

**LTE CPE B2368
V100R001C00**

User Guide

Issue 03
Date 2019-01-31



Copyright © Huawei Technologies Co., Ltd. 2019. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI 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

Purpose

The Device is an LTE (Long Term Evolution) device. ODU refers to the outdoor unit and IDU refers to the indoor unit. The LTE Device also provides a complete security solution with a robust firewall based on Stateful Packet Inspection (SPI) technology and Denial of Service (DoS).

Change History

Changes between document issues are cumulative. The latest document issue contains all the changes made in earlier issues.

Issue	Date	Description
03	2019-01-31	Updated descriptions in 15.2 The SIP Service Provider Screen .
02	2018-03-31	Add 30 Personal Data Description .
01	2018-03-22	This issue is the first release.

Contents

About This Document.....	ii
1 Introduction.....	1
1.1 Applications for the LTE Device.....	1
1.1.1 Internet Access.....	1
1.1.2 VoIP Features.....	1
1.1.3 Wireless Connection.....	2
1.2 The WLAN Button.....	2
1.3 Ways to Manage the LTE Device.....	3
1.4 Good Habits for Managing the LTE Device.....	3
1.5 Hardware.....	3
1.5.1 ODU.....	4
1.5.2 IDU.....	5
1.5.3 The RESET Button.....	7
2 Introducing the Web Configurator.....	9
2.1 Overview.....	9
2.1.1 Basic Setting Information.....	9
2.1.2 Accessing the Web Configurator.....	12
2.2 The Web Configurator Layout.....	16
2.2.1 Title Bar.....	17
2.2.2 Main Window.....	17
2.2.3 User Account.....	17
2.2.4 Navigation Panel.....	18
3 Connection Status and System Info.....	19
3.1 Overview.....	19
3.2 The Connection Status Screen.....	19
3.3 The System Info Screen.....	20
4 Broadband.....	28
4.1 Overview.....	28
4.2 Broadband Screen.....	28
4.2.1 Edit Broadband Connection.....	29
4.3 SIM Screen.....	31
4.3.1 SIM Locked Screen.....	32

4.4 LTE Setting Screen.....	33
5 Wireless.....	36
5.1 Overview.....	36
5.1.1 Wireless Network Overview.....	36
5.1.2 Before You Begin.....	38
5.2 The Wireless General Screen.....	38
5.2.1 More Secure (WPA(2)-PSK).....	43
5.3 The More AP Screen.....	44
5.3.1 Edit More AP.....	45
5.4 The WPS Screen.....	47
5.5 Technical Reference.....	49
5.5.1 Wireless Security Overview.....	49
5.5.2 Signal Problems.....	51
5.5.3 BSS.....	51
5.5.4 MBSSID.....	52
5.5.5 WiFi Protected Setup (WPS).....	52
5.5.5.1 Push Button Configuration.....	53
5.5.5.2 PIN Configuration.....	53
5.5.5.3 How WPS Works.....	54
5.5.5.4 Limitations of WPS.....	55
6 Home Networking.....	57
6.1 Overview.....	57
6.1.1 What You Need To Know.....	57
6.1.1.1 About LAN IP Address.....	57
6.1.1.2 About UPnP.....	58
6.2 The LAN Setup Screen.....	58
6.3 The Static DHCP Screen.....	61
6.3.1 Before You Begin.....	61
6.4 The UPnP Screen.....	63
6.5 The UPnP List Screen.....	63
7 Static Route.....	65
7.1 Overview.....	65
7.2 Configuring Static Route.....	66
7.2.1 Add/Edit Static Route.....	67
8 Network Address Translation (NAT).....	69
8.1 Overview.....	69
8.1.1 What You Need To Know.....	69
8.2 The Port Forwarding Screen.....	70
8.2.1 The Port Forwarding Screen.....	70
8.2.2 The Port Forwarding Edit Screen.....	72
8.3 The DMZ Screen.....	73

8.4 The Sessions Screen.....	74
8.5 The ALG Screen.....	74
8.6 Technical Reference.....	75
8.6.1 NAT Definitions.....	75
8.6.2 What NAT Does.....	75
8.6.3 How NAT Works.....	76
9 Dynamic DNS.....	77
9.1 Overview.....	77
9.1.1 What You Need To Know.....	77
9.2 The Dynamic DNS Screen.....	77
10 Firewall.....	78
10.1 Overview.....	78
10.1.1 What You Need to Know.....	79
10.2 The General Screen.....	79
10.3 The Services Screen.....	80
10.3.1 The Add New Services Entry Screen.....	81
10.4 The Access Control Screen.....	82
10.4.1 The Add New ACL Rule/Edit Screen.....	84
10.5 The DoS Screen.....	85
10.6 Firewall Technical Reference.....	86
10.6.1 Guidelines For Enhancing Security With Your Firewall.....	86
10.6.2 Security Considerations.....	87
11 MAC Filter.....	88
11.1 Overview.....	88
11.1.1 What You Need to Know.....	88
11.2 The MAC Filter Screen.....	88
12 Parental Control.....	91
12.1 Overview.....	91
12.2 The Parental Control Screen.....	91
12.2.1 Add/Edit a Parental Control Rule.....	92
13 L2TP VPN.....	95
13.1 Overview.....	95
13.2 The Setup Screen.....	95
13.2.1 The Add/Edit L2TP Tunnel Screen.....	96
13.3 The Monitor Screen.....	98
13.4 A Layer 3 L2TP VPN Configuration Example.....	99
13.5 A Layer 2 L2TP VPN Configuration Example.....	100
14 GRE VPN.....	102
14.1 Overview.....	102
14.2 The Setup Screen.....	102

14.2.1 The Add/Edit GRE Tunnel Screen.....	103
14.3 A Layer 2 GRE VPN Configuration Example.....	105
14.4 A Layer 3 GRE VPN Configuration Example.....	106
15 VoIP.....	108
15.1 Overview.....	108
15.1.1 What You Need to Know.....	109
15.1.2 Before You Begin.....	110
15.2 The SIP Service Provider Screen.....	110
15.3 The SIP Account Screen.....	118
15.3.1 Edit SIP Account.....	118
15.4 The Phone Region Screen.....	122
15.5 The Call Rule Screen.....	123
15.6 Technical Reference.....	124
15.6.1 VoIP.....	124
15.6.2 SIP.....	125
15.6.3 Quality of Service (QoS).....	130
15.6.4 Phone Services Overview.....	130
16 LTE Status.....	134
16.1 Overview.....	134
17 Logs.....	135
17.1 Overview.....	135
17.1.1 What You Need To Know.....	135
17.2 The System Log Screen.....	136
17.3 The Phone Log Screen.....	137
17.4 The VoIP Call History Screen.....	138
18 Traffic Status.....	139
18.1 Overview.....	139
18.2 The WAN Status Screen.....	139
18.3 The LAN Status Screen.....	140
18.4 The NAT Status Screen.....	142
18.5 The VoIP Status Screen.....	142
19 User Account.....	145
19.1 Overview.....	145
19.2 The User Account Screen.....	145
20 Remote MGMT.....	147
20.1 Overview.....	147
20.1.1 What You Need to Know.....	147
20.2 The Remote MGMT Screen.....	147
20.3 The TR069 Screen.....	148
21 System.....	150

21.1 Overview.....	150
21.1.1 What You Need to Know.....	150
21.2 The System Screen.....	150
21.3 The Encryption Key Screen.....	151
21.3.1 Normal: IDU and ODU Bundle.....	151
21.3.2 New ODU with Old IDU.....	152
21.3.3 New IDU with Old ODU.....	153
22 Time Setting.....	154
22.1 Overview.....	154
22.2 The Time Setting Screen.....	154
23 Log Setting.....	157
23.1 Overview.....	157
23.2 The Log Setting Screen.....	157
24 Software Upgrade.....	159
24.1 Overview.....	159
24.2 The Software Upgrade Screen.....	159
25 Online Upgrade.....	162
25.1 Overview.....	162
25.2 The Online Upgrade Screen.....	162
25.3 Online Upgrade Types.....	164
25.4 Online Upgrade Procedures.....	165
26 Backup/Restore.....	172
26.1 Overview.....	172
26.2 The Backup/Restore Screen.....	172
27 The Reboot Screen.....	175
28 Diagnostic.....	176
28.1 Overview.....	176
28.2 The Ping/TraceRoute Screen.....	176
29 Troubleshooting.....	178
29.1 Overview.....	178
29.2 Power, Hardware Connections, and LEDs.....	178
29.3 LTE Device Access and Login.....	178
29.4 Internet Access.....	180
29.5 Wireless Internet Access.....	180
29.6 Phone Calls and VoIP.....	181
29.7 UPnP.....	182
30 Personal Data Description.....	183

1 Introduction

1.1 Applications for the LTE Device

Here are some examples for which the LTE Device is well suited.

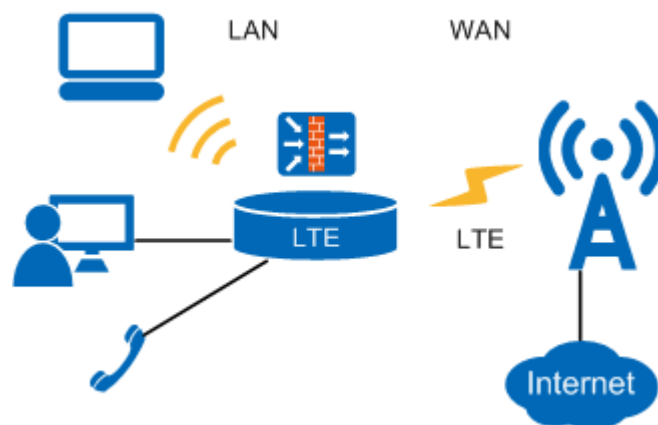
1.1.1 Internet Access

Your LTE Device provides Internet access by connecting to an LTE network wirelessly. Your LTE Device supports the following LTE frequency bands although the band it actually uses depends on your LTE service provider.

- B2368-22 and B2368-66 support LTE bands B38/B40/B41/B42/B43/B1/B3/B7/B8/B20.
- B2368-57 supports LTE bands B40/B41/B42/B4/B7/B28.

See [Figure 1-1](#), computers can connect to the LTE Device's **ETHERNET** ports (or wirelessly).

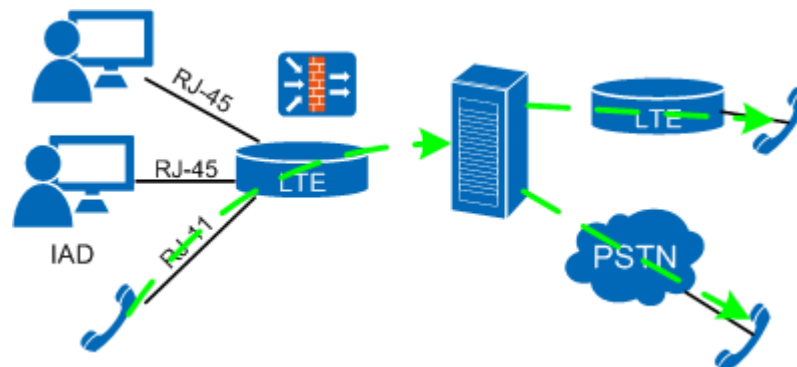
Figure 1-1 LTE Device's Internet Access Application



1.1.2 VoIP Features

You can register one SIP (Session Initiation Protocol) profile with one account for that profile and use the LTE Device to make and receive VoIP telephone calls:

Figure 1-2 LTE Device's VoIP Application

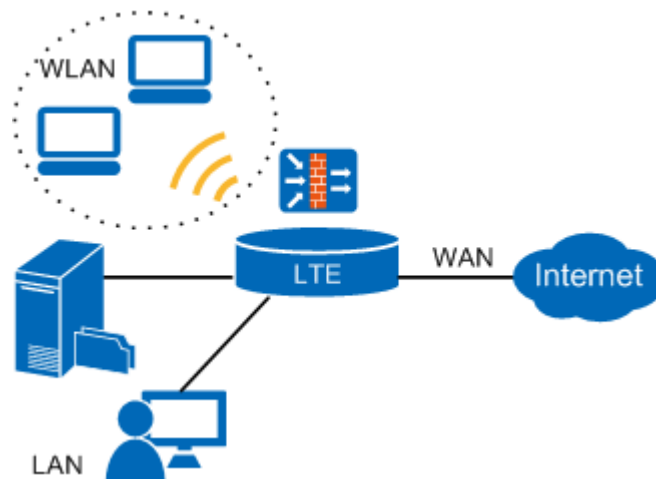


The LTE Device sends your call to a VoIP service provider's SIP server which forwards your calls to either VoIP or PSTN phones. Enable the LTE Device's SIP ALG feature to support SIP phones and IAD devices on the LAN.

