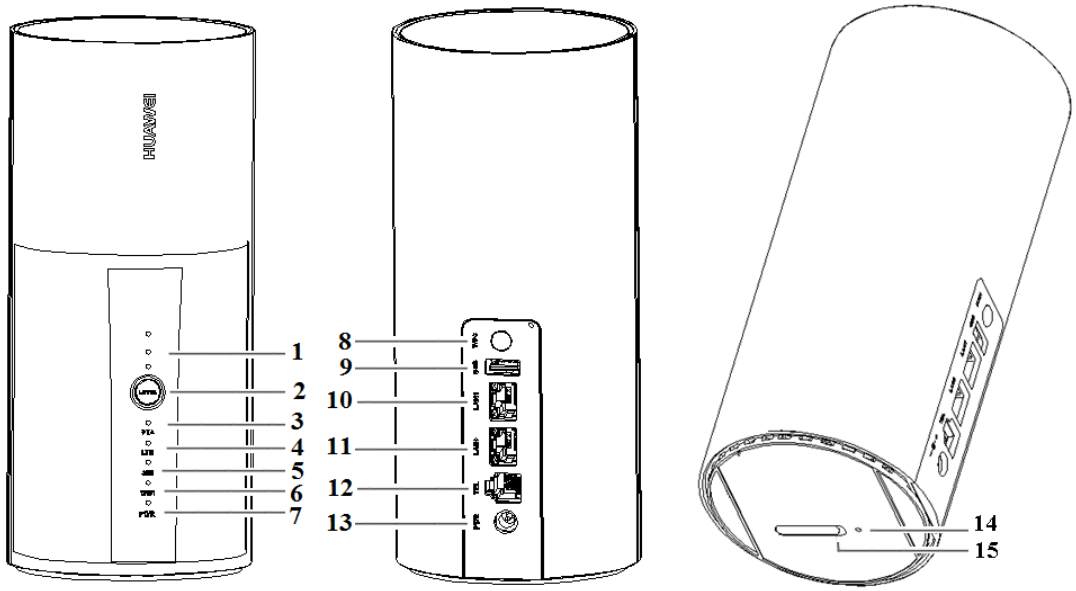
Figure 2-1 eA280 appearance

Panel

The panel of the eA280 provides the Power over Ethernet (PoE) port, SIM card maintenance window, and indicator.

Figure 2-2 shows the panel of the eA280.

Figure 2-2 Panel of the eA280



1 Signal indicator	2 WPS button	3 Mode indicator r	4 LTE indicator
5 SIM indicator	6 Wi-Fi indicator	7 Power indicator	8 PWR button
9 USB port	10 LAN1 port	11 LAN0 port	12 TEL port
13 Power port	14 Reset button	15 micro SIM card slot	

Table 2-1 lists the buttons on eA280.

Table 2-1 eA280 buttons

Item	Description
Power button	1s–5s: power on 8s or above: power off Press this button to power the LTE CPE on or off.
WPS button	1s–5s: start 5 GHz Wi-Fi WPS 5s or above: start 2.4 GHz Wi-Fi WPS

Item	Description
Reset button	Press and hold for more than 2 seconds to restore the LTE CPE to its factory settings. **NOTE** Restoring the default settings of the LTE CPE will override all the previous settings.

Table 2-2 lists the ports on eA280.

Table 2-2 eA280 ports

Item	Description
Power port	Connects to the LTE CPE's power adapter.
TEL port	Connects to telephones.
LAN port	Connects to computers, switches, or other network devices.
Micro SIM card slot	Accommodates a micro SIM card.
USB port	Only for equipment maintenance

Table 2-3 lists the indicators on eA280.

Table 2-3 eA280 indicators

Item	Description
STA indicator	• If the indicator is off, data services are disconnected. • If the indicator is steady green, the LTE CPE has successfully obtained the IP address of the peer device in the WAN, and the WLAN function has been enabled.
LTE indicator	• If the indicator is off, the micro SIM card may not be inserted into, or may be invalid. Users need to enter the PIN or PUK. • If the indicator is steady red, the network is unavailable. • If the indicator blinks green, the LTE CPE is accessing the network. • If the indicator is steady green, the LTE CPE has successfully accessed the network.

