



User Manual

LTE200

Issueⁱ1.1.0

Date 2020-08

About this document

Overview

This document introduces the hardware, function, installation, configuration, and maintenance information of the LTE200 LTE CPE.

Chapter	Detail
1 Product Overview	Introduce hardware, software, and antennas specifications
2 Hardware Introduction	Introduce port information
3 Installation Introduction	Introduce installing procedures
4 Configuration Introduction	Introduce configuration method
5 Maintenance Introduction	Introduce maintenance method
6 FAQ	Introduce the problems and solutions
7 Privacy and Security	Introduce the privacy and security

Product version

Main model	Sub-models	Details
LTE200	LTE200	

Reader

This document is intended for:

- System engineers
- Product engineers
- Technical support engineers

History

Issue	Date	Details
V1.0.0	2019-04	Initial official release
V1.0.1	2019-10	Revision
V1.1.0	2020-08	Revision

Contents

ABOUT THIS DOCUMENT	1
CONTENTS.....	0
1 PRODUCT OVERVIEW.....	5
1.1 PRODUCT INTRODUCTION	5
1.2 APPLICATION SCENARIOS	5
1.3 HARDWARE SPECIFICATION	6
1.4 SOFTWARE SPECIFICATION.....	7
1.5 ANTENNA SPECIFICATION	9
1.6 DEVICE PORTS.....	9
1.6.1 <i>Web port</i>	9
1.6.2 <i>TR069 port</i>	10
2 HARDWARE INTRODUCTION	12
2.1 LTE200 HARDWARE	12
2.1.1 <i>Appearance</i>	12
2.1.2 <i>Panel interface</i>	12
2.1.3 <i>LED indicators</i>	13
2.1.4 <i>Button</i>	13
2.2 CABLES	14

2.2.1 <i>RJ45 Network cables</i>	14
2.2.2 <i>RJ11 Telephoneline</i>	14
3 INSTALLATION INTRODUCTION	15
3.1 INSTALLATION PREPARATION	15
3.2 INSTALLATION PROCEDURE.....	15
3.3 INSTALLATION CHECK.....	15
4 CONFIGURATION INTRODUCTION	17
4.1 LOG INTO WEB UI	17
4.2 QUICK CONFIGURATION	17
4.2.1 <i>LTE quick configuration</i>	17
4.2.2 <i>VOIP quick configuration</i>	18
4.2.3 <i>WLAN quick configuration</i>	18
4.3 LTE CONFIGURATION	19
4.3.1 <i>LTE Data service settings</i>	19
4.3.2 <i>LTE APN settings</i>	20
4.3.3 <i>LTE mode settings</i>	20
4.3.4 <i>PIN settings</i>	21
4.4 ETHERNET	22
4.4.1 <i>Ethernet connection</i>	22
4.5 LAN CONFIGURATION	23
4.5.1 <i>LAN interface settings</i>	23

4.5.2 DHCP Settings	24
4.5.3 IPv6 settings.....	24
4.6 WLAN CONFIGURATION.....	25
4.6.1 WLAN Basic.....	25
4.6.2 WLAN security.....	25
4.6.3 WPS	26
4.7 QoS CONFIGURATION.....	26
4.7.1 QoS Policy	26
4.7.2 Rate Limit settings	27
4.8 ROUTE CONFIGURATION	27
4.8.1 Static Routing.....	27
4.9 WAN SETTINGS.....	28
4.10 DDNS SETTINGS.....	28
4.11 FIREWALL SETTINGS	29
4.11.1 DMZ	29
4.11.2 Attack Protection Settings	29
4.12 MAC FILTER	30
4.13 IP/PORT FILTER	30
4.13.1 IP/Port Filtering	31
4.14 VOIP SETTINGS.....	31
4.14.1 Basic settings	31
4.14.2 Advanced settings.....	32

5 MAINTENANCE INTRODUCTION	33
5.1 DIAGNOSIS.....	33
5.1.1 Ping testing	33
5.1.2 Tracert testing	33
5.1.3 Inform Manual reporting.....	34
5.2 DEVICE MANAGEMENT	34
5.2.1 Device Restart	34
5.2.2 Software Upgrade	34
5.2.3 Restore Factory Settings	35
5.3 USER MANAGEMENT	35
5.3.1 Change Password	35
5.4 TIME MANAGEMENT	36
5.4.1 Time server	36
5.5 TR069 REMOTE MANAGEMENT	36
6 FAQ.....	38
Q1. THE LOGIN WINDOW INTERFACE DOES NOT DISPLAY.....	38
Q2. HOW TO RESET THE CPE.....	38
Q3. I FORGET THE PASSWORD OF WEB MANAGEMENT INTERFACE.....	38
Q4. I FORGET THE PASSWORD OF WI-FI.	38
7 PRIVACY AND SECURITY	39
7.1 PRIVACY PROTECTION.....	39

7.2 SECURITY MAINTENANCE.....	39
7.3 DEFAULT SECURITY CONFIGURATION	39
8 ACRONYMS AND ABBREVIATIONS.....	40

1 Product Overview

About this chapter

This chapter introduces the product function, application, specification, and interface information.

1.1 Product Introduction

LTE200 is an LTE wireless gateway CPE that implements the conversion between LTE wireless data and wired Ethernet data. It supports data backhaul function and can be used independently. LTE200 is used for home and SOHO deployment.

LTE200 supports the LTE R11 standards and CAT4UE category, which provides the following services:

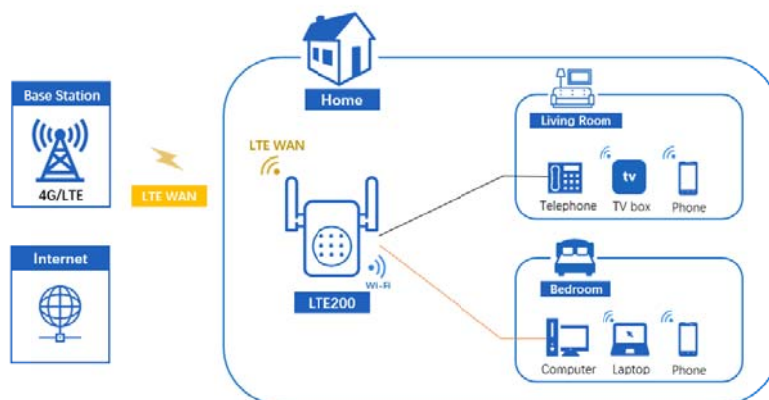
- Data service
- Voice service
- SMS
- Wi-Fi service
- Local maintenance management function

1.2 Application Scenarios

LTE200 provides wireless broadband and wired Ethernet data services.

LTE200 is primarily for home and SOHO deployment.

Figure 1-1 Application diagram



1.3 Hardware Specification

The LTE200 hardware specifications are shown in table 1-1.

Table 1-1 Hardware specifications

Item	Description			
Technical standard	WAN	<ul style="list-style-type: none"> • Mobile Network: 3GPP Release 11 • Ethernet: IEEE 802.3/802.3u 		
	LAN	IEEE 802.3/802.3u		
	WLAN	IEEE 802.11b/g/n		
Working frequency band	LTE200	LTE FDD: Band 2/4/5/12/13/14/66/71 WCDMA: Band 2/4/5		
Data service	LTE FDD	DL 150 Mbps, UL 50 Mbps		
	WCDMA	DL 384 Kbps, UL 384 Kbps		
	WLAN	<ul style="list-style-type: none"> • 802.11b: 11 Mbps, 5.5 Mbps, 2 Mbps, 1 Mbps • 802.11g: 54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, 9 Mbps, 6 Mbps • 802.11n: 300 Mbps (HT40 MCS15), 144.4 Mbps (HT20 MCS15) 		
External port	<ul style="list-style-type: none"> • One power adapter port • one WLAN/LAN port (RJ45) • phone port (RJ11) • One SIM card slot 			
Antennas	<ul style="list-style-type: none"> • External 2*2 LTE antenna • Internal WLAN 2.4GHz antenna 			
Indicator	<ul style="list-style-type: none"> • One Phone indicator • One WPS indicator • One 2.4GHz Wi-Fi indicator • LAN indicator • One LTE indicator • One system indicator • One power indicator 			
Button	<ul style="list-style-type: none"> • One Wi-Fi button • One WPS button • One Reset Button 			
Maximum transmit power	LTE FDD	Class 3 (23dBm±2dB)		
	WCDMA	Class 3 (24dBm+1/-3dB)		
	WLAN	802.11b	13 dBm (+3 dB/-3 dB) @11 Mbps	
		802.11g	<ul style="list-style-type: none"> • 24 dBm (+3 dB/-3 dB) @6 Mbps • 24 dBm (+3 dB/-3 dB) @54 Mbps 	
802.11n		<ul style="list-style-type: none"> • 24 dBm (+3 dB/-3 dB) @MCS0 • 24 dBm (+3 dB/-3 dB) @MCS7 		
Receiving	WLAN	802.11b	Typ. -92 dBm@1 Mbps	