1.1.3 Wireless Connection

By default, the wireless LAN (WLAN) is enabled on the LTE Device. Once Wireless is enabled, IEEE 802.11b/g/n/ac compliant clients can wirelessly connect to the LTE Device to access network resources. You can set up a wireless network with WPS (WiFi Protected Setup) or manually add a client to your wireless network.

Figure 1-3 Wireless Connection Application



1.2 The WLAN Button

You can use the **WIRELESS On/Off** button on top of the device to turn the 2.4 GHz and 5 GHz wireless LAN on or off. You can also use it to activate WPS in order to quickly set up a wireless network with strong security.

Turn the Wireless LAN On or Off

Step 1 Make sure the **PWR/SYS** LED is on (not blinking).

- Step 2** Press the **WIRELESS On/Off** button for one second and release it. The **WLAN/WPS** LED should change from on to off or vice versa.

----End

Activate WPS

- Step 1** Make sure the **PWR/SYS** LED is on (not blinking).
- Step 2** Press the **WIRELESS On/Off** button for more than five seconds and release it. Press the **WPS** button on another WPS-enabled device within range of the LTE Device. The **WLAN/WPS** LED should flash while the LTE Device sets up a WPS connection with the wireless device.

----End



You must activate WPS in the LTE Device and in another wireless device within two minutes of each other. See [5.4 The WPS Screen](#) for more information.

1.3 Ways to Manage the LTE Device

Web Configurator is for management of the LTE Device using a (supported) web browser.

1.4 Good Habits for Managing the LTE Device

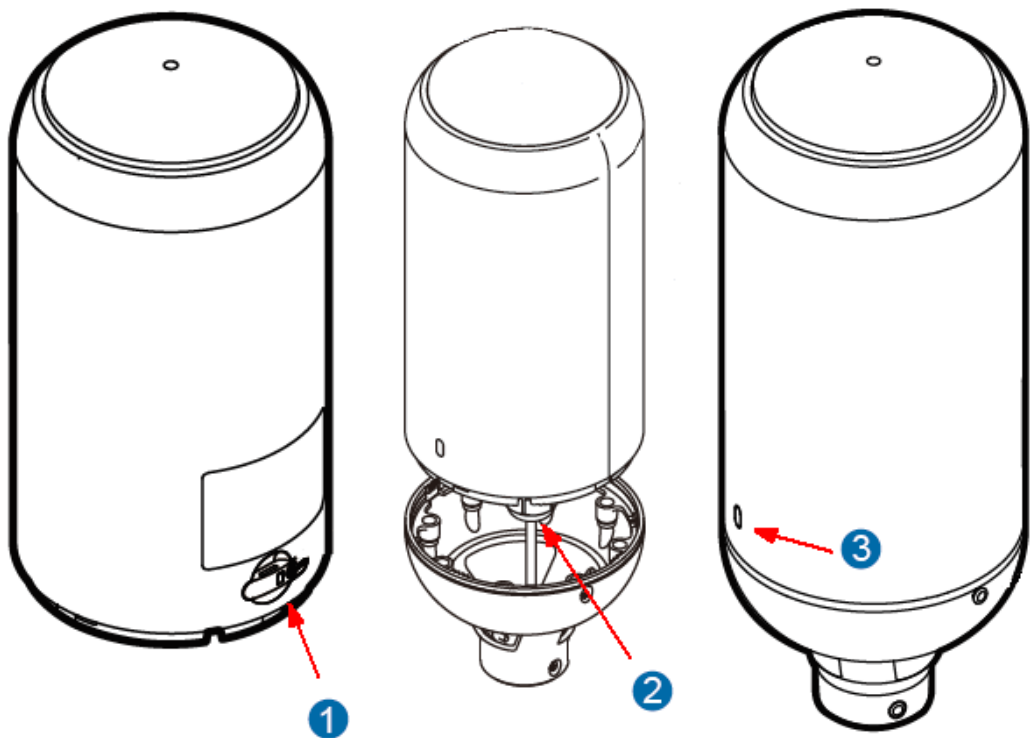
Do the following things regularly to make the LTE Device more secure and to manage the LTE Device more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password to access the Web Configurator, you will have to reset the LTE Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the LTE Device. You could simply restore your last configuration. Keep in mind that backing up a configuration file will not back up passwords used to set up your VoIP account. Write down any information your ISP provides you.

1.5 Hardware

1.5.1 ODU

Figure 1-4 ODU



1. One slot for one SIM card (Only 3FF Micro-SIM is supported).
2. One RJ-45 connector for connecting to the IDU PoE port.
3. LED indicator inside.

Table 1-1 ODU LED Indicators

Color	LED Behavior	Status Indication
Off		Power Off
Red	Steady ON	Error, malfunction, or no SIM
	Blinking	Upgrading
Green	Blinking	Booting up
	Steady ON	Strong LTE signal: SINR $\geq$ 10 dB
Blue	Steady ON	Medium LTE signal: 10 dB > SINR $\geq$ 4 dB
Orange	Steady ON	Weak LTE signal: SINR < 4 dB
	Blinking	No LTE signal, searching, or disconnected.

1.5.2 IDU

The following graphic displays the Labels of the LEDs.

Figure 1-5 IDU Front Panel

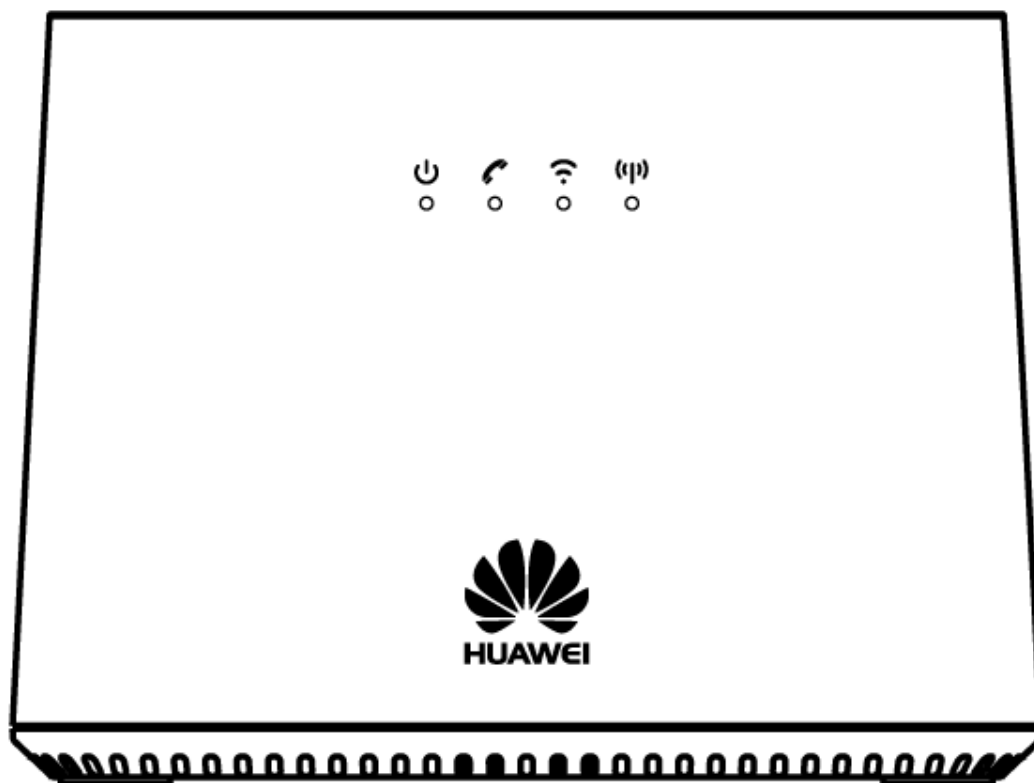
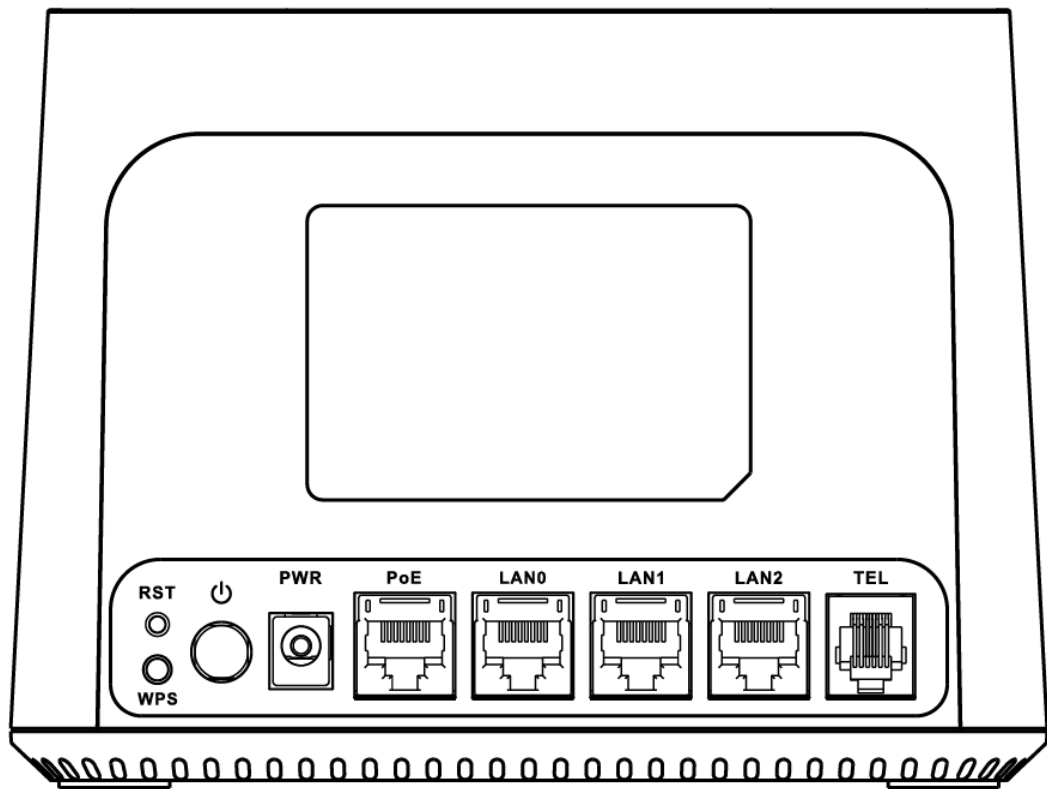


Figure 1-6 IDU Rear Panel



 **NOTE**

None of the LEDs are on if the LTE Device is not receiving power.

Table 1-2 IDU LED Descriptions (From Left To Right)

LED	COLOR	STATUS	Description
	Green	On	The LTE Device is receiving power and ready for use.
		Blinking	The LTE Device is booting up.
	Red	On	The LTE Device detected an error while self-testing, or there is a device malfunction or no SIM card.
		Blinking	The LTE Device is upgrading the firmware.
	Off		The LTE Device is not receiving power.
	Green	On	A SIP account is registered for the phone port.
		Blinking	A telephone connected to the phone port has its receiver off of the hook or there is an incoming call.
	Yellow	On	A SIP account is registered for the phone port and there is a voice message in the corresponding SIP account.