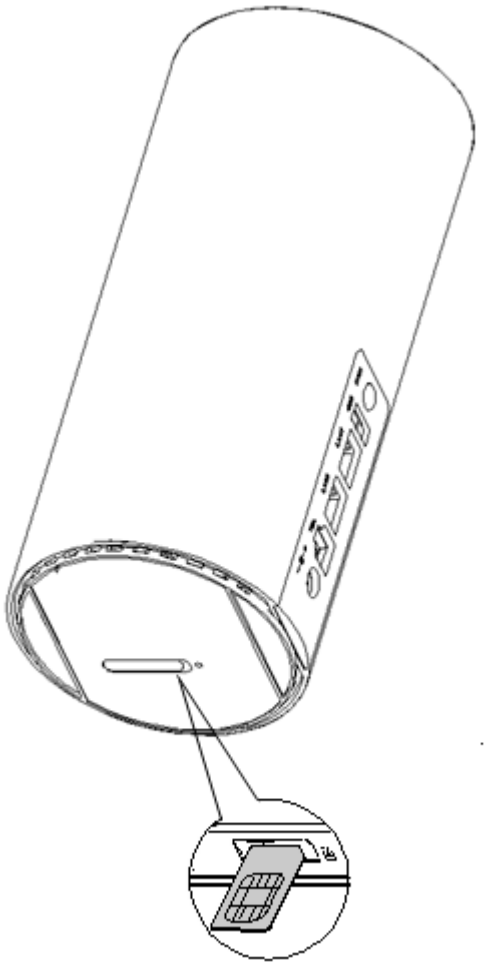
Item	Description
SIM indicator	• If the indicator is off, no micro SIM cards are inserted. • If the indicator is steady red, the inserted micro SIM card cannot work normally (for example, the card is invalid), or the PIN or PUK must be entered. • If the indicator is steady green, the micro SIM card works normally.
Wi-Fi indicator	• If the indicator is off, both 2.4 GHz Wi-Fi and 5 GHz Wi-Fi are disabled. • If the indicator blinks green, the LTE CPE is undergoing a WPS process. If the indicator status alternatively changes between on for 0.2s and off for 0.1s, the LTE CPE is undergoing the 2.4 GHz WPS process. If the indicator status alternatively changes between on for 0.5s and off for 0.1s, the LTE CPE is undergoing the 5 GHz WPS process. After either of the processes is successful, the indicator is steady green. • If the indicator is steady green, either 2.4 GHz Wi-Fi or 5 GHz Wi-Fi is enabled.
Power indicator	• If the indicator is off, the LTE CPE is not started. • If the indicator is steady red, the LTE CPE is being initialized or the initialization fails. • If the indicator is steady green, the LTE CPE has been successfully initialized. • If the indicator blinks green, the LTE CPE is being upgraded.
Signal indicators	• If an indicator is steady red, no signals are available. • The indicator that is steady blue indicates the signal strength. If all indicators are steady blue, the signal strength is strong.

3 Getting Start

3.1 Installing the Micro SIM Card

Figure 3-1 shows how to install the micro SIM card.

Figure 3-1 Installing the micro SIM card



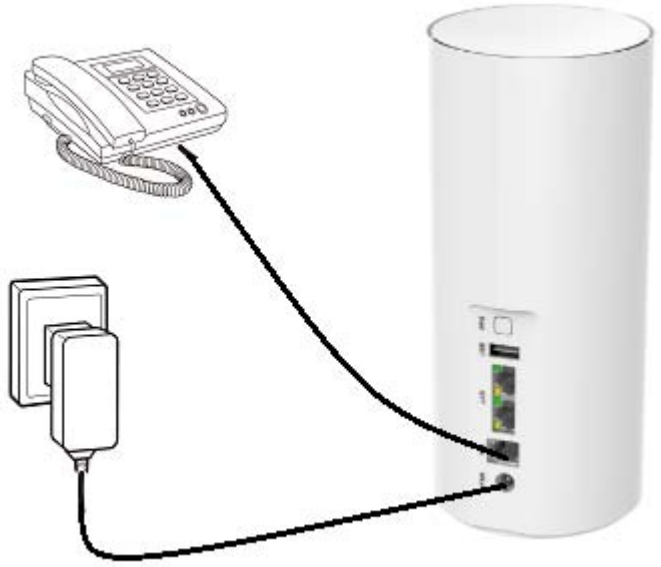
NOTE

- When removing the micro SIM card, gently press the micro SIM card in and then release. The card will automatically pop out.
- Do not remove the micro SIM card when it is in use. Doing so will affect the performance of your LTE CPE, and data stored on the micro SIM card may be lost.

3.2 Connecting to the Power Adapter

Figure 3-2 shows how to connect to the power adapter.

Figure 3-2 Connecting to the power adapter



NOTE

- Only use power adapters compatible with the LTE CPE and provided by a designated manufacturer. Use of an incompatible power adapter or one from an unknown manufacturer may cause the LTE CPE to malfunction, fail, or could even cause a fire. Such use voids all warranties, whether expressed or implied, on the product.
- The LTE CPE's power adapter model is HW-120100XYW, HW-120200XYW, HKA01212010-XY or HKA02412020-XY. X and Y represent letters or numbers that vary by region. For details about the specific adapter model, contact an authorized dealer.