Sensitivity		Typ. -85 dBm@11 Mbps
	802.11g	Typ. -88 dBm@6 Mbps Typ. -70 dBm@54 Mbps
	802.11n HT20	Typ. -88 dBm@MCS0 Typ. -68 dBm@MCS7
	802.11n HT40	Typ. -84 dBm@MCS0 Typ. -66 dBm@MCS7
Power consumption	Full load	<10W
	Standby mode	<4W
AC/DC power supply	<ul style="list-style-type: none"> • DC: 12 V/1 A • AC: 220V±20% 50Hz±5% 	
Operating environment	Temperature	<ul style="list-style-type: none"> • Operating: -10°C to 55°C • Storage: -40°C to +70°
	Humidity	5% - 95%
	Atmospheric pressure	86kPa to 106kPa

1.4 Software Specification

Table 1-2 Software specifications

Item	Description	
Mobile network	Service management	
	Auto/manual APN	
	SIM card settings	
WAN	Support WAN/LAN transform	
	Connection mode: PPPoE/DHCP/Static	
	10 Mbps, 100 Mbps, and 1000 Mbps auto-negotiation	
	MDI/MDIX auto-sensing	
	IEEE 802.3/802.3u is compatible	
WLAN	IEEE 802.11b/g/n	
	MSSID	
	Channel adaption	
	Wireless power saving: adaptable power control	
	WPS (PBC/PIN mode)	
	WMM	
	Isolation	<ul style="list-style-type: none"> • AP isolation • SSID isolation
	Security mode	<ul style="list-style-type: none"> • WPA2.0 PSK • WPA1.0+WPA2.0 PSK • WEP shared Key • Open

	WPA encryption	<ul style="list-style-type: none"> • AES • TKIP • TKIP+AES
Voice service	VoIP	<ul style="list-style-type: none"> • SIP protocol • Call forwarding • Number hiding • Conference • Call waiting and call holding
SMS	<ul style="list-style-type: none"> • Short message sending and receiving • Support extra-long message 	
Gateway	IPv4/IPv6 protocol	
	Static (v4/v6) routing	
	DHCP server	<ul style="list-style-type: none"> • Default routing address is 192.168.1.1 • Default address from 192.168.1.2 to 192.168.1.254 • IP address can be defined by user • Default DHCP lease is 24 hours
	NAT/ALG/DMZ	
	Dynamic Domain Name System (DDNS)	
	IGMP snooping and IGMP proxy	
	MLD snooping and MLD proxy	
	SNTP	
Firewall setup	Firewall level settings	
	Built-in NAT firewall	
	Defense of attacks	<ul style="list-style-type: none"> • Dos Attacks • Port Scan • ARP spoofing • ARP flooding
	URL filtering	<ul style="list-style-type: none"> • Up to 32 URL items
	IP filtering	
	MAC filtering	<ul style="list-style-type: none"> • Black/White list • Up to 16 MAC address items
	Port filtering	<ul style="list-style-type: none"> • Inflow filtering • Outflow filtering • Up to 16 flow items
QoS	802.11e WMM	
	Classification of service flow	
	DSCP/802.1p	
	SP and WRR mode	
	Port/VLAN/IP Rate limitation	
Management	Web UI local management	
	TR069 remote management	
	CLI	
	UPnP	

	Diagnostic	Ping
		Tracert
		TR069
System Requirements	Operating System	Window XP, Windows Vista, Windows 7/8/8.1/10 with latest upgrades
	Web Brower	<ul style="list-style-type: none"> • IE 8.0 and above • Firefox 24.0 and above • Safari 6.0 and above • Opera 12.0 and above • Chrome 27.0 and above

1.5 Antenna Specification

Table 1-3 The LTE antenna specifications

Item	Description
Frequency	600 MHz ~ 894 MHz 1710 MHz ~ 2170 MHz
Input impedance	50 Ω
Standing wave ratio	< 3
Gain	4 dBi (peak value)

Table 1-4 The WLAN 2.4 GHz antenna specifications

Item	Description
Frequency	2.400 GHz~2.500 GHz
Input impedance	50 Ω
Standing wave ratio	< 2
Gain	3 dBi

1.6 Device Ports

1.6.1 Webport

User can log into the CPE Web UI over HTTP to manage the CPE, including configuring, querying settings, exporting running logs, querying device logs, importing and exporting the configuration, restarting and updating the CPE, and restoring the CPE to its default settings. For more details, see the Web UI online help.

- The default Web UI login username and password are **admin** and **admin** respectively.
 - User can change the login password on the Web UI.
 - To improve security, change the default password at your first login and regularly

change the password.

- A password must meet the following rules:
 - a) A password consists of 8 to 15 characters.
 - b) 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: `~!@#%&^&*()-_+=\|[]{};:","<.>/?

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

NOTE

- The maximum number of Web UI login attempts is three. After three login failures, the Web UI login page is locked and will be unlocked after oneminute.
- When the Web UI login password is forgotten, restore the device to the factory default configuration through 'Reset' button; refer to the AT command manual to restore factory defaults by yourself; or contact the device operator to reset the password through TR-069.
- If you do not perform any operation within 300seconds after logging in to the Web UI, the system automatically logs you out.

1.6.2 TR069port

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

- The management functions include device configuration, configuration query, running log exporting, and device updating.
- The account used for connections between the CPE and TR-069 management equipment is managed by personnel in the central office. The default account name and passwords are **tr069** and **tr069** respectively.
- Digest-MD5 authentication is used for connections between the CPE and TR-069 management equipment in the central office, and the authentication complies with TR-069 Amendment 4.
- You can also change the password for connections between the CPE and TR-069 management equipment in the central office. A password must meet the following Rules:
 1. A password consists of 6 to 15 characters.
 2. A password must meet the following rules:
 - at least one lowercase letter (a-z);
 - at least one uppercase letter (A-Z);
 - at least one number (0-9);

- at least one of special characters: `~!@#%&*()-_+=\|{};,<.>/?

NOTE:

- **Ensure that the settings for the CPE and central office TR-069 management equipment are the same. Otherwise, the CPE cannot be managed by the central office TR-069 management equipment.**
- **The central office TR-069 management equipment will use the SN as the unique identifier for device management.**
- **It is recommended that you change the password after first-time logging in.**

2 Hardware Introduction

About this chapter

This chapter introduces the hardware and cables of the LTE200

2.1 LTE200 Hardware

2.1.1 Appearance

Figure 2-1 shows the appearance of the LTE200

Figure 2-1 The appearance of the CPE



2.1.2 Panel interface

The LTE200 panel includes power port, SIM card slot, WAN/LAN port, phone port, and indicator.

Table 2-1 lists the ports of the LTE200

Table 2-1 LTE200 ports

Item	Description
SIM slot	Micro-SIM
WAN/LAN port	Compatible with RJ45 ethernet cable, and support WAN/LNA transform
Phone port	Compatible with RJ11 Telephoneline
Power port	Connect with power supply

2.1.3 LED indicators

Table 2-2 The status of LED indicators

Indicator	Color	Status	Description	Note
POWER	Green	Black	Power down	1. Normal flash frequency is 5Hz 2. Slowly flash frequency is 1Hz 3. Quickly flash frequency is 10Hz
		Light	Power On	
LTE	Orange	Light	Strong 3G signal	
		Slowly flash	Weak 3G signal	
		Quickly flash	Middle 3G signal	
	Green	Light	Strong 4G signal	
		Slowly flash	Weak 4G signal	
		Quickly flash	Middle 4G signal	
	-	Black	No signal	
INTERNET	Green	Black	No connection	
		Flash	Internet connecting	
LAN	Green	Light	Connected, no communication	
		Flash	Communicating	
		Black	No connection	
PHONE	Green	Light	Registered, no service	
		Flash	Calling	
		Black	unregistered	
Wi-Fi	Green	Light	Wi-Fi on	
		Black	Wi-Fi off	
WPS	Green	Light, black out after 2s	WPS on, matching completed	
		Flash	Negotiating	
		Light, black out after 2mins	WPS on, no negotiating	
		Black	WPS off	
SYS	Green	Light	Starting up	
		Flash	System running	
		Black	System error	