LED	COLOR	STATUS	Description
		Blinking	A telephone connected to the phone port has its receiver off of the hook and there is a voice message in the corresponding SIP account.
	Off		The phone port does not have a SIP account registered.
WPS /Wi-Fi 	Green	On	Either IEEE 802.11bgn or 802.11ac is activated.
		Blinking	The LTE Device is communicating with wireless clients.
	Yellow	Blinking	The LTE Device is setting up a WPS connection.
	Off		The wireless network is not activated.
LTE Signal Strength 	Green	On	Strong LTE signal: SINR ≥ 10 dB
	Blue	On	Medium LTE signal: $10 \text{ dB} > \text{SINR} \geq 4 \text{ dB}$
	Orange	On	Weak LTE signal: SINR $< 4 \text{ dB}$
		Blinking	No LTE signal, searching, or disconnected.
LAN 0-2 	Yellow (Giga Ethernet)	On	The LTE Device has a successful 1000 Mbps Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The LTE Device is sending or receiving data to/from the LAN at 1000 Mbps.
	Green (Fast Ethernet)	On	The LTE Device has a successful 10/100 Mbps Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The LTE Device is sending or receiving data to/from the LAN at 10/100 Mbps.
	Off		The LTE Device does not have an Ethernet connection with the LAN.

Refer to the *Quick Start Guide* for information on hardware connections.

1.5.3 The RESET Button

To reboot the device, just press down the **RESET BUTTON** and hold for 3-10 seconds, and then release the button.

To restore the device to the factory default configuration, make sure the **POWER LED** is on (not blinking) and press the **RESET BUTTON** for over 10 seconds.

If you forget your password or cannot access the web configurator, you can use the **RESET BUTTON** at the back of the device to reload the factory-default configuration file. This

means that you will lose all configurations that you had previously and the web access password will be reset to the default.

2 Introducing the Web Configurator

2.1 Overview

The web configurator is an HTML-based management interface that allows easy device setup and management via Internet browser. The browser must support Secure WEB access via HTTPS with .TLS1.2 support.

Therefore, the supported WEB browsers are:

1. Chrome 49.0 and up
2. Firefox 45 and up
3. Opera 36 and up
4. Safari 10.1.2 and up
5. Internet Explorer 11.0 and up (Windows 7 and up)

The recommended screen resolution is 1366 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser popup windows from your device. Web popup blocking is enabled by default in Windows 7.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

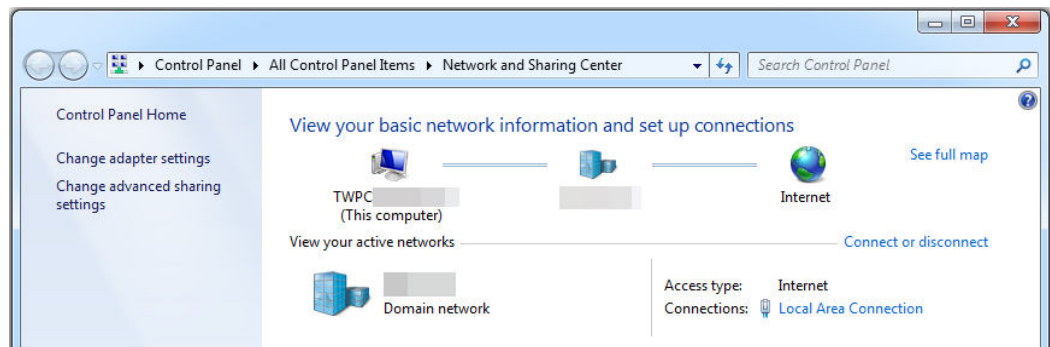
2.1.1 Basic Setting Information

Do the following before you start to use the LTE Device.

Step 1 Click **Start > Control Panel > Network and Sharing Center**.

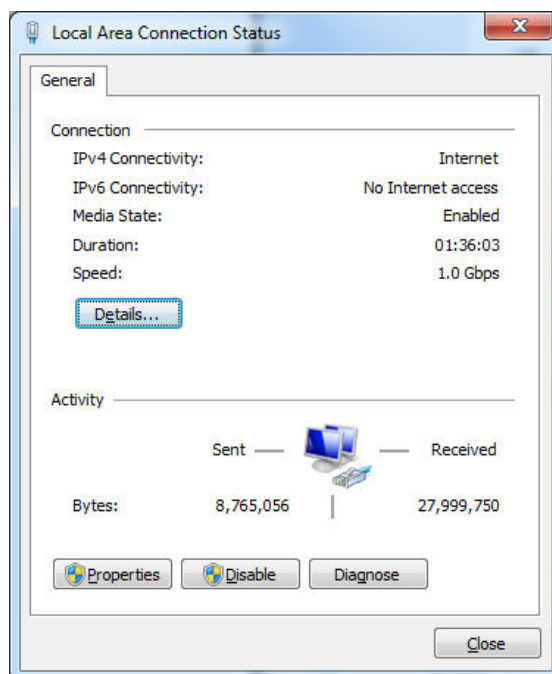
Step 2 Click your Internet connection.

Figure 2-1 Network and Sharing Center



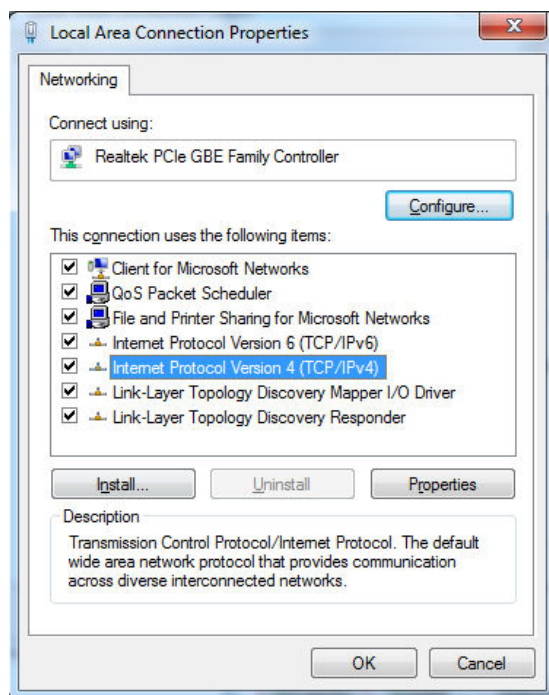
Step 3 Click **Properties**.

Figure 2-2 Connection Status



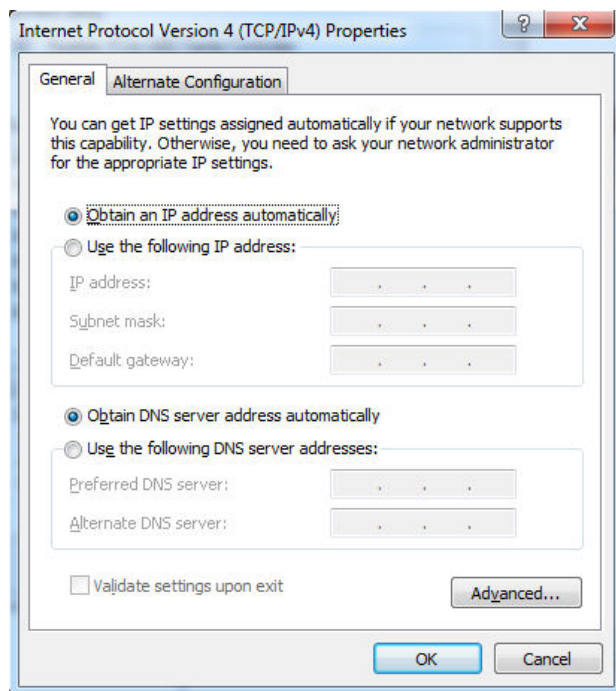
Step 4 Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

Figure 2-3 Connection Properties



Step 5 Select **Obtain an IP address automatically** and **Obtain DNS server address automatically** and click **OK** and then **Close** and **Close**.

Figure 2-4 Internet Protocol Version 4 (TCP/IPv4) Properties



----End

2.1.2 Accessing the Web Configurator

Step 1 Make sure your LTE Device hardware is properly connected (refer to the Quick Start Guide).

Step 2 Launch your web browser.

Step 3 Type "192.168.1.1" as the URL.

Step 4 The Web Configurator password screen displays.

- For user access, type "**user**" as the default username and "**LTE@Endusr**" as the default password.

Click **Login**. If you have changed the password, enter your password and click **Login**.

Figure 2-5 Password Screen (B2368-22)

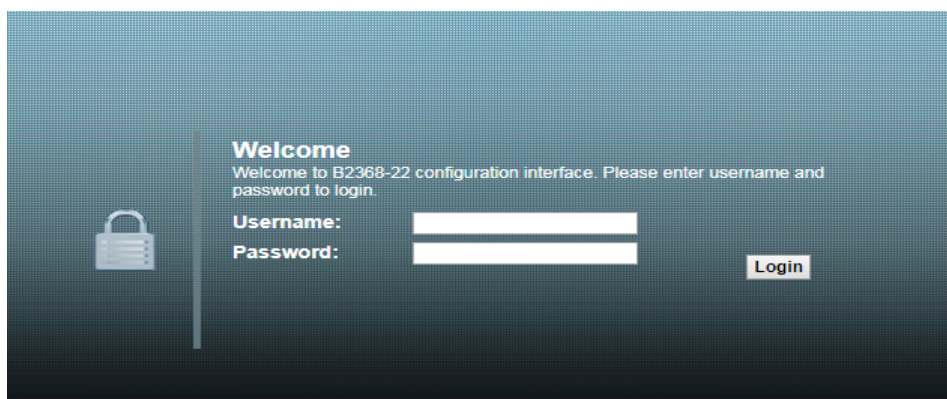


Figure 2-6 Password Screen (B2368-57)



Figure 2-7 Password Screen (B2368-66)



The following screen displays if you enter the password wrong three times.

Figure 2-8 Login Blocked Screen (B2368-22)

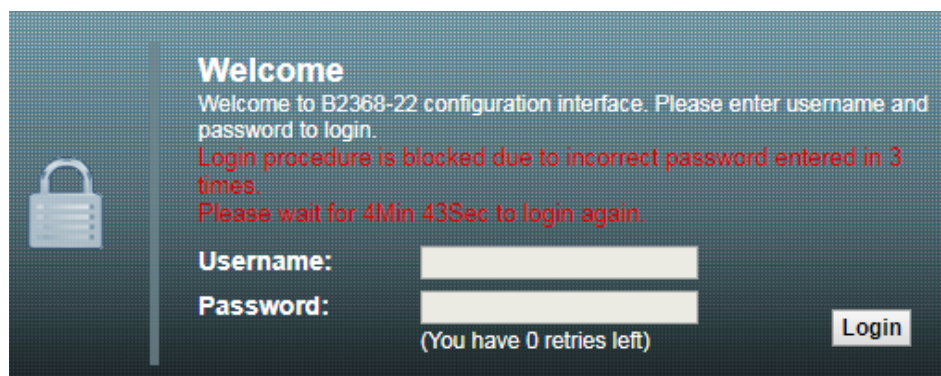
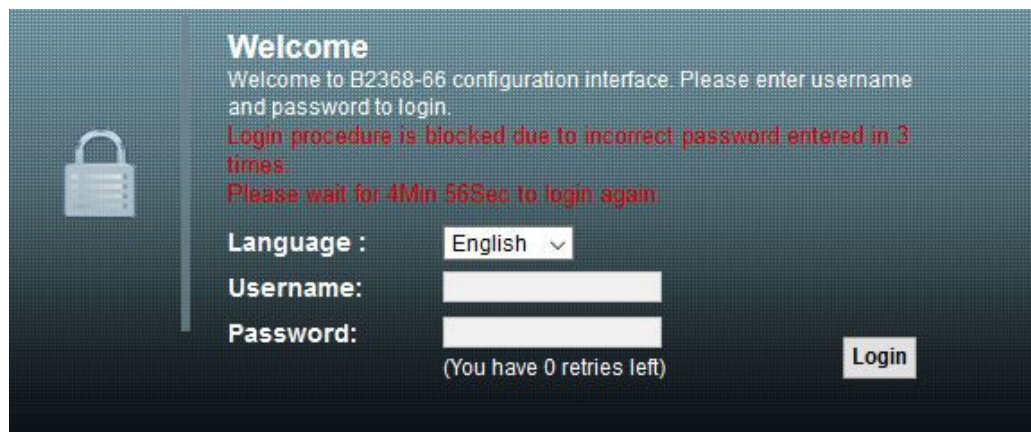


Figure 2-9 Login Blocked Screen (B2368-57)



Figure 2-10 Login Blocked Screen (B2368-66)



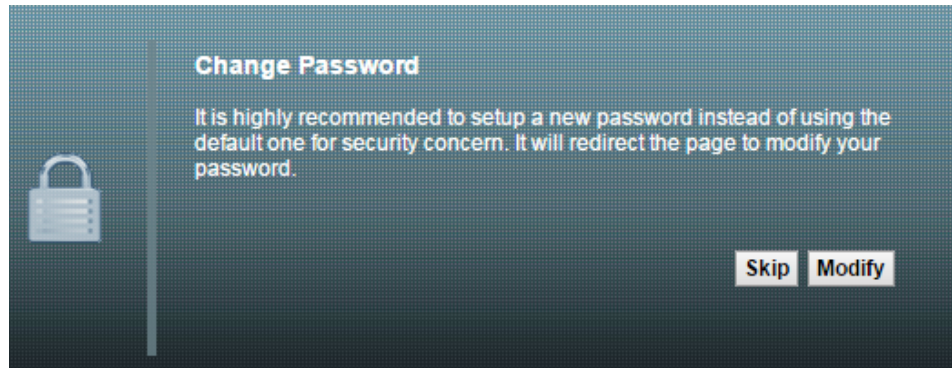
 NOTE

For security reasons, the LTE Device automatically logs you out if you do not use the web configurator for five minutes (default). If this happens, log in again.