4 Configuration Introduction

About This Chapter

This chapter describes the configuration of the eA280s.

4.1 Logging In to the WebUI

Prerequisites

- The deployment on the network side is complete.
- The computer has been connected to the eA280.
- The installation of the eA280 is complete.
- The eA280 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 eA280 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 the default value **admin** and **Password** set to the default value **admin**.

Step 3 Open the **Password Modification** page and set **New Password**.

----End

4.2 NAT Settings

Prerequisites

- Install EPC and LTE CPE and commission them so that they are ready to be connected.
- Configure the NAT Settings on EPC.

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.

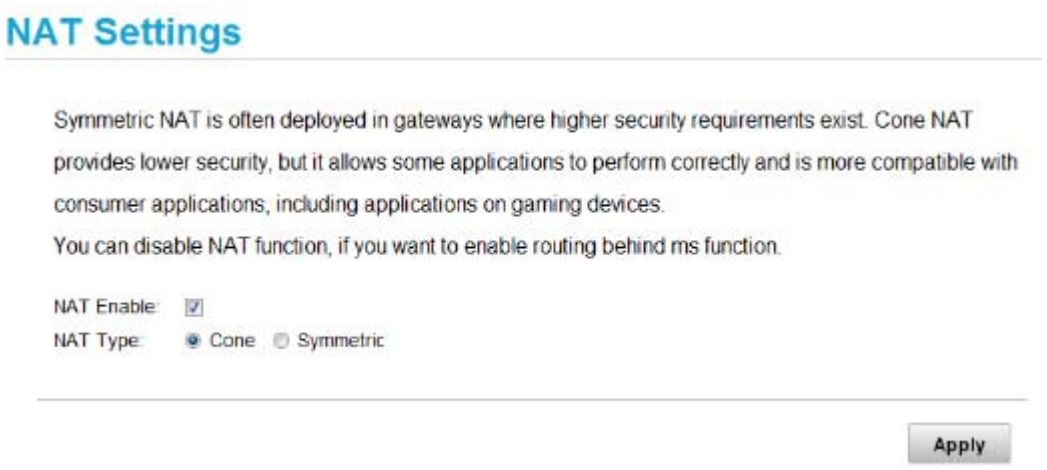
Procedure

Step 1 Log in to the WebUI.

For details, see section 4.1 "Logging 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 DHCP Relay

Prerequisites

- The DHCP server and LTE CPE are installed.
- Install the DHCP server and LTE CPE and commission them so that they are ready to be connected.

Procedure

NOTE
The DHCP clients connected to the LTE CPE cannot obtain IP addresses from the DHCP server until DHCP Relay and Routing Behind MS are both enabled.

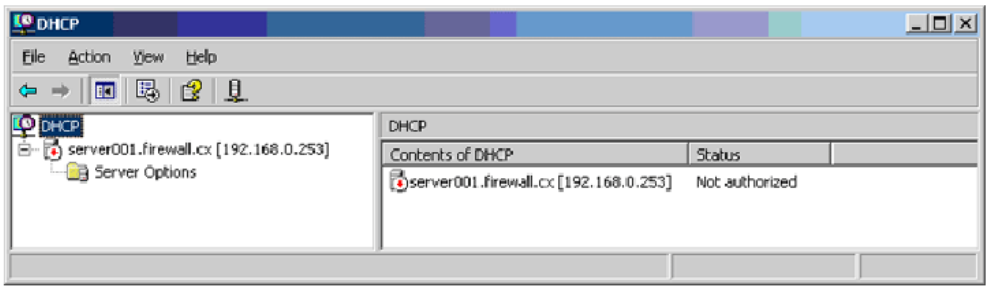
Step 1 Configure the DHCP server.

This document demonstrates how the DHCP server can be configured using Windows Server 2003.