2.1.4 Button

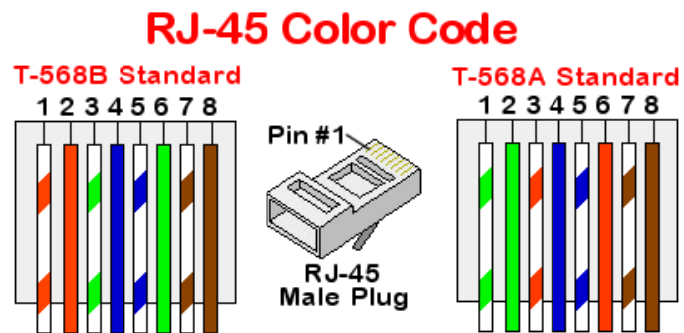
Table 2-3 The status of LED indicators

Button	Detail	Operation
Wi-Fi	Touch switch	press 1 second to enable or disable Wi-Fi
Reset	Touch switch	press 5 seconds to restore the factory default configuration
WPS	Touch switch	press 1 second to enable 2.4GHz Wi-Fi WPS;

2.2 Cables

2.2.1 RJ45 Network cables

The WAN/LAN port of the CPE can be connected through RJ45 cable. For two connection standards: T-568B and T-568A, the WAN/LAN ports support MDI/MDIX auto-sensing.



2.2.2 RJ11 Telephoneline

The Phone port can be connected to the fixed-line telephone through RJ11 cable.

3 InstallationIntroduction

About this chapter

This section introduces how to install the LTE200.

3.1 Installation Preparation

Before installation, please check the total number of items based on the packing list attached to each packing case and check whether each packing case is intact.

3.2 Installation Procedure

Step1. Choosing the working place

LTE200 CPE is mainly used in indoor environment, please choose a suitable working place before installation, and keep it away from high temperature, high pressure and humid environment. The requirements of operating environment are shown in the following table.

Storage temperature	-40°C to 70°C
Working temperature	-10°C to 55°C
Humidity	5% to 95%
Atmospheric pressure	86kPa to 106kPa

Step2. Inserting SIM card

- Open the lid of SIM slot, then insert the 4G/LTE SIM card into the SIM slot.

Step3. Connecting the Power Adapter

- Do not power on the device before installation and cabling are completed.
- The LTE200 series CPE only support the power adapter with them.
- The power input is 12V/1A.

Step4. Connecting Cables

- The Phone port can be connected to the telephone for the voice service, through RJ11 telephone line.
- The internet port can be connected to the computer or ethernet port through RJ45 network cable.

3.3 Installation Check

After you install the LTE200, perform a hardware installation check and a power-on check.
After powering on, check the working status of the CPE depends on the LED indicators.

4 Configuration Introduction

About this chapter

This chapter describes the configuration Introduction of the LTE200

4.1 Log into Web UI

Prerequisites

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

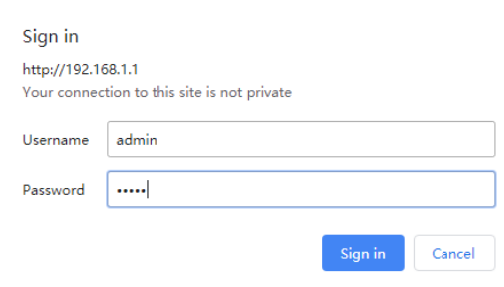
Operating steps

Step1. Start the IE browser, enter https://192.168.1.1 in the address bar, and press Enter.
Connect the CPE from the near end using the Web management page.



Step2. Log into the web management page with default username and password.

Step3. Access Password Modification and modify New Password.

A screenshot of a web browser's sign-in page. The page title is "Sign in" and the URL is "http://192.168.1.1". A warning message states "Your connection to this site is not private". There are two input fields: "Username" with the value "admin" and "Password" with masked characters ".....". At the bottom right, there are two buttons: "Sign in" (blue) and "Cancel" (white).

4.2 QuickConfiguration

4.2.1 LTE quick configuration

Operating steps:

Step1. Enter "Wizard" -> "LTE Connect".

Step2. The initial uplink mode of the CPE is LTE WAN. After inserting SIM card, the device can read the card, and register the network automatically.

Step3. For manual settings, click "User-defined". Then, change the APN, Username, Password, etc. After changing, click "Save&Apply".

Status	Wizard	LAN	Wireless	WAN	Advance	VoIP	Diagnostics	Admin	LTE	SMS																		
<p>Wizard</p> <ul style="list-style-type: none"> > LTE Connect > ETH Connectt > VoIP > Wireless 																												
<p>LTE Connect Settings This page used to config LTE connection</p> <table border="1"> <thead> <tr> <th colspan="2">LTE Connect Settings</th> </tr> </thead> <tbody> <tr> <td>APN Profile</td> <td>User-defined ▼</td> </tr> <tr> <td>APN Self-define</td> <td><input type="text"/></td> </tr> <tr> <td>APN Name</td> <td><input type="text"/></td> </tr> <tr> <td>APN Username</td> <td><input type="text"/></td> </tr> <tr> <td>APN Password</td> <td><input type="text"/></td> </tr> <tr> <td>APN Authentication</td> <td>NONE ▼</td> </tr> <tr> <td>APN Connect Type</td> <td>IPv4IPv6 ▼</td> </tr> <tr> <td>APN MTU</td> <td>1500</td> </tr> </tbody> </table> <p>Add Delete Modify</p>											LTE Connect Settings		APN Profile	User-defined ▼	APN Self-define	<input type="text"/>	APN Name	<input type="text"/>	APN Username	<input type="text"/>	APN Password	<input type="text"/>	APN Authentication	NONE ▼	APN Connect Type	IPv4IPv6 ▼	APN MTU	1500
LTE Connect Settings																												
APN Profile	User-defined ▼																											
APN Self-define	<input type="text"/>																											
APN Name	<input type="text"/>																											
APN Username	<input type="text"/>																											
APN Password	<input type="text"/>																											
APN Authentication	NONE ▼																											
APN Connect Type	IPv4IPv6 ▼																											
APN MTU	1500																											
<p>LTE Data Service Setting</p> <p>LTE Data Service Setting <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled</p> <p>Apply Changes</p>																												

4.2.2 VOIP quick configuration

Operating steps:

Step1. Enter “Wizard” -> “VoIP”.

Step2. Input the parameters of VoIP and click the “Enable” of “Proxy”.

 Note: The Display Name, Number, Login ID, Password, Proxy Addr, Proxy Port are necessary parameters.

Step3. After inputting all parameters, click “Apply”.

Status	Wizard	LAN	Wireless	WAN	Advance	VoIP	Diagnostics	Admin	LTE	SMS																																
<p>Wizard</p> <ul style="list-style-type: none"> > LTE Connect > ETH Connectt > VoIP > Wireless 																																										
<p>Main Proxy</p> <table border="1"> <tbody> <tr> <td>Display Name</td> <td><input type="text"/></td> </tr> <tr> <td>Number</td> <td><input type="text"/></td> </tr> <tr> <td>Login ID</td> <td><input type="text"/></td> </tr> <tr> <td>Password</td> <td><input type="text"/></td> </tr> <tr> <td>Proxy</td> <td><input type="checkbox"/> Enable</td> </tr> <tr> <td>Proxy Addr</td> <td><input type="text"/></td> </tr> <tr> <td>Proxy Port</td> <td>5050</td> </tr> <tr> <td>SIP Subscribe</td> <td><input type="checkbox"/> Enable</td> </tr> <tr> <td>SIP Domain</td> <td><input type="text"/></td> </tr> <tr> <td>Reg Expire (sec)</td> <td>3600</td> </tr> <tr> <td>Outbound Proxy</td> <td><input type="checkbox"/> Enable</td> </tr> <tr> <td>Outbound Proxy Addr</td> <td><input type="text"/></td> </tr> <tr> <td>Outbound Proxy Port</td> <td>5050</td> </tr> <tr> <td>Enable Session timer</td> <td><input checked="" type="checkbox"/> Enable</td> </tr> <tr> <td>Session Expire (sec)</td> <td>1800</td> </tr> <tr> <td>Register Status</td> <td>Disabled</td> </tr> </tbody> </table>											Display Name	<input type="text"/>	Number	<input type="text"/>	Login ID	<input type="text"/>	Password	<input type="text"/>	Proxy	<input type="checkbox"/> Enable	Proxy Addr	<input type="text"/>	Proxy Port	5050	SIP Subscribe	<input type="checkbox"/> Enable	SIP Domain	<input type="text"/>	Reg Expire (sec)	3600	Outbound Proxy	<input type="checkbox"/> Enable	Outbound Proxy Addr	<input type="text"/>	Outbound Proxy Port	5050	Enable Session timer	<input checked="" type="checkbox"/> Enable	Session Expire (sec)	1800	Register Status	Disabled
Display Name	<input type="text"/>																																									
Number	<input type="text"/>																																									
Login ID	<input type="text"/>																																									
Password	<input type="text"/>																																									
Proxy	<input type="checkbox"/> Enable																																									
Proxy Addr	<input type="text"/>																																									
Proxy Port	5050																																									
SIP Subscribe	<input type="checkbox"/> Enable																																									
SIP Domain	<input type="text"/>																																									
Reg Expire (sec)	3600																																									
Outbound Proxy	<input type="checkbox"/> Enable																																									
Outbound Proxy Addr	<input type="text"/>																																									
Outbound Proxy Port	5050																																									
Enable Session timer	<input checked="" type="checkbox"/> Enable																																									
Session Expire (sec)	1800																																									
Register Status	Disabled																																									