Step 5 The following screen displays if you have not yet changed your password.

It is strongly recommended you change the default password. Enter a new password, retype it to confirm and click **Modify**; alternatively click **Skip** to proceed to the main menu if you do not want to change the password now.

Figure 2-11 Change Password Screen



Step 6 The **Connection Status** screen appears.

Figure 2-12 Connection Status (B2368-22)

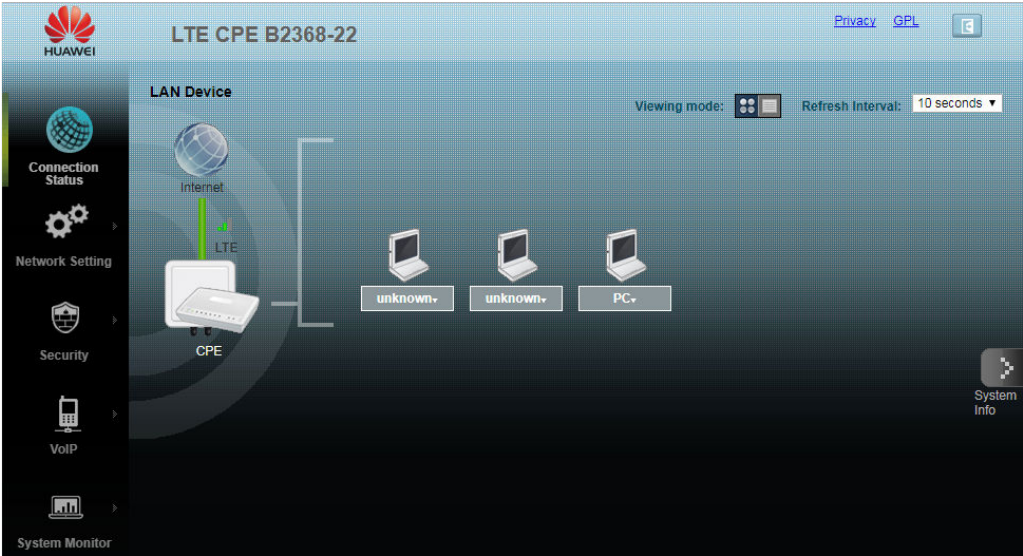
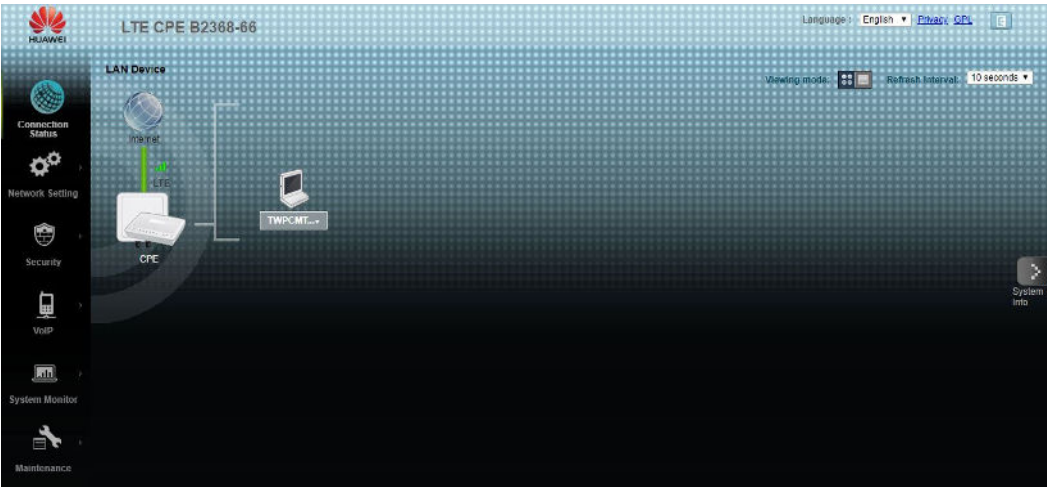


Figure 2-13 Connection Status (B2368-57)



Figure 2-14 Connection Status (B2368-66)



Step 7 Click **System Info** to display the **System Info** screen, where you can view the LTE Device's interface and system information.

---End

2.2 The Web Configurator Layout

Click **Connection Status > System Info** to show the following screen. (See [3.3 The System Info Screen](#) for more information.)

Figure 2-15 Web Configurator Layout (B2368-22)

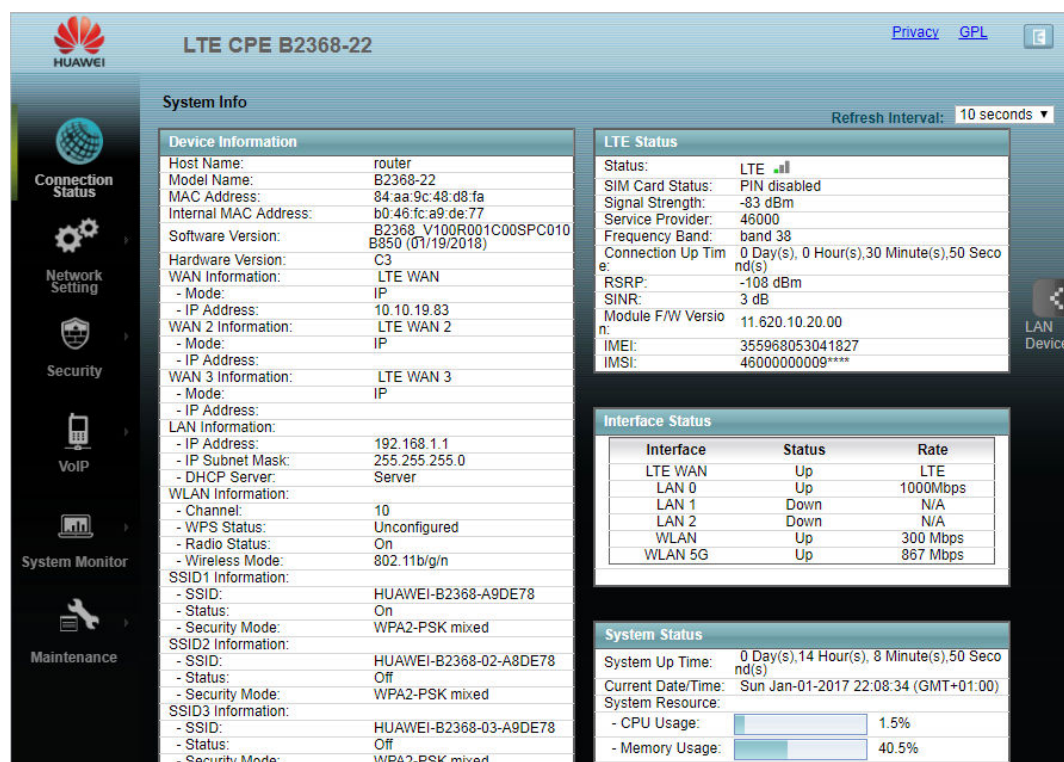


Figure 2-16 Web Configurator Layout (B2368-57)

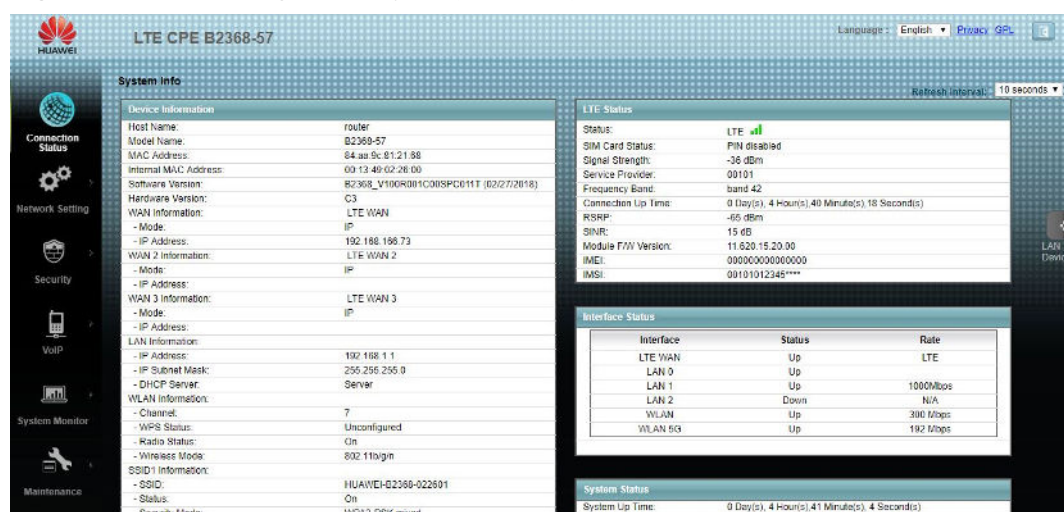
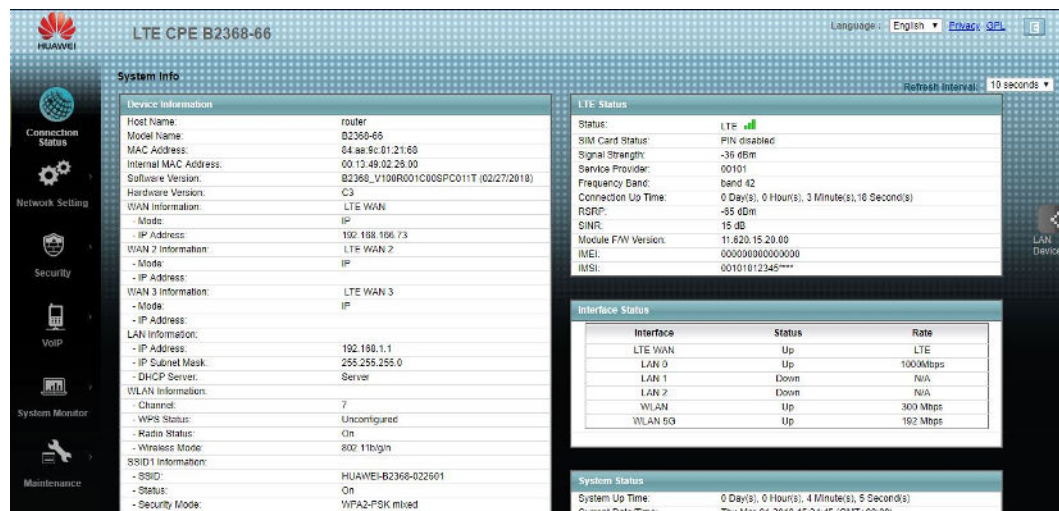


Figure 2-17 Web Configurator Layout (B2368-66)



As illustrated above, the main screen is divided into these parts:

- title bar
- main window
- navigation panel

2.2.1 Title Bar

The title bar provides links to the privacy policy and open source software notice. Click the Logout icon in the upper right corner to log out of the web configurator.