a. On the computer, go to **Control Panel > Management Tools > DHCP.**

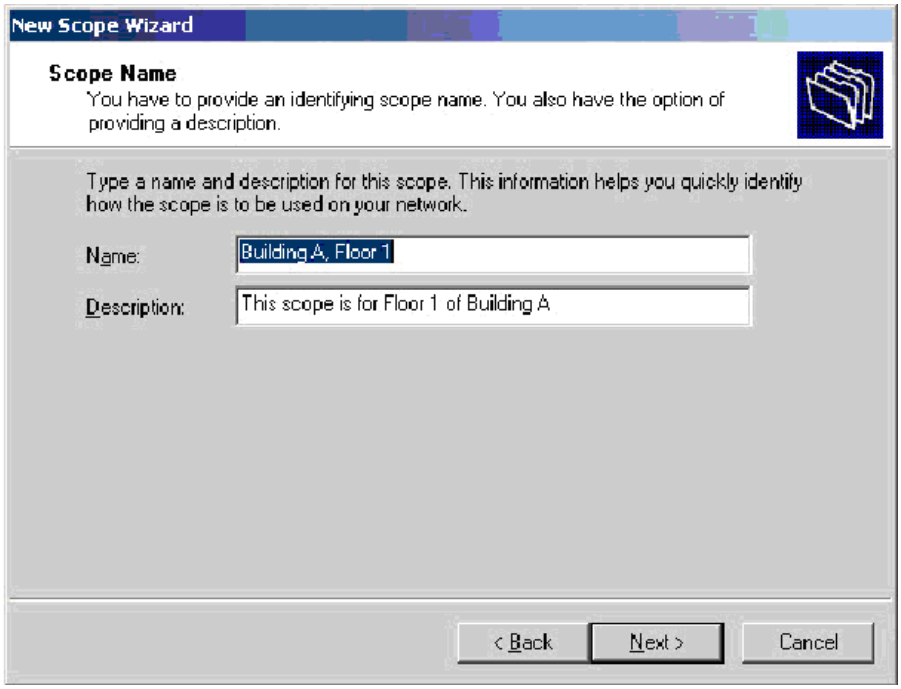
From the left panel, right-click **Server Options**, and choose **New Scope Wizard**.

Figure 4-2 Choosing New Scope Wizard



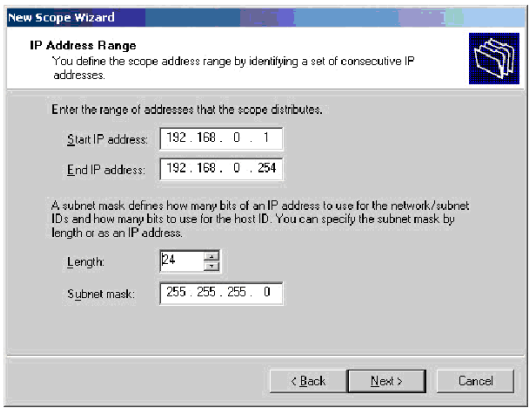
b. Add a scope name.

Figure 4-3 Adding a scope name



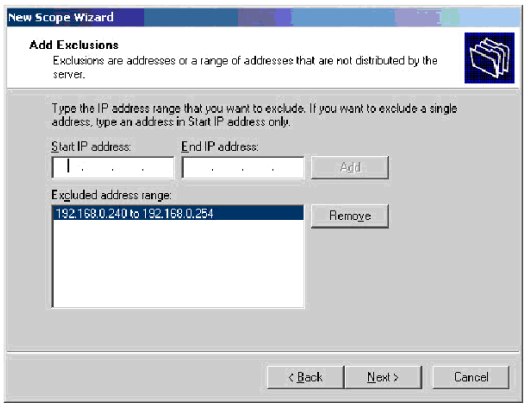
c. Set the IP address range.

Figure 4-4 Setting the IP address range



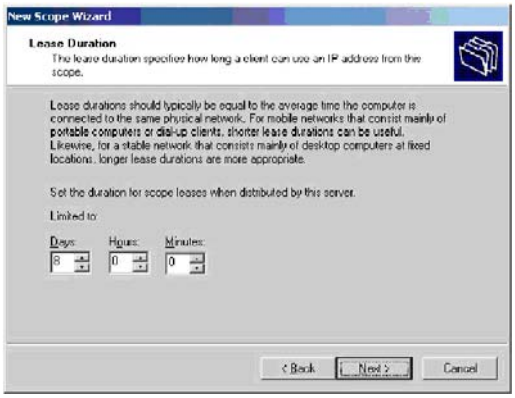
d. Click **Next**.

Figure 4-5 Clicking Next



e. Set the lease duration.

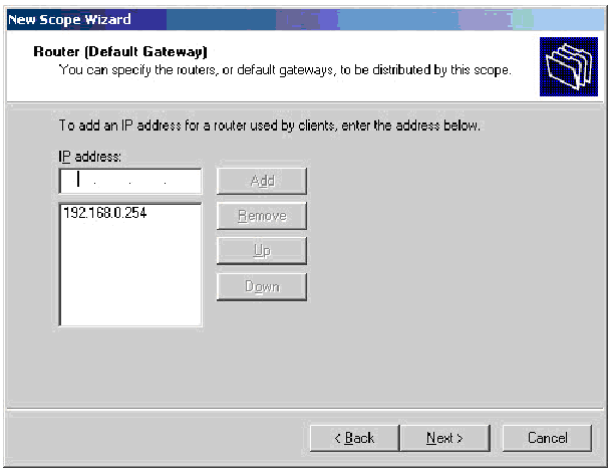
Figure 4-6 Setting the lease duration



f. On the screen that is displayed, choose **Yes, I want to configure these settings now** and click **Next**.

g. Set the default gateway.