4.2.3 WLAN quick configuration


Operating steps:

Step1. Enter “Wizard” -> “Wireless”.

Step2. Change the SSID name by input the new name into the bar.

Step3. Select an encryption mode and input new password. Click “Confirm” to save the settings.

After changing the configuration of WLAN, the Wi-Fi will restart.

 Note: WPA2 Mixed mode is recommended. When the encryption mode is OPEN, user can access to the Wi-Fi without

password.

Status	Wizard	LAN	Wireless	WAN	Advance	VoIP	Diagnostics	Admin	LTE	SMS
<p>Wizard</p> <ul style="list-style-type: none"> > LTE Connect > ETH Connect > VoIP > Wireless 										
<p>WLAN Basic Settings</p> <p>This page is used to configure the parameters for WLAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.</p> <p><input type="checkbox"/> Disable WLAN Interface</p> <p>Band: <input type="text" value="2.4 GHz (B+G+N)"/></p> <p>SSID: <input type="text" value="FA224-588F"/></p> <p>Channel Width: <input type="text" value="20MHz"/></p> <p>Channel Number: <input type="text" value="Auto"/></p> <p>Encryption: <input type="text" value="WPA2 Mixed"/></p> <p>Authentication Mode: <input type="radio"/> Enterprise (RADIUS) <input checked="" type="radio"/> Personal (Pre-Shared Key)</p> <p>WPA Cipher Suite: <input checked="" type="checkbox"/> TKIP <input checked="" type="checkbox"/> AES</p> <p>WPA2 Cipher Suite: <input checked="" type="checkbox"/> TKIP <input checked="" type="checkbox"/> AES</p> <p>Group Key Update Timer: <input type="text" value="86400"/></p> <p>Pre-Shared Key Format: <input type="text" value="Passphrase"/></p> <p>Pre-Shared Key: <input type="text" value="*****"/></p> <p><input type="button" value="Apply Changes"/></p>										

4.3 LTE configuration

4.3.1 LTE Data service settings

Prerequisites:

- Network is ready
- LTE200 power on and start
- CPE register LTE network

Operating steps:

Step1. Enter "LTE" → "LTE Connect":

LTE Data Service Setting	
LTE Data Service Setting	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
<input type="button" value="Apply Changes"/>	

- Data Service Setting:
 - Enable: wireless network can transmit data
 - Disable: wireless network is NOT allowed to transmit data

Step2. Enter "LTE" → "LTE Data Service":

LTE Roaming Service	
LTE Roaming Service Setting	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
<input type="button" value="Apply Changes"/>	

- Roaming Settings:
 - Enable: In the roaming state, wireless network can transmit data (Data Channel must be set as Enable).
 - Disable: In the roaming state, wireless network is NOT allowed to transmit data

4.3.2 LTE APN settings

Prerequisites:

- Network is ready
- LTE200 power on and start
- CPE register LTE network

Operating steps:

Step1. Enter “LTE”→ “LTE Connect”,enter Overview of LTE Connection page. The APN will be configured automatically.

Step2. For manual setting, change the “APN Profile” to “User-defined”. Then, input the APN, APN name, APN Username, APN Password.

- Add: add a manual APN setting.
- Delete: delete the manual setting.
- Modify:click “Modify” button, modify related Settings of APN.
- Apply Changes: apply the setting.

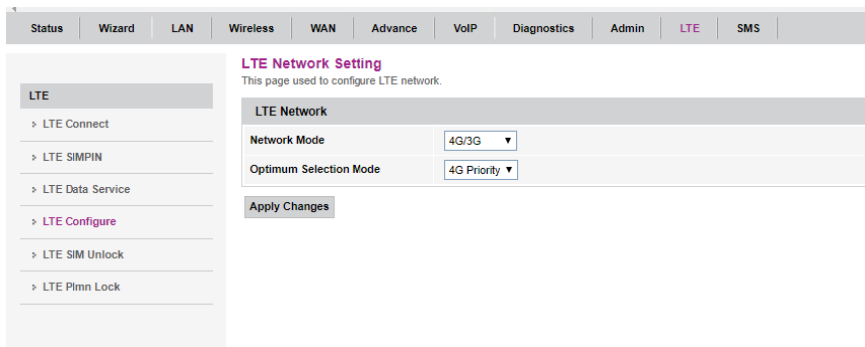
4.3.3 LTE mode settings

Prerequisites:

- Network is ready
- LTE200 power on and start
- CPE register LTE network

Operating steps:

Step1. Enter “LTE”→“LTE Configure”:



- Network Mode:
 - 4G/3G: Indicates that CPE currently supports both 4G and 3G networks
 - 4G: Indicates that CPE only supports 4G network
 - 3G: Indicates that CPE only supports 4G network
- Optimum Selection Mode:
 - 4G prior: Indicates the preferred 4G network
 - 3G prior: Indicates the preferred 3G network

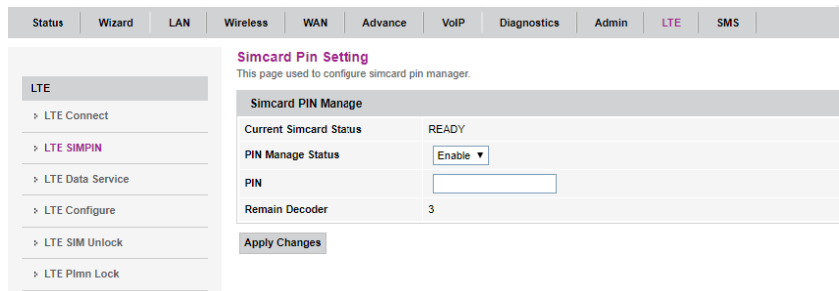
4.3.4 PIN settings

Prerequisites:

- Network is ready
- LTE200 power on and start
- CPE register LTE network

Operating steps:

Step1. Enter“LTE”→“LTE SIMPIN”:



- Current SIM Card state:
 - READY: Indicates a normal SIM card, normally read and write the files of SIM card
 - SIM PIN: Indicates a normal SIM card; And to read or write the SIM card, need to enter a right PIN code
 - SIM PUK: Indicates a normal SIM card; And to read or write the SIM card, need to enter a right PUK code and set a new PIN code
- PIN Code:
 - ON: Indicates that the PIN lock will be opened (the status of PIN lock is turned off)
 - OFF: Indicates that the PIN lock will be turned off (the status of PIN lock is opened)
 - Modify: Indicates that the PIN lock will be turned off (the status of PIN lock is

opened)

- Number of Decode: Indicates the remaining number of times to enter PIN or PUK code

4.4 Ethernet

4.4.1 Ethernet connection

Prerequisite:

- Enter “WAN”→ “WAN Uplink Mode”, the “WAN Uplink Mode” is “ETH”.
- Insert mobile broadband network line into WAN/LAN port.
- Got the username and password for the mobile broadband network.


Operation steps:

Step1. Enter “WAN”-> “WAN” to create a new WAN Connection.

Step2. The following configuration items remain default:


“WAN Conn Deletion”,“Enable”,“Mode”,“Route Bridge Hybrid Mode”,“Enable LAN DHCP”,“Public Multicast VLAN Settings [1-4094]”,“802.1p Priority”,“LAN port Binding” and “SSID port Binding”.