2.2.2 Main Window

The main window displays information and configuration fields. It is discussed in the rest of this document.

After you click **System Info** on the **Connection Status** screen, the **System Info** screen is displayed. See [3.3 The System Info Screen](#) for more information about the **System Info** screen.

If you click **LAN Device** on the **System Info** screen (A in [Figure 2-15](#)), the **Connection Status** screen appears. See [3.2 The Connection Status Screen](#) for more information about the **Connection Status** screen.

2.2.3 User Account

Use the **Maintenance > User Accounts** screen to configure system password for different user accounts. See [Chapter 19 User Account](#) for more information.

2.2.4 Navigation Panel

Use the menu items on the navigation panel to open screens to configure LTE Device features.

3 Connection Status and System Info

3.1 Overview

After you log into the web configurator, the **Connection Status** screen appears. This shows the network connection status of the LTE Device and clients connected to it.

Use the **System Info** screen to look at the current status of the device, system resources, interfaces (LAN, WAN and WLAN), and SIP accounts. You can also register and unregister SIP accounts.

3.2 The Connection Status Screen

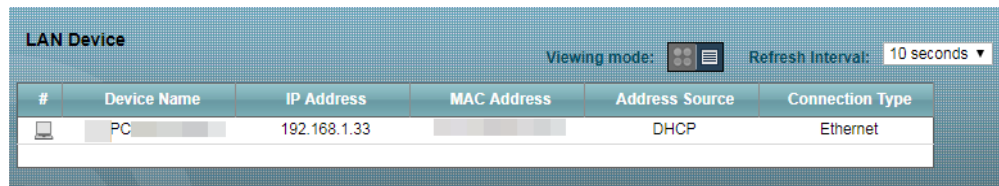
Use this screen to view the network connection status of the device and its clients. A warning message appears if there is a connection problem.

Figure 3-1 Connection Status: Icon View



If you prefer to view the status in a list, click **List View** in the **Viewing mode** selection box. You can configure how often you want the LTE Device to update this screen in **Refresh Interval**.

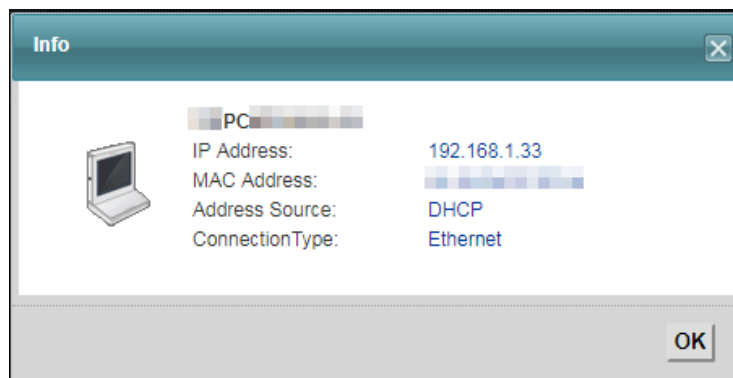
Figure 3-2 Connection Status: List View



#	Device Name	IP Address	MAC Address	Address Source	Connection Type
	PC	192.168.1.33		DHCP	Ethernet

In **Icon View**, if you want to view information about a client, click the client's name and **Info**.

Figure 3-3 Connection Status: List View > Info



In **List View**, you can also view the client's information.

3.3 The System Info Screen

Click **Connection Status > System Info** to open this screen.

Figure 3-4 System Info Screen (B2368-22)

System Info

Refresh Interval: 10 seconds ▼

Device Information

Host Name: router

Model Name: B2368-22

MAC Address: 84:aa:9c:41:f9:43

Internal MAC Address: 84:aa:9c:41:86:0c

Software Version: V100R001C00SPC010B580 (12/20/2017)

Hardware Version: C3

WAN Information: LTE WAN

- Mode: IP

- IP Address: 10.76.29.41

WAN 2 Information: LTE WAN 2

- Mode: IP

- IP Address:

WAN 3 Information: LTE WAN 3

- Mode: IP

- IP Address:

LAN Information:

- IP Address: 192.168.1.1

- IP Subnet Mask: 255.255.255.0

- DHCP Server: Server

WLAN Information:

- Channel: 4

- WPS Status: Unconfigured

- Radio Status: On

- Wireless Mode: 802.11b/g/n

SSID1 Information:

- SSID: HUAWEI-B2368-41860D

- Status: On

- Security Mode: WPA2-PSK mixed

SSID2 Information:

- SSID: HUAWEI-B2368-02-40860D

- Status: Off

- Security Mode: WPA2-PSK mixed

SSID3 Information:

- SSID: HUAWEI-B2368-03-41860D

- Status: Off

- Security Mode: WPA2-PSK mixed

SSID4 Information:

- SSID: HUAWEI-B2368-04-42860D

- Status: Off

- Security Mode: WPA2-PSK mixed

WLAN 5G Information:

- Channel: 56

- WPS Status: Unconfigured

- Radio Status: On

- Wireless Mode: 802.11a/n/ac

5G SSID1 Information:

- SSID: HUAWEI-B2368-5G-41860E

- Status: On

- Security Mode: WPA2-PSK mixed

5G SSID2 Information:

- SSID: HUAWEI-B2368-5G-02-40860E

- Status: Off

- Security Mode: WPA2-PSK mixed

5G SSID3 Information:

- SSID: HUAWEI-B2368-5G-03-41860E

- Status: Off

- Security Mode: WPA2-PSK mixed

5G SSID4 Information:

- SSID: HUAWEI-B2368-5G-04-42860E

- Status: Off

- Security Mode: WPA2-PSK mixed

LTE Status

Status: LTE

SIM Card Status: PIN disabled

Signal Strength: -98 dBm

Service Provider: 46692

Frequency Band: band 1

Connection Up Time: 0 Day(s), 0 Hour(s), 1 Minute(s), 31 Second(s)

RSRP: -97 dBm

SINR: 4 dB

Module F/W Version: 11.620.09.20.00

IMEI: 0000000000000000

IMSI: 466924252204139

Interface Status

Interface	Status	Rate
LTE WAN	Up	LTE
LAN 0	Down	N/A
LAN 1	Up	100Mbps
LAN 2	Up	1000Mbps
WLAN	Up	300 Mbps
WLAN 5G	Up	867 Mbps

System Status

System Up Time: 0 Day(s), 0 Hour(s), 2 Minute(s), 21 Second(s)

Current Date/Time: Wed Dec-27-2017 13:40:00 (GMT+01:00)

System Resource:

- CPU Usage: 0.7%

- Memory Usage: 37.8%

Registration Status

Account	Action	Account Status	URI
SIP 1	Register	In-Active	ChangeMe@ChangeMe

Figure 3-5 System Info Screen (B2368-57)

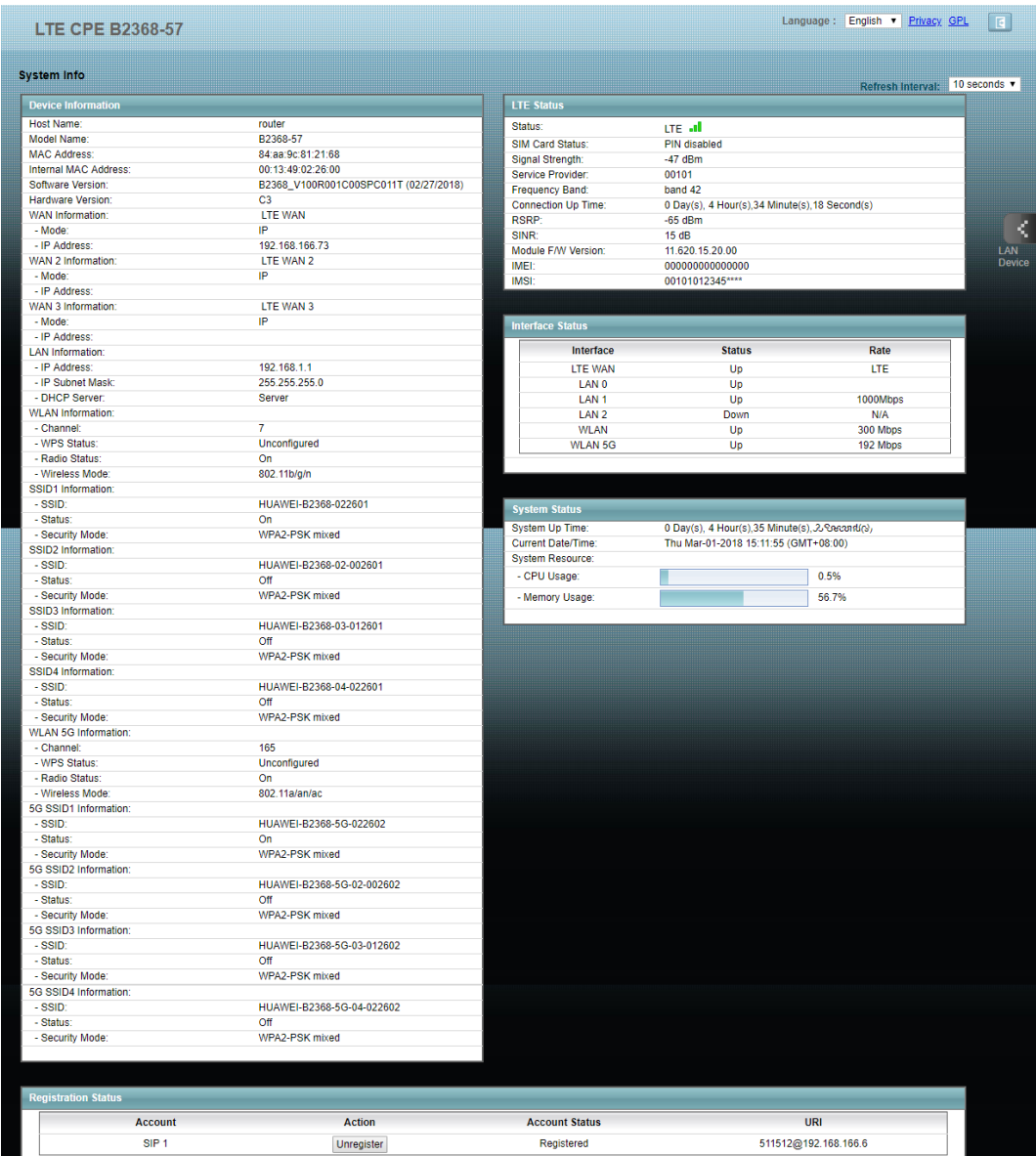
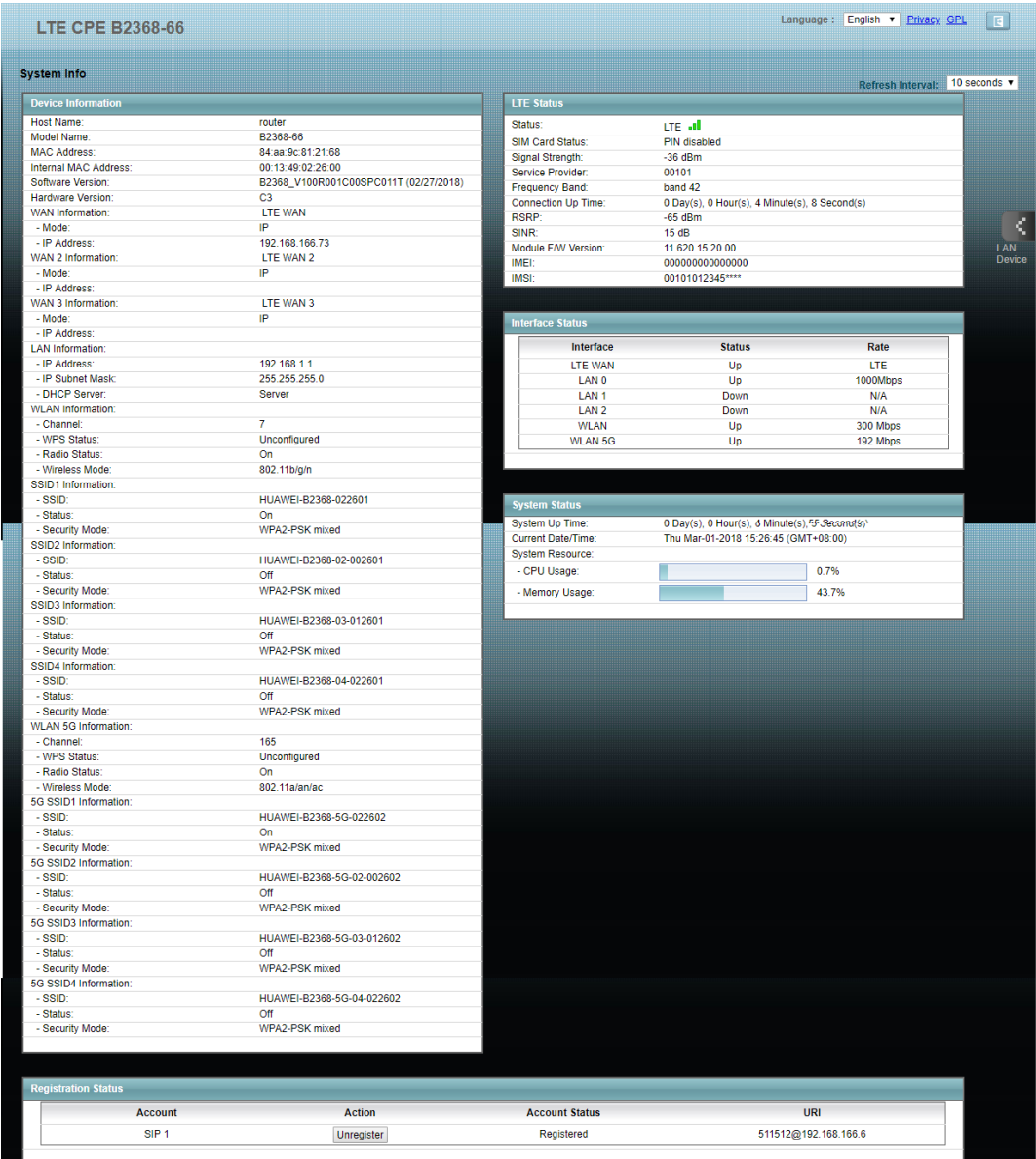