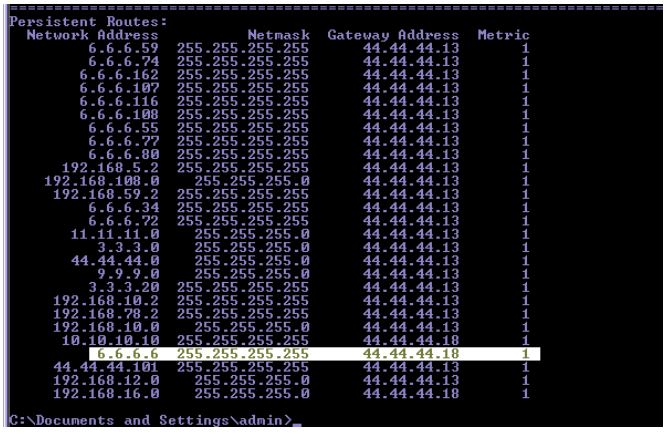
Figure 4-7 Setting the default gateway



h. Click **Next** on each of the following pages and then click **Finish**.

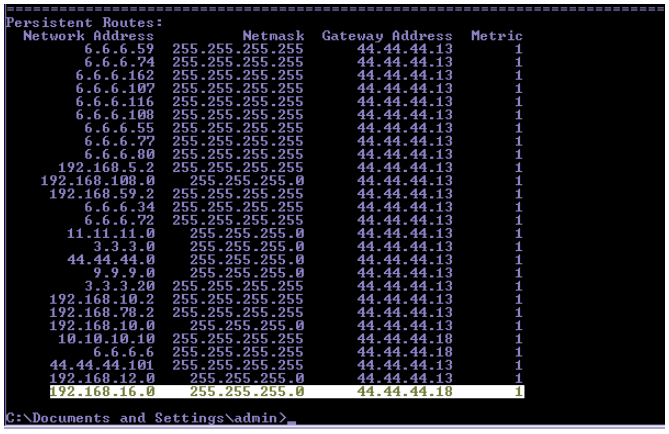
Add a route from the DHCP server to the LTE CPE. The next hop is the EPC's IF IP address.

Figure 4-8 Next hop



Add a route from the DHCP server to LAN devices connected to the LTE CPE. The next hop is the EPC's IF IP address.

Figure 4-9 Next hop



Step 2 Log in to the WebUI.

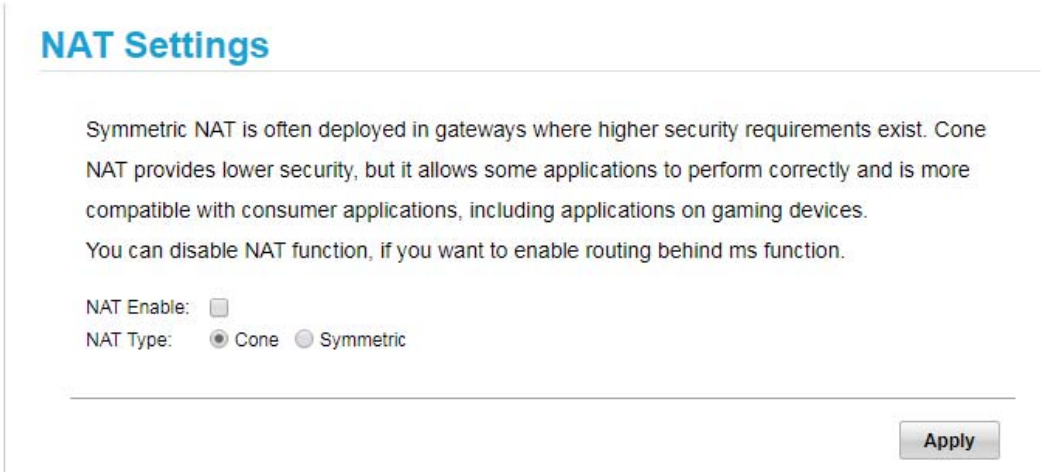
For details, see section 4.1 "Logging In to the WebUI."

Step 3 Go to **Settings** > **DHCP**, set **IP Address**, and click **Apply**.