Step3. “Link Method” is set to “Establish Link By PPP”.

 Note: General Broadband Dial-up is set to “Establish Link By PPP”.

If “Link Method” is set to “Establish Link By IP”, you should contact the network administrator.

Step4. “Service Mode” is set to “INTERNET”.


 Note: If the service contains “INTERNET”, it expresses this wan connection support for data service.

If the service contains “VOIP”, it expresses this wan connection support for voice service.

If the service contains “TR069”, it expresses this wan connection support for remote management service.

“OTHER” service mode is generally not recommended.

Step5. “Enable VLAN” is set to “Disable” and “VLAN ID settings” remain empty.

 Note: If “Enable VLAN” is set to “Enable”, you should contact the network administrator and set a VLAN ID.

Step6. “WAN Protocol Version” is set to “IPV4” and “MTU” remain default.

Step7. Enter the username and password of broadband dial-up in “PPPoE Settings”, “Keep alive time” remain empty and “PPPoE Mode” remain default.

Step8. Click “Confirm” button.

Status	Wizard	LAN	Wireless	WAN	Advance	VoIP	Diagnostics	Admin	LTE	SMS
--------	--------	-----	----------	-----	---------	------	-------------	-------	-----	-----

WAN

- > WAN
- > WAN Uplink Mode

WAN
This page is used to configure the parameters for WAN

new link ▾

Enable VLAN:

VLAN ID:

802.1p_Mark:

Channel Mode:

Enable NAPT:

Enable QoS:

Admin Status: Enable Disable

Connection Type:

MTU:

Enable IGMP-Proxy:

Enable MLD-Proxy:::

IP Protocol:

WAN IP Settings:

Type: Fixed IP DHCP

Local IP Address:

Remote IP Address:

Subnet Mask:

IP Unnumbered:

Request DNS: Enable Disable

Primary DNS Server:

Secondary DNS Server:

IPv6 WAN Setting:

Address Mode: Slaac Static

Enable DHCPv6 Client:

Port Mapping:

<input type="checkbox"/> LAN_2	<input type="checkbox"/> LAN_4
<input type="checkbox"/> LAN_3	<input type="checkbox"/> WLAN0-AP2
<input type="checkbox"/> WLAN0	<input type="checkbox"/> WLAN0-AP4
<input type="checkbox"/> WLAN0-AP1	
<input type="checkbox"/> WLAN0-AP3	

4.5 LAN configuration

4.5.1 LAN interface settings

Operation steps:

- Step1.** Enter "LAN"->"LANInterface Settings" page.
- Step2.** Select the IP version and enter the gateway address in "LAN IP address" and enter the mask in "IP Subnet mask".
- Step3.** Click "Apply Changes" button.

Status	Wizard	LAN	Wireless	WAN	Advance	VoIP	Diagnostics	Admin	LTE	SMS
--------	--------	-----	----------	-----	---------	------	-------------	-------	-----	-----

LAN

- > LAN Interface Settings
- > DHCPv4

IPv6

LAN Interface Settings

This page is used to configure the LAN interface of your Device. Here you may change the setting for IP addresses, subnet mask, etc.

InterfaceName:	br0
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
IPv6 Address Mode:	<input checked="" type="radio"/> Auto <input type="radio"/> Manual
IPv6 Address:	::
IPv6 Prefix Length:	0
IP Version:	IPv4/IPv6 ▼

IGMP Snooping:	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
Ethernet to Wireless Blocking:	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
Mac Based Tag Decision:	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled

Apply Changes

4.5.2 DHCP Settings

Operation steps:

- Step1.** Enter "LAN"->"DHCPv4" page.
- Step2.** Select the DHCP Server mode.
- Step3.** Define the "IP range" and the "lease time".
- Step4.** Click "Apply Changes" button.

Status	Wizard	LAN	Wireless	WAN	Advance	VoIP	Diagnostics	Admin	LTE	SMS
--------	--------	-----	----------	-----	---------	------	-------------	-------	-----	-----

LAN

- > LAN Interface Settings
- > DHCPv4

IPv6

DHCP Settings

This page is used to configure DHCP Server and DHCP Relay.

DHCP Mode:	<input type="radio"/> NONE <input type="radio"/> DHCP Relay <input checked="" type="radio"/> DHCP Server
------------	--

Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.

LAN IP Address: 192.168.1.1 Subnet Mask: 255.255.255.0

IP Pool User Config	<input type="checkbox"/>
Associated Clients:	Show Client
Max Lease Time:	86400 seconds (-1 indicates an infinite lease)
DomainName:	bbrouter
Gateway Address:	192.168.1.1
DNS option:	<input checked="" type="radio"/> Use DNS Relay <input type="radio"/> Set Manually

Apply Changes **Port-Based Filter** **MAC-Based Assignment**

4.5.3 IPv6 settings

Operation steps:

- Step1.** Enter "LAN"->"IPv6" page, enable the IPv6.
- Step2.** Enter "LAN"-> "RADVD" page, define the parameters of IPv6 RADVD.

The screenshot shows the 'RADVD Configuration' page. On the left, there is a navigation menu with 'LAN' selected, and sub-items for 'IPv6 Enable/Disable', 'RADVD', and 'DHCPv6'. The main content area contains the following settings:

- MaxRtrAdvInterval: 600
- MinRtrAdvInterval: 198
- AdvManagedFlag: off on
- AdvOtherConfigFlag: off on
- Prefix Mode: Auto
- Enable ULA: off on

An 'Apply Changes' button is located at the bottom of the configuration area.

4.6 WLAN configuration

4.6.1 WLAN Basic

Operating Steps:

- Step1.** Enter “Wireless” -> “Basic Settings”.
- Step2.** Select required SSID in the “SSID list”.
- Step3.** Change the SSID Name, Mode, Channel, Bandwidth, Power.

 Note: SSID name supports 16bits Chinese, English, number, and special symbols.

The screenshot shows the 'WLAN Basic Settings' page for the 'wlan0 (2.4GHz)' interface. The page includes a description: 'This page is used to configure the parameters for WLAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.' The settings are as follows:


- Disable WLAN Interface
- Band: 2.4 GHz (B+G+N)
- Mode: AP
- SSID: FA224-588F
- Channel Width: 40MHz
- Control Sideband: Upper
- Channel Number: Auto
- Radio Power (%): 100%
- Associated Clients:
- Enable Universal Repeater Mode (Acting as AP and client simultaneously)

An 'Apply Changes' button is located at the bottom of the configuration area.

4.6.2 WLAN security

Operating Steps:

- Step1.** Enter “Wireless” -> “Security”.
- Step2.** Select required SSID in the “SSID list”.
- Step3.** Choose an encryption mode (OPEN/WPA/WPA2/WPA-PSK/WPA2-PSK)

 Note: WPA2 Mixed mode is recommended. When the encryption mode is OPEN, user can access to the Wi-Fi without password.

- Step4.** When the encryption mode is WEP, choose the WEP encryption mode to OPEN type or Shared type. Input password and click “confirm”.
- Step5.** When the encryption mode is WPA, WPA2, WPA/WPA2, choose the WPA encryption mode to TKIP, AES, or TUIP/AES. Input password and click “confirm”.

Status	Wizard	LAN	Wireless	WAN	Advance	VoIP	Diagnostics	Admin	LTE	SMS
<p>wlan0 (2.4GHz)</p> <ul style="list-style-type: none"> Basic Settings Advanced Settings Security Access Control WPS 										
<p>WLAN Security Settings</p> <p>This page allows you setup the WLAN security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.</p>										
<p>SSID Type: <input type="text" value="Root AP - FA224-588F"/></p> <p>Encryption: <input type="text" value="WPA2 Mixed"/></p> <p>Authentication Mode: <input type="radio"/> Enterprise (RADIUS) <input checked="" type="radio"/> Personal (Pre-Shared Key)</p> <p>WPA Cipher Suite: <input checked="" type="checkbox"/> TKIP <input checked="" type="checkbox"/> AES</p> <p>WPA2 Cipher Suite: <input checked="" type="checkbox"/> TKIP <input checked="" type="checkbox"/> AES</p> <p>Group Key Update Timer: <input type="text" value="86400"/></p> <p>Pre-Shared Key Format: <input type="text" value="Passphrase"/></p> <p>Pre-Shared Key: <input type="text" value="*****"/></p> <p><input type="button" value="Apply Changes"/></p>										

4.6.3 WPS

Operating Steps:

Step1. Enter "Wireless" -> "WPS" page.