Figure 3-6 System Info Screen (B2368-66)



Each field is described in the following table.

Table 3-1 System Info Screen

Label	Description
Refresh Interval	Select how often you want the LTE Device to update this screen from the drop-down list box.
Device Information	
Host Name	This field displays the LTE Device system name. It is used for identification. You can change this in the Maintenance > System screen's Host Name field.
Model Name	This is the model name of your device.

Label	Description
MAC Address	This is the MAC (Media Access Control) or Ethernet address of your ODU Device.
Internal MAC Address	This is the MAC (Media Access Control) or Ethernet address of your IDU Device.
Software Version	This field displays the current version of the firmware inside the device. Go to the Maintenance > Firmware Upgrade screen to change it.
Hardware Version	This field displays the version of the device hardware.
WAN Information	
Mode	This is the method of encapsulation used by your ISP.
IP Address	This field displays the current IP address of the LTE Device in the WAN.
WAN 2 Information	
Mode	This is the method of encapsulation used by your ISP.
IP Address	This field displays the current IP address of the LTE Device in the WAN.
LAN Information	
IP Address	This field displays the current IP address of the LTE Device in the LAN.
IP Subnet Mask	This field displays the current subnet mask in the LAN.
DHCP Server	This field displays what DHCP services the LTE Device is providing to the LAN. Choices are: Server - The LTE Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. None - The LTE Device is not providing any DHCP services to the LAN.
WLAN Information	
Channel	This is the channel number used by the LTE Device now.
WPS Status	Configured displays when a wireless client has connected to the LTE Device or WPS is enabled and wireless or wireless security settings have been configured. Unconfigured displays if WPS is disabled or wireless security settings have not been configured.
Radio Status	On displays when the WLAN radio is enabled. Off displays when the WLAN radio is turned off.
SSID (1~4) Information	
SSID	This is the descriptive name used to identify the LTE Device in the wireless LAN.

Label	Description
Status	This shows whether or not the SSID is enabled (on).
Security Mode	This displays the type of security the LTE Device is using in the wireless LAN.
WLAN 5G Information	
Channel	This is the 5 GHz channel number used by the LTE Device now.
WPS Status	Configured displays when a wireless client has connected to the LTE Device or WPS is enabled and wireless or wireless security settings have been configured. Unconfigured displays if WPS is disabled or wireless security settings have not been configured.
Radio Status	On displays when the WLAN radio is enabled. Off displays when the WLAN radio is turned off.
5G SSID (1~4) Information	
SSID	This is the descriptive name used to identify the LTE Device in the wireless LAN.
Status	This shows whether or not the SSID is enabled (on).
Security Mode	This displays the type of security the LTE Device is using in the wireless LAN.
LTE Status	
Status	This displays 4G LTE if there is an LTE connection, otherwise, it displays N/A .
SIM Card Status	This displays PIN disable if SIM card needs PIN or PUK to unlock, it displays PIN required or PUK required .
Signal Strength	This displays the strength of the LTE connection that the LTE Device has with the base station which is also known as eNodeB or eNB.
Service Provider	This displays the service provider's name of the connected LTE Network.
Frequency Band	This displays the LTE band if there is an LTE connection, otherwise, it displays N/A .
Connection Uptime	This displays how long the LTE connection has been available since it was last established successfully.
RSRP	This displays the RSRP strength of the LTE connection that the LTE Device has with the base station which is also known as eNodeB or eNB.
SINR	This displays the SINR strength of the LTE connection that the LTE Device has with the base station which is also known as eNodeB or eNB.

Label	Description
Module F/W Version	This displays the firmware version of LTE module.
IMEI	This displays the LTE Device's International Mobile Equipment Identity number (IMEI). An IMEI is a unique ID used to identify a mobile device.
IMSI	This displays the International Mobile Subscriber Identity (IMSI) of the SIM card inserted in the outdoor unit. An IMSI is a unique ID used to identify a mobile subscriber in a mobile network.
Interface Status	
Interface	This column displays each interface the LTE Device has.
Status	This field indicates whether or not the LTE Device is using the interface. For the LTE WAN interface, this field displays Up when the LTE Device is connected to an LTE network and Down when the LTE Device does not have an LTE connection. For the LAN interfaces, this field displays Up when the LTE Device is using the interface and Down when the LTE Device is not using the interface. For the WLAN interface, it displays Up when WLAN is enabled or Down when WLAN is disabled.
Rate	For the LTE WAN interface, this displays 4G LTE if there is an LTE connection. For the LAN interface, this displays the port speed and duplex setting. For the WLAN interface, it displays the maximum transmission rate when WLAN is enabled or N/A when WLAN is disabled.
System Status	
System Up Time	This field displays how long the LTE Device has been running since it last started up. The LTE Device starts up when you plug it in, when you restart it (Maintenance > Reboot), or when you reset it (see 1.5.3 The RESET Button).
Current Date/Time	This field displays the current date and time in the LTE Device. You can change this in Maintenance > Time Setting .
System Resource	
CPU Usage	This field displays what percentage of the LTE Device's processing ability is currently used. When this percentage is close to 100%, the LTE Device is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications.

Label	Description
Memory Usage	This field displays what percentage of the LTE Device's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100%, the LTE Device is probably becoming unstable, and you should restart the device. See 23 Log Setting , or turn off the device (unplug the power) for a few seconds.
Registration Status	
Account	This column displays each SIP account in the LTE Device.
Action	This field displays the current registration status of the SIP account. You have to register SIP accounts with a SIP server to use VoIP. If the SIP account is already registered with the SIP server, ● Click Unregister to delete the SIP account's registration in the SIP server. This does not cancel your SIP account, but it deletes the mapping between your SIP identity and your IP address or domain name. ● The second field displays Registered. If the SIP account is not registered with the SIP server, ● Click Register to have the LTE Device attempt to register the SIP account with the SIP server. ● The second field displays the reason the account is not registered. Inactive - The SIP account is not active. You can activate it in VoIP > SIP > SIP Settings. Register Fail - The last time the LTE Device tried to register the SIP account with the SIP server, the attempt failed. The LTE Device automatically tries to register the SIP account when you turn on the LTE Device or when you activate it.
Account Status	This field shows Active when the SIP account has been registered and ready for use or In-Active when the SIP account is not yet registered.
URI	This field displays the account number and service domain of the SIP account. You can change these in VoIP > SIP > SIP Settings .

4 Broadband

4.1 Overview

This chapter discusses the LTE Device's **Broadband** screens. Use these to configure broadband settings, specify the PIN for your SIM card, and lock a band, frequency or cell tower for the LTE Device's LTE connection.

4.2 Broadband Screen

Use this screen to lock a band, frequency or cell tower for the LTE Device's LTE connection. Click **Network Setting > Broadband** to open the following screen.

Figure 4-1 Network Setting > Broadband > Broadband

LTE Connection Switch

Action

☒ Connect ☐ Disconnect

Apply

Cancel

Data Roaming

Data Roaming

☐ Enable ☒ Disable

Apply

Cancel

Internet Setup

#	Enabled	Name	APN	NAT	Modify
1	Enabled	Data	Auto APN	Enabled	
2	Disabled	Voice	apn2	--	
3	Disabled	DM	apn3	--	

Note :

It supports only one auto APN at the same time.

The following table describes the fields in this screen.

Table 4-1 Network Setting > Broadband > Broadband

Label	Description
Action	Select Connect to have the LTE Device use the LTE connection. Select Disconnect to have the LTE Device not use the LTE connection.
Apply	Click this to save the change in this section.
Cancel	Click this to restore your previously saved settings in this section.
Data Roaming	Select Enable to allow the LTE Device to use other carriers' LTE connections. Select Disable to stop the LTE Device from using other carriers' LTE connections.
Apply	Click this to save the change in this section.
Cancel	Click this to restore your previously saved settings in this section.
Internet Setup	
#	The index number of the broadband connection in the list.
Enabled	This shows whether the broadband connection is turned on or off.
Name	This shows the name of the broadband connection.
APN	This is the name of the LTE network to which the broadband connection connects.
NAT	This shows whether NAT is activated or not for this connection.
Modify	Click the Edit icon to configure the connection.

4.2.1 Edit Broadband Connection

Use this screen to configure a WAN connection.

Click an LTE connection's **Edit** icon to display a screen like the one shown next.

Figure 4-2 Network Setting > Broadband > Broadband > Edit

WAN Interface Edit

General
Name : Data

APN
Auto APN ☒
APN : apn
MTU 1500 (600-1500)

Routing Feature
NAT Enable : ☐
IP Pass Through : ☒

IP Pass Through setting
IP Pass Through Mode ☒ Dynamic ☐ Static
Specific Device MAC Address : 00:00:00:00:00:00
IP Pass Through Lease Time : 300 Seconds

Warning: VPN feature and IP Pass Through feature can't be used at the same time!

Apply Back

The following table describes the fields in this screen.

Table 4-2 Network Setting > Broadband > Broadband > Edit

Label	Description
Name	This shows the name of the broadband connection.
Auto APN	Select this to have the LTE Device configure the APN (Access Point Name) of the LTE network automatically. Otherwise, enter the APN manually in the field below.
APN	Enter the Access Point Name (APN) of an LTE network, which your service provider gave you.
MTU	The Maximum Transmission Unit (MTU) defines the size of the largest packet allowed on an interface or connection. Enter the MTU for this WAN interface in this field.
NAT Enable	Select this to activate NAT on the WAN.
IP Pass Through	Select this to allow the ISP to assign IP addresses directly to the LAN devices. This disables NAT and DHCP server configuration (Network Setting > Home Networking > LAN Setup). The LTE Device will be remotely managed by HTTPS and SNMP. Choosing this option also displays more IP pass through configuration parameters.