Figure 4-10 Setting the DHCP server address

Step 4 Go to **Settings** >**Security** > **NAT Settings**, deselect **NAT Enable** under **NAT Settings**, and click **Apply** to enable Routing Behind MS.

Figure 4-11 Enabling Routing Behind MS



----End

4.4 VoIP

Prerequisites

- Hardware and software for the eSpace U1980 are installed and the LTE CPE is installed.
- If the eSpace U1980 server is used as the VoIP server, Install the eSpace U1980 and LTE CPE and commission them so that they are ready to be connected.

Procedure

Step 1 Log in to the WebUI.

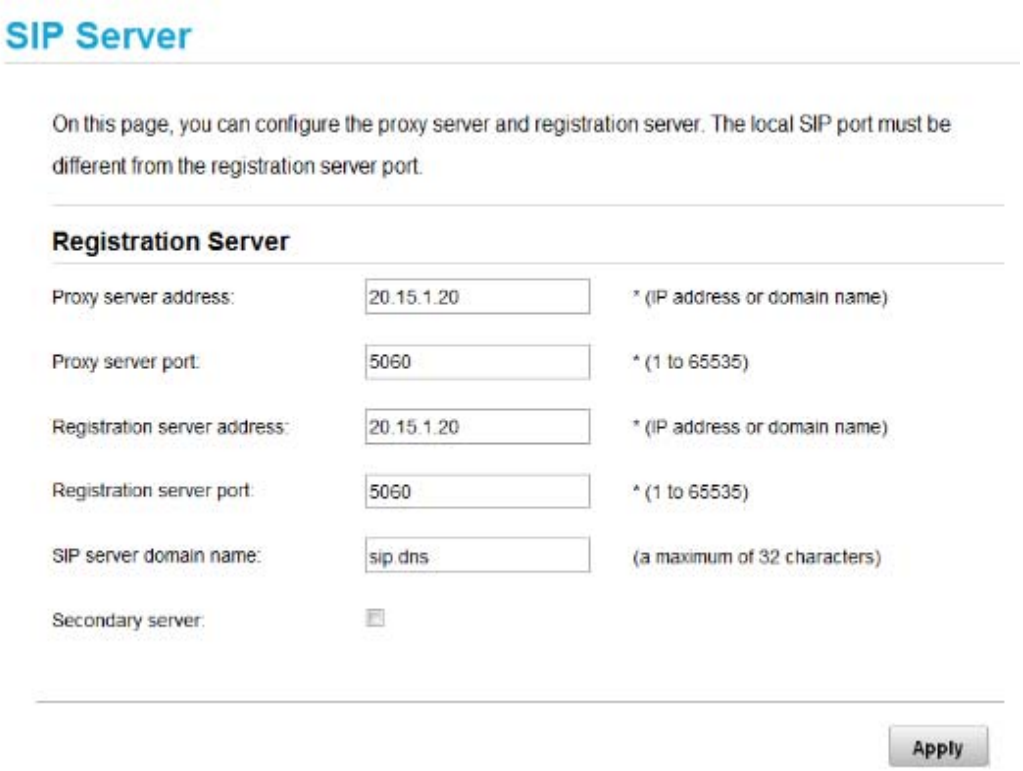
For details, see section 4.1 "Logging In to the WebUI."

Step 2 Choose **Settings** >**VoIP** > **SIP Server** to configure parameters for the connection between the LTE CPE and SIP server.

- Set **Proxy server address** and **Registration server address** to the same IP address.
- Set **Proxy server port** and **Registration server port** to **5060**.

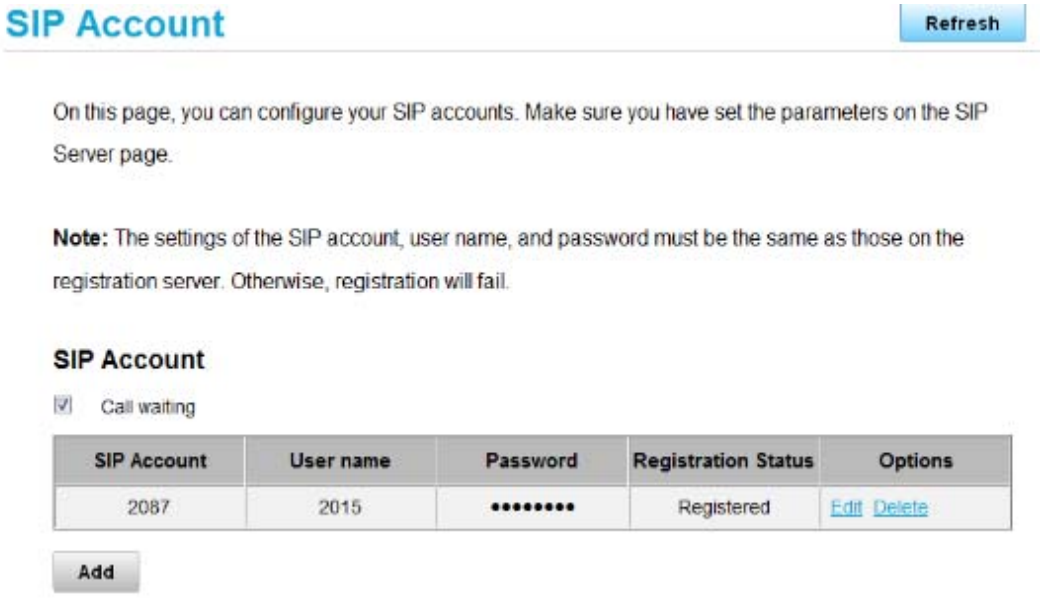
If a DNS server is deployed on the network and domain name resolution is required for the LTE CPE to communicate with the SIP server, the SIP server's domain name must first be configured. In this example, the LTE CPE and SIP are configured to communicate with each other directly. See the following figure:

Figure 4-12 Configuring parameters for the connection between the LTE CPE and SIP server



Step 3 On the **SIP Account** page, configure an SIP account and credentials, and click **Add**, as shown in Figure 4-13.

Figure 4-13 Configuring an SIP account



Step 4 On the **SIP Account** page, change the newly added SIP accounts and credentials as required.

To do so, select the required row and click **Edit**. On the displayed page, enter the account number provided by the operator and enter the user name and password provided by the operator in the **User name** and **Password** text boxes.

----End

4.5 Profile Management

Step 1 Log in to the WebUI.

For details, see section 4.1 "Logging In to the WebUI."

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

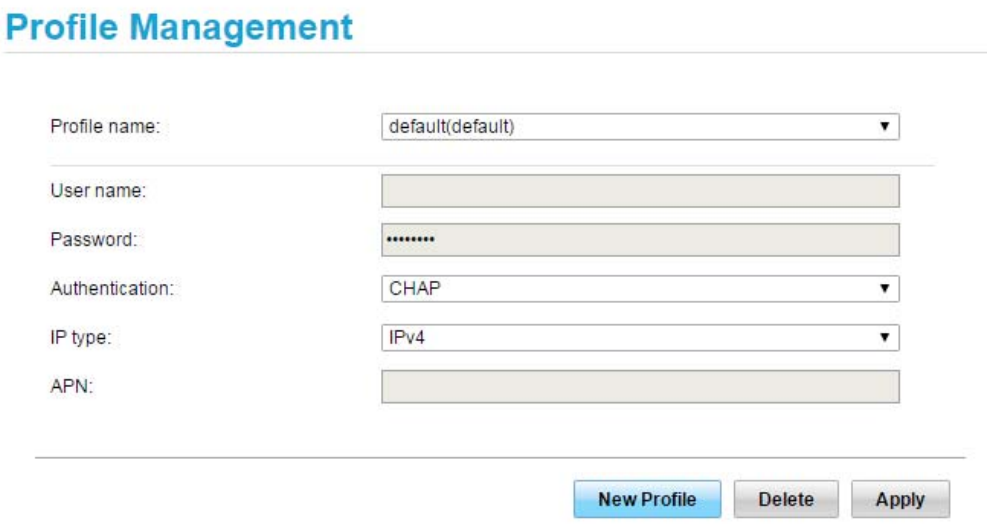
Step 3 Click **New Profile**. On the displayed page, set **Profile name**, **User name**, **Password**, **Authentication,IP type** and **APN** as required.

NOTE

- 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 4 Click **Apply**.

Figure 4-14 Profile management



4.6 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 CPE parameters. If you set the ACS parameters on both the CPE and ACS, the network parameters on the CPE are automatically set using the TR-069 function, and you do not need to set other parameters on the CPE.

If you want to retain TR-069 settings after restoring factory settings, you can set the **Preserve Settings** to **Enable**.

NOTICE

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

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

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

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

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

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

Step 2 To enable the CPE to send informing 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 the ACS function, set ACS URL to the loopback address 127.0.0.1.

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

To use the 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 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 When **Enable Certificate** is enabled, you can import the certificate for authentication.

This interface is extensible to replace certificates for authentication between ACS and CPE. To make authentication run right, the certificates in ACS and CPE must match each other. By default, there is not a pair of certificates in ACS and CPE. Contact device provider for certificates if you want to use them.

Step 8 Click **Submit**.

NOTE

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

----End

4.7 Security Settings

4.7.1 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 "Logging In to the WebUI."