Step2. Choose a WPS mode.

- When the WPS mode is PBC, press the WPS button on the CPE, the SSID can be searched by the user device, and the connection can be built.
- When the WPS mode is Auto/Manual PIN, input the generated PIN code into the user device, the connection can be built.
- When the WPS mode is Peer PIN code, input the user device's generated PIN code into the Web UI, and click "Start PIN", the connection can be built.

Status	Wizard	LAN	Wireless	WAN	Advance	VoIP	Diagnostics	Admin	LTE	SMS
<p>wlan0 (2.4GHz)</p> <ul style="list-style-type: none"> Basic Settings Advanced Settings Security Access Control WPS 										
<p>Wi-Fi Protected Setup</p> <p>This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your WLAN client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.</p>										
<p><input type="checkbox"/> Disable WPS</p> <p>WPS Status: <input type="radio"/> Configured <input checked="" type="radio"/> UnConfigured</p> <p>Auto-lock-down state: <input type="text" value="Unlocked"/> <input type="button" value="Unlock"/></p> <p>Self-PIN Number: <input type="text" value="12345670"/> <input type="button" value="Regenerate PIN"/></p> <p>Push Button Configuration: <input type="button" value="Start PBC"/></p> <p><input type="button" value="Apply Changes"/> <input type="button" value="Reset"/></p> <p>Client PIN Number: <input type="text" value=""/> <input type="button" value="Start PIN"/></p>										

4.7 QoS configuration

4.7.1 QoS Policy

Operating Steps:

Step1. Enter "Advance" -> "IP QoS" -> "QoS Policy" page.

Step2. Enable the "IP QoS", choose the protocol of policy and select the queue.

Step3. Click the "Apply Changes" button to complete the configuration.

Status	Wizard	LAN	Wireless	WAN	Advance	VoIP	Diagnostics	Admin	LTE	SMS																									
<div style="display: flex; justify-content: space-between;"> <div style="width: 20%;"> <p>Service</p> <p>Firewall</p> <p>Advance</p> <p>IP QoS</p> <p>> QoS Policy</p> <p>> QoS Classification</p> <p>> Traffic Shaping</p> </div> <div style="width: 80%;"> <h3>IP QoS Configuration</h3> <p>IP QoS <input type="radio"/> Disable <input checked="" type="radio"/> Enable</p> <h4>QoS Queue Config</h4> <p>This page is used to configure the QoS policy and Queue. If select PRIO of policy, the lower numbers imply greater precedence. If select WRR of policy, please input the weight of this queue. Default is 40:30:20:10. After configuration, please click 'Apply Changes'</p> <p>Policy: <input checked="" type="radio"/> PRIO <input type="radio"/> WRR</p> <table border="1"> <thead> <tr> <th>Queue</th> <th>Policy</th> <th>Priority</th> <th>Weight</th> <th>Enable</th> </tr> </thead> <tbody> <tr> <td>Q1</td> <td>PRIO</td> <td>1</td> <td>--</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Q2</td> <td>PRIO</td> <td>2</td> <td>--</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Q3</td> <td>PRIO</td> <td>3</td> <td>--</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Q4</td> <td>PRIO</td> <td>4</td> <td>--</td> <td><input type="checkbox"/></td> </tr> </tbody> </table> <h4>QoS Bandwidth Config</h4> <p>This part is used to configure the bandwidth of different type of WAN. If select Disable, CPE will select the appropriate bandwidth based on WAN. If select Enable, User is allowed to configure specific bandwidth of WAN.</p> <p>User Defined Bandwidth: <input checked="" type="radio"/> Disable <input type="radio"/> Enable</p> <p>Total Bandwidth Limit: <input type="text" value="100000"/> Kb</p> <p><input type="button" value="Apply Changes"/></p> </div> </div>											Queue	Policy	Priority	Weight	Enable	Q1	PRIO	1	--	<input type="checkbox"/>	Q2	PRIO	2	--	<input type="checkbox"/>	Q3	PRIO	3	--	<input type="checkbox"/>	Q4	PRIO	4	--	<input type="checkbox"/>
Queue	Policy	Priority	Weight	Enable																															
Q1	PRIO	1	--	<input type="checkbox"/>																															
Q2	PRIO	2	--	<input type="checkbox"/>																															
Q3	PRIO	3	--	<input type="checkbox"/>																															
Q4	PRIO	4	--	<input type="checkbox"/>																															

4.7.2 Rate Limit settings

Operating Steps:

- Step1.** Enter "Advance" -> "IP QoS" -> "Traffic Shaping" page.
- Step2.** Click "Add" button to build the new rule.
- Step3.** Input the "Source IP" and "Destination IP". Define the rete limitation in the "Rate Limit" bar by the unit kb/s.
- Step4.** Click the "Apply Changes" button to complete the configuration.

Status	Wizard	LAN	Wireless	WAN	Advance	VoIP	Diagnostics	Admin	LTE	SMS
<div style="display: flex; justify-content: space-between;"> <div style="width: 20%;"> <p>Service</p> <p>Firewall</p> <p>Advance</p> <p>IP QoS</p> <p>> GoS Policy</p> <p>> GoS Classification</p> <p>> Traffic Shaping</p> </div> <div style="width: 80%;"> <h3>Add IP QoS Traffic Shaping Rule</h3> <p>IP Version: <input type="text" value="IPv4"/></p> <p>Direction: <input type="text" value="Upstream"/></p> <p>Protocol: <input type="text" value="NONE"/></p> <p>Source IP: <input type="text"/></p> <p>Source Mask: <input type="text"/></p> <p>Destination IP: <input type="text"/></p> <p>Destination Mask: <input type="text"/></p> <p>Source Port: <input type="text"/></p> <p>Destination Port: <input type="text"/></p> <p>Rate Limit: <input type="text"/> kb/s</p> <p><input type="button" value="Close"/> <input type="button" value="Apply Changes"/></p> </div> </div>										

4.8 Route configuration

4.8.1 Static Routing

Operating Steps:


- Step1.** Enter "Advance" -> "Advance" -> "Routing".
- Step2.** Click the "Show Routes" button to display the static route.
- Step3.** Enter the destination IP or network to be reached in the "Destination IP Address" text

field.

- Step4.** Enter the subnet mask in "Destination Subnet Mask" text field.
- Step5.** Click the "IPv4 Interface" check box and select the interface in the corresponding list.
- Step6.** Click the "Gateway Address" check box and enter the corresponding gateway address in text field.
- Step7.** Click the "OK" button to complete the static route configuration.
- Step8.** If you want to delete the added static route, select the "Delete" radio button in the static route list and click the "Delete" button.

4.9 WAN settings

Choose the WAN mode in the "WAN Uplink Mode" interface.

 Note: When the Uplink mode is LTE, the WAN/LAN port is work as LAN port. When the Uplink mode is ETH, the WAN/LAN port is work as WAN port.

4.10 DDNS settings

Operating Steps:

- Step1.** Enter "Advance" -> "Dynamic DNS".
- Step2.** Select the "Enable" checkbox.
- Step3.** In the "Service Provider" list, select the DDNS service provider you want to use. The available service providers are DynDNS.org, ORAY, and GUNDIP.
- Step4.** Enter the domain name in the "Domain Name" text field.
- Step5.** Select the WAN connection you want to use in the "Interfaces" list.
- Step6.** Enter the username and password registered in the DDNS service provider in the "Username" and "Password" text field.
- Step7.** Click the "Add" button and the DDNS configuration is complete.

Step8. If you want to delete the DDNS configuration, select the “Remove” checkbox in the DDNS configuration list, and click the “Remove” button.

Dynamic DNS Configuration
This page is used to configure the Dynamic DNS address from DynDNS.org or TZO or No-IP. Here you can Add/Remove to configure Dynamic DNS.

Enable:

DDNS Provider:

Hostname:

Interface:

DynDns Settings

UserName:

Password:

TZO Settings

Email:

Key:

Dynamic DNS Table

Select	State	Hostname	UserName	Service	Status
--------	-------	----------	----------	---------	--------

4.11 Firewall settings

4.11.1 DMZ

Operating Steps:

- Step1.** Enter “Advance”-> “Firewall”-> “DOS” page.
- Step2.** Enable the “DMZ Host” and input the “DMZ Host IP Address”.
- Step3.** Click “Apply Change” to save the setting.