Label	Description
IP Pass Through Mode	Select Dynamic to give the client get the ISP allocated IP via DHCP with 5 minutes lease time. Select Static to allow only clients with a designated MAC address to get the ISP allocated IP via DHCP.
Specific Device MAC Address	When you set the IP pass mode to static, specify the designated MAC address here.
IP Pass Through Lease Time	Specify for how many seconds the LAN client can use the ISP assigned IP address.
Apply	Click Apply to save your changes.
Back	Click Back to return to the previous screen.

4.3 SIM Screen

If your LTE Device has the **SIM** screen, you may use it to specify the PIN for your SIM card. Click **Network Setting > Broadband > SIM** to open the following screen.

Figure 4-3 Network Setting > Broadband > SIM

The PIN lock of the SIM protects the device against unauthorized accesses to internet. You can active, modify, or unlock the PIN.
The device cannot provide internet services when the SIM card is not inserted or the PIN fails to be verified.

PIN Management

SIM card status :

PIN verification :

Input PIN :

Remain attempts :

PIN disabled

☒ Enable ☐ Disable

3

Apply

Cancel

The following table describes the fields in this screen.

Table 4-3 Network Setting > Broadband > SIM

Label	Description
SIM card status	This displays the SIM card status: PIN disabled - the SIM card has no PIN code security. PIN required - the SIM card has PIN code security, but you did not enter the PIN code yet. PIN verified - the SIM card has PIN code security, and you entered the correct PIN code. PIN locked - you entered an incorrect PIN code too many times, so the SIM card has been locked; contact the ISP for a PUK (Pin Unlock Key) to unlock the SIM card. SIM error - the LTE Device does not detect that there is a SIM card inserted.
PIN verification	A PIN (Personal Identification Number) code is a key to a 3G card. Without the PIN code, you cannot use the 3G card. Select Enable if the 4G service provider requires you to enter a PIN to use the SIM card. Select Disable if the 4G service provider lets you use the SIM without inputting a PIN.
Input PIN	If you enabled PIN verification, enter the 4-digit PIN code (0000 for example) provided by your ISP. If you enter the PIN code incorrectly too many times, the ISP may block your SIM card and not let you use the account to access the Internet.
Remain attempts	This is how many more times you can try to enter the PIN code before the ISP blocks your SIM card.
Apply	Click this to save the change in this section.
Cancel	Click this to restore your previously saved settings in this section.

4.3.1 SIM Locked Screen

If the SIM card is locked, use this screen to enter the PUK (Pin Unlock Key) code.

NOTE

You may have to ask the service provider for a PUK code to unlock the SIM card.

CAUTION

You will need a new SIM card if you enter the wrong PUK code too many times!

Figure 4-4 Network Setting > Broadband > SIM: Locked

BroadbandSIMLTE Setting

You have entered in the incorrect PIN code 3 times. The device will request a PUK(PIN Unlock Key) code. The PUK is required to unlock SIM card.
If the incorrect PUK code is entered 10 times, your SIM card will be permanently locked and a new SIM card must be purchased. The device will display the following status: "SIM card locked call operator"

PIN Management

SIM card status :

PUK :

New PIN :

Confirm New PIN :

Remain attempts :

PIN locked

10

Apply

Cancel

The following table describes the fields in this screen.

Table 4-4 Network Setting > Broadband > SIM: Locked

Label	Description
SIM card status	This displays the SIM card status: PIN locked - you entered an incorrect PIN code too many times, so the SIM card has been locked; contact the ISP for a PUK (Pin Unlock Key) to unlock the SIM card.
PUK	Enter the PUK (Pin Unlock Key) code from the ISP to unlock the SIM card.
New PIN	Enter the new PIN code for the SIM card.
Confirm New PIN	Re-enter the new PIN code for the SIM card.
Remain attempts	This shows how many more times you can try to enter the PUK code before permanently damaging the SIM card.
Apply	Click this to save the change in this section.
Cancel	Click this to restore your previously saved settings in this section.

4.4 LTE Setting Screen

Use this screen to lock a band, frequency or cell tower for the LTE Device's LTE connection. Click **Network Setting > Broadband > LTE Setting** to open the following screen.

Figure 4-5 Network Setting > Broadband > LTE Setting

This page is using to lock a band, freq or cell for the CPE.

LTE Setting :

☒ Enable ☐ Disable

LockMode :

LockBand

Band:

☐ 1 ☐ 3 ☐ 7 ☐ 8 ☐ 20 ☐ 38 ☐ 40 ☐ 41 ☐ 42 ☐ 43

Apply

Cancel

This page is using to lock a band, freq or cell for the CPE.

LTE Setting :

☒ Enable ☐ Disable

LockMode :

LockDlEarfcn

Band:

1

DL EARFCN: Disable inter-frequency reselect or handover: ☐

Apply

Cancel

This page is using to lock a band, freq or cell for the CPE.

LTE Setting :

☒ Enable ☐ Disable

LockMode :

LockCell

Band:

1

DL EARFCN: PCI:

Apply

Cancel

The following table describes the fields in this screen.

Table 4-5 Network Setting > Broadband > LTE Setting

Label	Description
LTE Setting	Select Enable to set the LTE Device's LTE connection to use a specific band, frequency, or cell tower. Select Disable to let the LTE Device's LTE connection automatically select a band, frequency, or cell tower to use.

Issue 03 (2019-01-31)

Copyright © Huawei Technologies Co., Ltd.

34

Label	Description
LockMode	Select LockBand to set the LTE Device's LTE connection to use a specific LTE band. Then select the LTE band on the right. Select LockDlEarfcn to set the LTE Device's LTE connection to use a specific downlink frequency. Then select the LTE band and specify the downlink EARFCN (E-UTRA Absolute Radio Frequency Channel Number) on the right (0-65535). If you do not want to reselect and handover, please tick "Disable inter-frequency reselect or handover" Select LockCell to set the LTE Device's LTE connection to use a specific cell tower. Then select the LTE band, specify the downlink EARFCN (0-65535), and specify the cell tower's PCI (Physical Cell Identifier) on the right (0-503).
Apply	Click this to save your changes and to apply them to the LTE Device.
Cancel	Click this to set every field in this screen to its last-saved value.

5 Wireless

5.1 Overview

This chapter describes the LTE Device's **Network Setting > Wireless** screens. Use these screens to set up your LTE Device's wireless connection.

5.1.1 Wireless Network Overview

Wireless networks consist of wireless clients, access points and bridges.

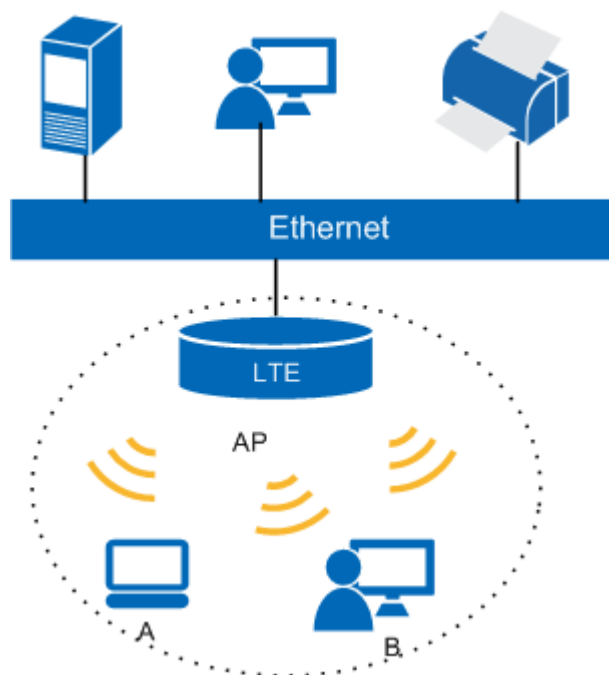
- A wireless client is a radio connected to a user's computer.
- An access point is a radio with a wired connection to a network, which can connect with numerous wireless clients and let them access the network.
- A bridge is a radio that relays communications between access points and wireless clients, extending a network's range.

Traditionally, a wireless network operates in one of two ways.

- An "infrastructure" type of network has one or more access points and one or more wireless clients. The wireless clients connect to the access points.
- An "ad-hoc" type of network is one in which there is no access point. Wireless clients connect to one another in order to exchange information.

The following figure provides an example of a wireless network.

Figure 5-1 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** use the access point (**AP**) to interact with the other devices (such as the printer) or with the Internet. Your LTE Device is the AP.

Every wireless network must follow these basic guidelines.

- Every device in the same wireless network must use the same SSID.
The SSID is the name of the wireless network. It stands for Service Set Identifier.
- If two wireless networks overlap, they should use a different channel.
Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every device in the same wireless network must use security compatible with the AP.
- Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

Radio Channels

In the radio spectrum, there are certain frequency bands allocated for unlicensed, civilian use. For the purposes of wireless networking, these bands are divided into numerous channels. This allows a variety of networks to exist in the same place without interfering with one another. When you create a network, you must select a channel to use.

Since the available unlicensed spectrum varies from one country to another, the number of available channels also varies.

A channel is the radio frequency used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

5.1.2 Before You Begin

Before you start using these screens, ask yourself the following questions. See [5.5 Technical Reference](#) if some of the terms used here do not make sense to you.

- What wireless standards do the other wireless devices support (IEEE 802.11g, for example)? What is the most appropriate standard to use?
- What security options do the other wireless devices support (WPA-PSK, for example)?
- What is the best one to use?
- Do the other wireless devices support WPS (Wi-Fi Protected Setup)? If so, you can set up a well-secured network very easily.
Even if some of your devices support WPS and some do not, you can use WPS to set up your network and then add the non-WPS devices manually, although this is somewhat more complicated to do.
- What advanced options do you want to configure, if any? If you want to configure advanced options, ensure that you know precisely what you want to do. If you do not want to configure advanced options, leave them alone.

NOTE

The following sections show the regular (2.4 GHz) wireless screens. The 5 GHz wireless screens work the same.

5.2 The Wireless General Screen

Use this screen to enable the Wireless LAN or Wireless 5 GHz LAN, enter the SSID and select the wireless security mode.

NOTE

If you are configuring the LTE Device from a computer connected to the wireless LAN and you change the LTE Device's SSID or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the LTE Device's new settings.

Click **Network Setting > Wireless** (or **Wireless 5G**) to open the **General** screen. The regular (2.4 GHz) wireless screen is shown here. The 5 GHz wireless screen works the same. Select the **Enable Wireless LAN** checkbox to show the Wireless configurations.

Figure 5-2 Network Setting > Wireless > General

Wireless

General

More AP

WPS

A wireless network name (also known as SSID) and a security level are basic elements to start a wireless service. It is recommended to set a security level other than No Security to protect your data from unauthorized access or damage via wireless network.

Wireless Network Setup

Wireless : ☒ Enable Wireless LAN

Wireless Network Settings

Wireless Network Name(SSID):

HUAWEI-B2368-418664

☐ Hide SSID

Wireless Isolation:

☐ Enable ☒ Disable

BSSID :

84:AA:9C:41:96:64

Mode Select :

802.11b/g/n ▼

BandWidth :

20/40 MHz ▼

Channel Selection :

Auto ▼

Operating Channel

4

Security Level



No Security

More Secure (Recommended)

Security Mode :

WPA2-PSK ▼

Enter 8-63 characters (a-z, A-Z, 0-9). Using 2 or more of 3 types(a-z/A-Z, 0-9) is strongly recommended

Show Password : ☐

Pre-Shared Key :

.....

more...

Apply

Cancel

Note :

There is potential security risk when choosing No Security or security mode WPA-PSK.

Figure 5-3 Network Setting > Wireless 5G > General

Wireless 5G

GeneralMore APWPS

A wireless network name (also known as SSID) and a security level are basic elements to start a wireless service. It is recommended to set a security level other than No Security to protect your data from unauthorized access or damage via wireless network.