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

Step 3 Click **Apply**.

----End

4.7.2 LAN IP Address Filtering

Step 1 Log in to the WebUI.

For details, see section 4.1 "Logging 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

4.7.3 MAC Address Filtering

Step 1 Log in to the WebUI.

For details, see section 4.1 "Logging 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

4.7.4 Domain Name Filtering

Step 1 Log in to the WebUI.

For details, see section 4.1 "Logging 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 eA280 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 target version.

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

----End

5.3 TR069 eSight Update

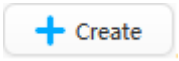
5.3.1 Firmware Version

Prerequisites:

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

Procedure:

Step 1 Choose **Configuration** > **eLTE Device** > **CPE Management** > **Firmware Upgrade Management** > **Firmware Version** 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**.

NOTE

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.

NOTE

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:

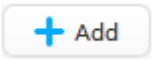
Step 1 Choose **Configuration** > **eLTE Device** > **CPE Management** > **Firmware Upgrade Management** > **Upgrade Management** from the main menu.

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 CPE.
   - If you set to **ON**, eSight performs the upgrade task when the target version is the same as the current version of the 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 eA280.

6.1 Maintenance Preparation

Before performing site maintenance for the eA280, learn about the site information, select required maintenance items.

Learning About the Site Information

Gather the following site information before going to the eA280 site to perform maintenance.

- Persisting faults and alarms
- Hardware configuration
- Natural environment

Selecting Maintenance Items

Select suitable maintenance items based on the eA280 site conditions.

Maintenance items must include the following aspects:

- Natural environment of the eA280 site
- Power supply of the eA280
- eA280

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 eA280 is complete.
- The eA280 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.

1. 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.

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

- When the LTE CPE does not run properly, the **System Check** can be used to preliminarily identify the problem.

1. 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.

2. Choose **Settings > TR-069 Management> Diagnosis** to open the **Diagnosis** page.
3. Set **Diagnosis Method** to **System Check**.
4. Click **Check**.
5. 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 FAQs

7.1 What Do I Do If the WebUI Fails to Be Opened?

Problem Description:

I cannot visit the Web management page of eA280 using a 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, contact Huawei technical engineers.

----End

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

Problem Description:

The power indicator is not working.

Solution:

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

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

NOTE

Power adapter for the eA280 power supply, supporting the power adapter specifications are as follows:

- The minimum input voltage:100 V
- The maximum input voltage: 240V
- Rate output voltage or current: 12V/2A
- Output voltage accuracy: +5%
- Input or output cable connector: AC VDE 2PIN/DC H PLUG 2.1x5.5x9.5mm,Length of wire 1.5M

----End

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

Problem Description:

The data service is not provided.

Solution:

Step 1 Check whether the LTE CPE is powered on. The power supply is provided if the Power indicator presents green.

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 LTE indicator is steady green.

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

----End

8 Privacy and Security

8.1 Privacy Policy

To better understand how we protect your personal information, 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 Wi-Fi encryption method to WPA2-PSK/AES/ WPA-PSK. Ensure Wi-Fi 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 eA280'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. Keep the password secure to prevent device parameters from being modified or exposed.

9 Acronyms and Abbreviations

This chapter lists the acronyms and abbreviations related to the eA280.

Table 9-1 List of acronyms and abbreviations

Acronym/Abbreviation	Full Name
APN	Access Point Name
ARP	Address Resolution Protocol
ALG	Application Level Gateway
3GPP	3rd Generation Partnership Project
CPE	Customer Premises Equipment
CRC	Cyclic Redundancy Check
DNS	Domain name server
DTMF	Dual Tone Multiple Frequency
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
GRE	Generic Routing Encapsulation
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
LTE	Long Term Evolution
ICMP	Internet Control Message Protocol
MAC	Media Access Control
NAT	Network Address Translation
PoE	Power over Ethernet
SDP	Session Description Protocol
SIM	Subscriber Identity Module
SIP	Simple Internet Protocol

Acronym/Abbreviation	Full Name
SPI	Security Parameter Index
SSL	Secure Sockets Layer
TR069	Technical Report 069
URL	Uniform Resource Location
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
WebUI	Web User Interface
WEP	Wired Equivalent Privacy
WPA-PSK	Wi-Fi Protected Access Pre-Shared Key

RSS-247 required, 5G WIFI frequency indoor use only.

eA280-135' FCC Statement

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 20 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 complies 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) th is 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 tra nsmitter 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 environnement non contrôlé. Cet émetteur 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 20cm between the radiator& your body.

Cet équipement doit être installé et utiliséavec une distance minimale de 20cm entre leradiateur & votre corps.