DMZ Configuration
A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

DMZ Host: Disable Enable

DMZ Host IP Address:

4.11.2 Attack Protection Settings

Operating Steps:

- Step1.** Enter “Advance”-> “Firewall”-> “DOS”.
- Step2.** “DOS Block”, “Flood”, “Spoof” and “Scan”, etc can be selected or not.
- Step3.** Click “Apply Change” to save the settings.

DoS Configuration
DoS (Denial-of-Service) attack which is launched by hacker aims to prevent legal user from taking normal services. In this page you can configure to prevent some kinds of DOS attack.

- Enable DoS Block
- Whole System Flood: SYN 100 packets/second
- Whole System Flood: FIN 100 packets/second
- Whole System Flood: UDP 100 packets/second
- Whole System Flood: ICMP 100 packets/second
- Per-Source IP Flood: SYN 100 packets/second
- Per-Source IP Flood: FIN 100 packets/second
- Per-Source IP Flood: UDP 100 packets/second
- Per-Source IP Flood: ICMP 100 packets/second
- TCP/UDP PortScan Low Sensitivity
- ICMP Smurf
- IP Land
- IP Spoof
- IP TearDrop
- PingOfDeath
- TCP Scan
- TCP SynWithData
- UDP Bomb
- UDP EchoChargen

Select All Clear

Enable Source IP Blocking 300 Block Interval (seconds)

Apply Changes

4.12 MAC filter

Operating Steps:

- Step1.** Enter “Advance” -> “MAC Filtering” page.
- Step2.** Click the button to “enable MAC filter” and select an “Filter rules”. When the rule is Blacklist, all added MAC address cannot access to network. When the rule is white list, only added MAC address can access to network.
- Step3.** Input MAC address into the bar and click “add” to add the address to the list.
- Step4.** Click “Delete” to remove the settings.

Note: Support 16 filtering addresses. Switching rule will causes all current added address to be cleared.

MAC Filtering
Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Mode: WhiteList BlackList

MAC Address:

Select	MAC Address

4.13IP/Port filter

4.13.1 IP/Port Filtering

Operating Steps:

Step1. Enter “Advance”-> “IP/Port Filtering” page.

Step2. Input source/destination start/end IP address and choose schedule rule which is defined in “Firewall Opening Time”, then choose the protocol which you want to filter. If protocol is selected, source/destination start/end port should be configured, then click “Add” to add this rule.

Step3. Click “Delete” to remove the settings.

The screenshot shows the 'IP/Port Filtering' configuration page. The navigation menu on the left includes: Service, Firewall, IP/Port Filtering (selected), MAC Filtering, Port Forwarding, URL Blocking, Domain Blocking, DMZ, IPv6 IP/Port Filtering, IPv6 ACL, IPv4 ACL, and DOS. The main content area has a title 'IP/Port Filtering' and a description: 'Entries in this table are used to restrict certain types of data packets through the Gateway. Use of such filters can be helpful in securing or restricting your local network.' Below the title are fields for 'Default Action' (radio buttons for Deny and Allow), 'Protocol' (dropdown menu showing TCP), 'Rule Action' (radio buttons for Deny and Allow), 'Source IP Address', 'Subnet Mask', 'Port', and 'Destination IP Address'. There is an 'Add' button and a 'Current Filter Table' section with a table header and 'Delete Selected' and 'Delete All' buttons.

4.14 VoIP settings

4.14.1 Basic settings

Operating Steps:

Step1. Enter “VoIP”-> “Port1” page.

Step2. a. Input primary/standby sip agent which include “SIP register local domain name”, sip registration server, sip proxy and sip external agent. And port need to be changed for each server if necessary.

b. Enable/disable the SIP account and input sip number, username and password.

c. Configure the coding packing time for each coding type.

d. Choose the coding sequence depend on your network and please note that one coding type can be chosen once or you cannot save the configuration.

Step3. Click “Apply” to save the settings or “Reset” to drop the settings.

Status	Wizard	LAN	Wireless	WAN	Advance	VoIP	Diagnostics	Admin	LTE	SMS
VoIP										
<ul style="list-style-type: none"> > Port1 > Advance > Other > Network > Call History 										
Default Proxy										
Select Default Proxy Proxy0 ▼										
Proxy0										
Display Name <input type="text"/>										
Number <input type="text"/>										
Login ID <input type="text"/>										
Password <input type="text"/>										
Proxy <input type="checkbox"/> Enable										
Proxy Addr <input type="text"/>										
Proxy Port <input type="text" value="5090"/>										
SIP Subscribe <input type="checkbox"/> Enable										
SIP Domain <input type="text"/>										
Reg Expire (sec) <input type="text" value="3600"/>										
Outbound Proxy <input type="checkbox"/> Enable										
Outbound Proxy Addr <input type="text"/>										
Outbound Proxy Port <input type="text" value="5090"/>										
Enable Session timer <input checked="" type="checkbox"/> Enable										
Session Expire (sec) <input type="text" value="1800"/>										
Register Status Disabled										

4.14.2 Advanced settings

Operating Steps:

Step1. Enter “VOIP”-> “Advance” page.

- Step2.**
- a. Enable call waiting or not.
 - b. Configure hot line dial.
 - c. Enable FAX or not.
 - d. Define sip registration timeout and session timeout.
 - e. Choose DTMF method from down list which include “Inband” “SIP INFO” and “RFC2833”.
 - f. Choose caller display mode from “FSK” and “DTMF”.
 - g. Choose the sip transport protocol from “TCP” and “UDP”.

Step3. Step 4 Click “Apply” to save the settings.

5 Maintenance Introduction

About this chapter

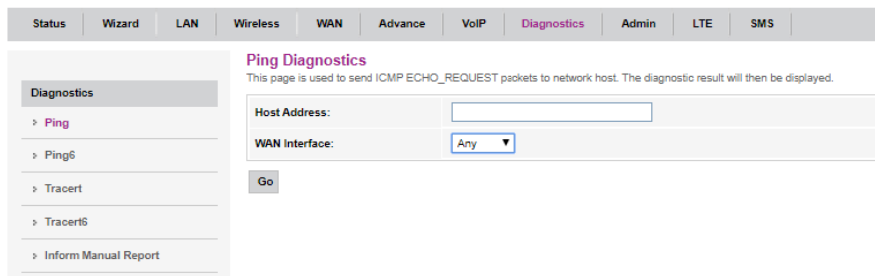
This chapter introduces the maintenance preparation and fault diagnosis methods for the CPE.

5.1 Diagnosis

5.1.1 Ping testing

Operating Steps:

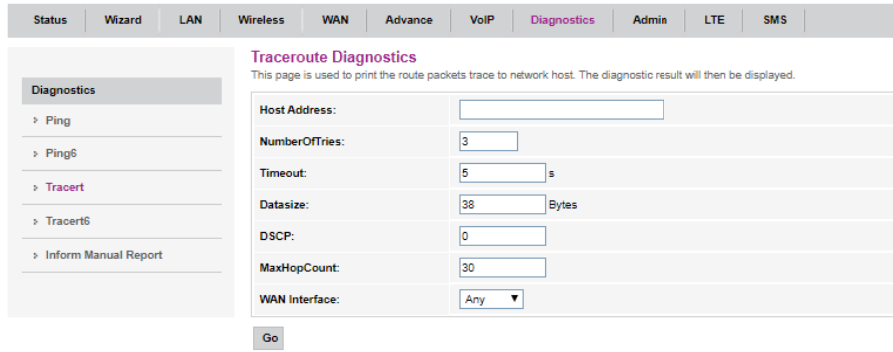
- Step1.** Enter "Diagnostics"-> "Ping" page.
- Step2.** a. Choose one connection WAN from the WAN list which you want to test.
b. Input the IP address or domain name you want to ping.
- Step3.** Click "Go" to start test and the result will be return after test is finished.



5.1.2 Tracert testing

Operating Steps:

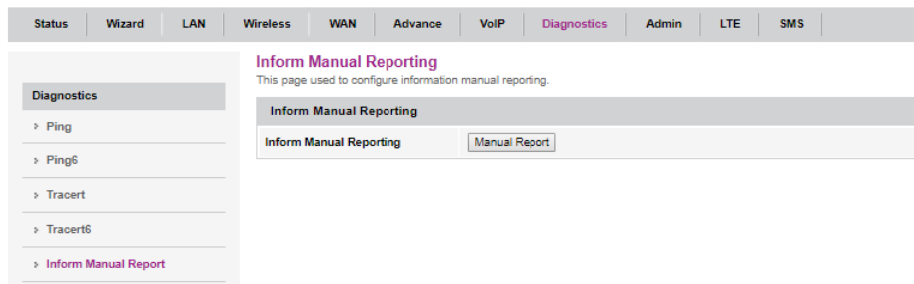
- Step1.** Enter "Diagnostics"-> "Tracert".
- Step2.** a. Choose one connection WAN from the WAN list which you want to test.
b. Input the destination address.
- Step3.** Click "Go" to start test and the result will be return after test is finished.



5.1.3 Inform Manual reporting

Operating Steps:

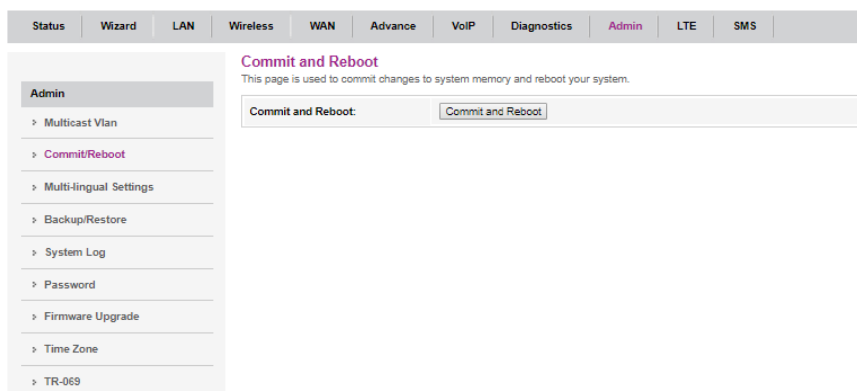
- Step1.** Enter “Diagnostics”->“Inform Manual report”.
- Step2.** Click “Manual report” to start test and the result will be return after test is finished.



5.2 Device management

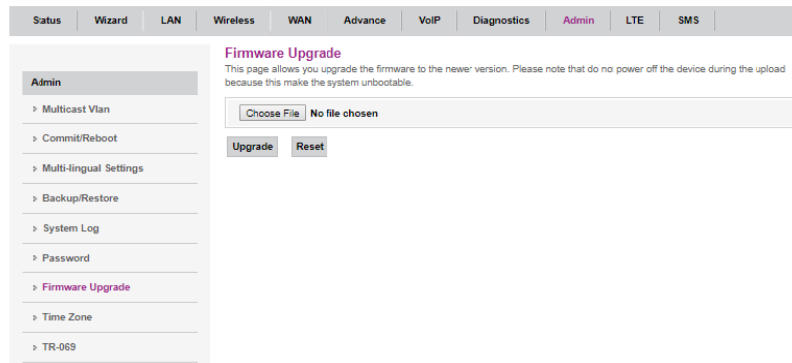
5.2.1 Device Restart

Enter “Admin”-> “Commit/Reboot”,Click the “Commit and Reboot” button.



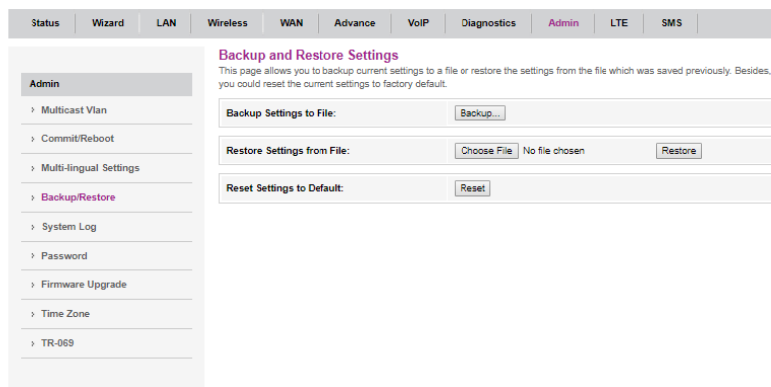
5.2.2 Software Upgrade

Enter “Admin”-> “Firmware Upgrade”, Choose the update file and click the “upgrade” button.



5.2.3 Restore Factory Settings

Enter “Admin”-> “Backup/Restore”, Click the “Reset” button.



5.3 User management

5.3.1 Change Password

Operating Steps:

- Step1.** Enter “Admin”->“Password”.
- Step2.** Input Old Password, New Password, Confirm New Password.
- Step3.** Click “Apply” to change the password.

Note: the default username/password of admin is admin/admin. the defaultusername/password of user is user/user.

5.4 Time management

5.4.1 Time server

Operating Steps:

- Step1.** Enter “Admin”-> “Time Zone”.
- Step2.** a. By select manual settings, YYYY/MM/DD and HH/MM/SS can be set.
b. By select sync from server, the server can to choose from down list or defined by user.
- Step3.** Click “Apply Changes” or “Refresh” to save change, or update settings.

5.5 TR069 Remote management

TR-069 is a communication specification between the terminal device and the ACS (Automatic Configuration Server). If the operator enables the TR-069 automatic service provisioning function, the parameter configuration in the LTE CPE will be automatically issued by the ACS. If the ACS parameters are configured on the LTE CPE and the corresponding settings are made on the ACS, the TR-069 function can automatically configure the network parameters without configuring any other parameters on the LTE CPE.

Precondition:

- The network side has been deployed.
- The LTE200 device has been installed.
- The device starts normally after it is powered on.
- TR069 WAN connection has been successfully created


Operating Steps:

Step1. Enter "Admin" -> "TR-069".

Step2. If you want to enable TR-069 to periodically send messages, set "TR069 Daemon" to Enabled.

Step3. Enter the "ACS URL" to connect to the ACS.

Step4. Enter the ACS username and password for authenticating the LTE CPE identity in the ACS Username and ACS Password text boxes.

 When the LTE CPE accesses the ACS, the username and password are required to authenticate to the ACS. The username and password should be consistent with the settings on the ACS.

Step5. Click "Apply" to complete the setup.

TR-069 Configuration
This page is used to configure the TR-069 CPE. Here you may change the setting for the ACS's parameters.

TR069 Daemon: Enabled Disabled
 EnableCWMPParameter: Enabled Disabled

ACS

URL:
 UserName:
 Password:
 Periodic Inform: Disabled Enabled
 Periodic Inform Interval:

Connection Request

UserName:
 Password:
 Path:
 Port:

STUN Setting

STUN: Disabled Enabled
 STUN Server Address:
 STUN Server Port:
 STUN Server User:
 STUN Server Password:

6FAQ

Q1. The login window interface does not display.

- A. The IP address of your computer may be a fixed IP address, please change it to 「obtain an IP address automatically」.
- B. Please change a Web browser and try again.
- C. Please check the cable connection, and the status of LED indicator; Restart your computer and CPE and try again.

Q2. How to reset the CPE.

- A. Power on the CPE, and long press the Reset button on the back of the device for 8 seconds. Please note that the set value will be cleared.
- B. Log in the Web management interface and choose the reset button on the web.

Q3. I forget the password of Web management interface.

- A. Please reset your CPE, the initial username is **admin**, and password is **admin**.

Q4. I forget the password of Wi-Fi.

- A. If you have not changed the password of your CPE before, the initial password is: **12345678**.
- B. If you have changed the password before, please connect the CPE through wired network, and log into the Web management interface, the password can be changed in the WLAN setting interface.

7 Privacy and Security

7.1 Privacy Protection

- To better understand how we protect your personal information, please see the privacy policy at official web.
- 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.

7.2 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.

7.3 Default Security Configuration

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

- Change the Web UI login password, keep it secure, and regularly change it subsequently.
- Verify that the TR-069 port password meets complexity requirements.
- Set the firewall level to low and enable the anti-DoS attack function.
- Configure the service list control function based on product application scenarios. If HTTP and ICMP access requests on the WAN side do not exist, disable WAN access.

8 Acronyms and Abbreviations

Table 8-1 Acronyms and abbreviations List

Abbreviations	Full name
3GPP	3rd Generation Partnership Project
ALG	Application Layer Gateway
CPE	Customer Premises Equipment
DDNS	Dynamic Domain Name Server
DHCP	Dynamic Host Configuration Protocol
GRE	Generic Routing Encapsulation
LAN	Local Area Network
LTE	Long Term Evolution
MAC	Media Access Control
NAT	Network Address Translation
PoE	Power over Ethernet
QoS	Quality of service
SIM	Subscriber Identity Module
SMS	Short Message Service
TR069	Technical Report 069
URL	Uniform Resource Location
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
WLAN	Wireless Local Area Network

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

Note: 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 equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment .

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

This equipment should be installed and operated with minimum distance 20cm between the radiator &you body.