Wireless Network Setup

Wireless :

☒ Enable Wireless LAN

Wireless Network Settings

Wireless Network Name(SSID):

HUAWEI-B2368-5G-418665

☐ Hide SSID

Wireless Isolation:

☐ Enable ☒ Disable

BSSID :

84-AA-9C:41:86:65

Mode Select :

802.11a/n/ac

BandWidth :

20/40/80 MHz

Channel Selection :

Auto

Operating Channel

52

Security Level

No Security

More Secure (Recommended)

Security Mode :

WPA2-PSK

Enter 8-63 characters (a-z, A-Z, 0-9). Using 2 or more of 3 types(a-z/A-Z, 0-9) is strongly recommended

Show Password :

☐

Pre-Shared Key :

more

Apply

Cancel

Note :

There is potential security risk when choosing No Security or security mode WPA-PSK.

The following table describes the Labels in this screen.

Table 5-1 Network > Wireless > General

Label	Description
Wireless Network Setup	
Wireless	Select the Enable Wireless LAN check box to activate the wireless LAN.
Wireless Network Settings	

Issue 03 (2019-01-31)

Copyright © Huawei Technologies Co., Ltd.

40

Label	Description
Wireless Network Name (SSID)	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.
Wireless Isolation	Select this to keep the wireless clients in this SSID from communicating with each other directly through the Router.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
BSSID	This shows the MAC address of the wireless interface on the LTE Device when wireless LAN is enabled.
Mode Select	Select the type of WLAN client device connections to support. In the Wireless General screen select which WLAN client devices can associate with the LTE Device's 2.4 GHz wireless network: ● 802.11b/g/n allows IEEE 802.11b, IEEE 802.11g and IEEE 802.11n compliant WLAN devices. The transmission rate of your LTE Device might be reduced. ● 802.11g/n allows IEEE 802.11g and IEEE 802.11n compliant WLAN devices. ● 802.11b/g allows IEEE 802.11b and IEEE 802.11g compliant WLAN devices. The transmission rate of your LTE Device might be reduced. ● 802.11n allows only IEEE 802.11n compliant WLAN devices. ● 802.11g allows only IEEE 802.11g compliant WLAN devices. ● 802.11b allows only IEEE 802.11b compliant WLAN devices. In the Wireless 5G General screen select which WLAN client devices can associate with the LTE Device's 5 GHz wireless network: ● 802.11a/an/ac allows IEEE 802.11a, IEEE 802.11n, and IEEE 802.11ac compliant WLAN devices. ● 802.11an/ac allows IEEE 802.11n and IEEE 802.11ac compliant WLAN devices. ● 802.11a/an allows IEEE 802.11a and IEEE 802.11n compliant WLAN devices. ● 802.11an allows only IEEE 802.11n compliant WLAN devices. ● 802.11a allows only IEEE 802.11a compliant WLAN devices.

Label	Description
BandWidth	Select the channel bandwidth the LTE Device's wireless LAN uses. For 5 GHz wireless, select 20/40/80 MHz to allow the LTE Device to use 1, 2, or 3 channels for maximum throughput. Select 20/40 MHz to allow the LTE Device to use 1 or 2 channels. Select 20 MHz to lesson radio interference with other wireless devices in your neighborhood.
Channel Selection	Set the channel depending on your particular region. Select a channel or use Auto to have the LTE Device automatically determine a channel to use. If you are having problems with wireless interference, changing the channel may help. Try to use a channel that is as many channels away from any channels used by neighboring APs as possible. The channel number which the LTE Device is currently using then displays in the Operating Channel field.
Operating Channel	This is the channel currently being used by your AP.
Security Level	
Security Mode	Select More Secure to add security on this wireless network. The wireless clients which want to associate to this network must have the same wireless security settings as the LTE Device. When you select to use security, additional options appears in this screen. Or you can select No Security to allow any client to associate this network without any data encryption or authentication. See the following sections for more details about wireless security modes.
Apply	Click Apply to save your changes back to the LTE Device.
Cancel	Click Cancel to restore your previously saved settings.

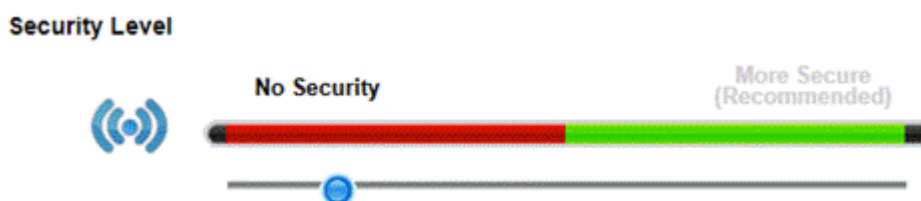
No Security

NOTE

Select **No Security** to allow wireless stations to communicate with the access points without any data encryption or authentication.

If you do not enable any wireless security on your LTE Device, your network is accessible to any wireless networking device that is within range.

Figure 5-4 Wireless> General: No Security



The following table describes the Labels in this screen.

Table 5-2 Wireless > General: No Security

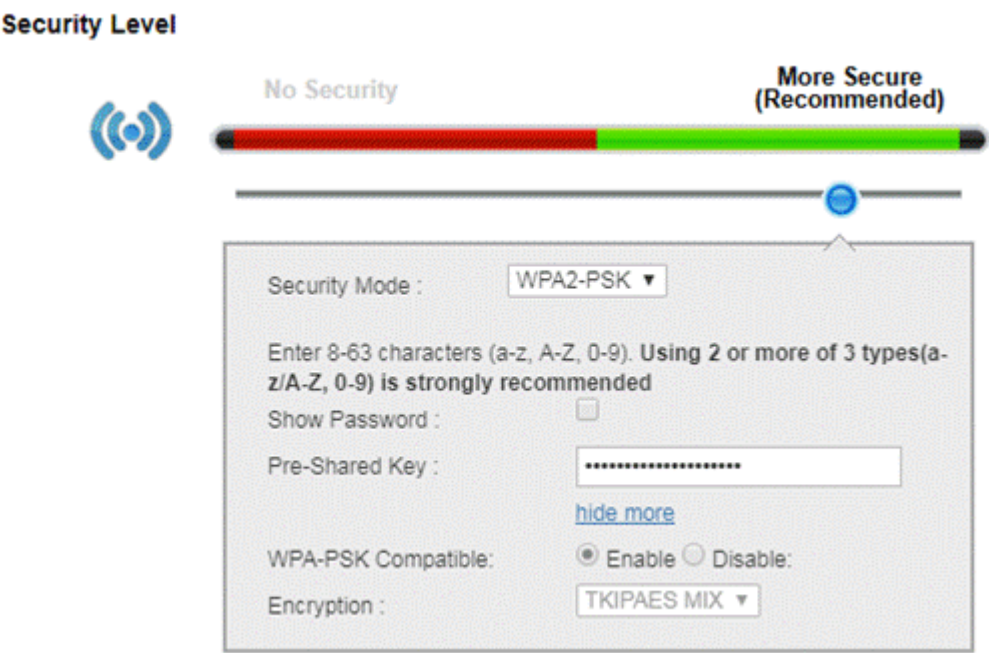
Label	Description
Security Level	Choose No Security from the sliding bar.

5.2.1 More Secure (WPA(2)-PSK)

The WPA-PSK security mode provides both data encryption and user authentication. Using a Pre-Shared Key (PSK), both the LTE Device and the connecting client share a common password in order to validate the connection. This type of encryption, while robust, is not as strong as the newer WPA2-PSK.

Click **Network Setting > Wireless** (or **Wireless 5G**) to display the **General** screen. Select **More Secure** as the security level. Then select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 5-5 Figure 1-1 Wireless > General: More Secure: WPA(2)-PSK



The following table describes the Labels in this screen.

Table 5-3 Wireless > General: WPA(2)-PSK

Label	Description
Security Level	Select More Secure to enable WPA(2)-PSK data encryption.

Label	Description
Security Mode	Select WPA-PSK or WPA2-PSK from the drop-down list box.
Show Password	Select this to display the password as readable text.
Pre-Shared Key	Type a pre-shared key from 8 to 63 case-sensitive ASCII characters.
more.../hide more	Click more... to show more fields in this section. Click hide more to hide them.
WPA-PSK Compatible	This field appears when you choose WPA2-PSK as the Security Mode . Check this field to allow wireless devices using WPA-PSK security mode to connect to your LTE Device. The LTE Device supports WPA-PSK and WPA2-PSK simultaneously.
Encryption	If the security mode is WPA-PSK, the encryption mode is set to TKIP to enable Temporal Key Integrity Protocol (TKIP) security on your wireless network. If the security mode is WPA2-PSK and WPA-PSK Compatible is disabled, the encryption mode is set to AES to enable Advanced Encryption System (AES) security on your wireless network. AES provides superior security to TKIP. If the security mode is WPA2-PSK and WPA-PSK Compatible is enabled, the encryption mode is set to TKIPAES MIX to allow both TKIP and AES types of security in your wireless network.

5.3 The More AP Screen

The LTE Device can broadcast up to four wireless network names at the same time. This means that users can connect to the LTE Device using different SSIDs. You can secure the connection on each SSID profile so that wireless clients connecting to the LTE Device using different SSIDs cannot communicate with each other.

This screen allows you to enable and configure multiple Basic Service Sets (BSSs) on the LTE Device.

Click **Network Setting > Wireless (or Wireless 5G) > More AP**. The following screen displays.

Figure 5-6 Network Settings > Wireless > More AP

#	Active	SSID	Security	Modify
2		HUAWEI-B2368-50AA01	WPA2-PSK mixed	
3		HUAWEI-B2368-51AA01	WPA2-PSK mixed	
4		HUAWEI-B2368-52AA01	WPA2-PSK mixed	

The following table describes the Labels in this screen.

Table 5-4 Network Settings > Wireless > More AP

Label	Description
#	This is the index number of the entry.
Active	This field indicates whether this SSID is active. A yellow bulb signifies that this SSID is active. A gray bulb signifies that this SSID is not active.
SSID	An SSID profile is the set of parameters relating to one of the LTE Device's BSSs. The SSID (Service Set IDentifier) identifies the Service Set with which a wireless device is associated. This field displays the name of the wireless profile on the network. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
Security	This field indicates the security mode of the SSID profile.
Modify	Click the Edit icon to configure the SSID profile.

5.3.1 Edit More AP

Use this screen to edit an SSID profile. Click the **Edit** icon next to an SSID in the **More AP** screen. The following screen displays.

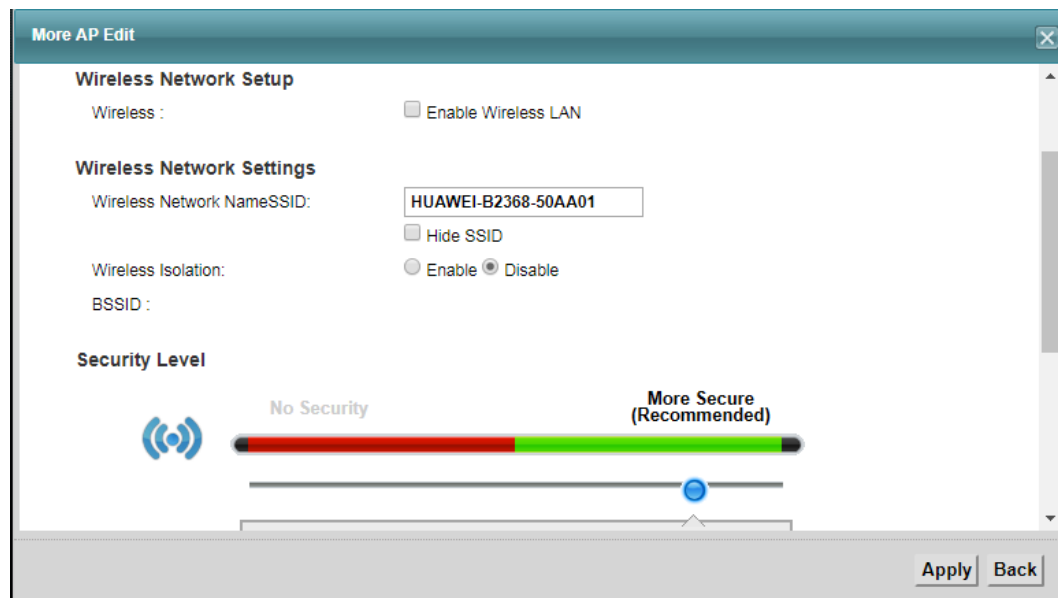
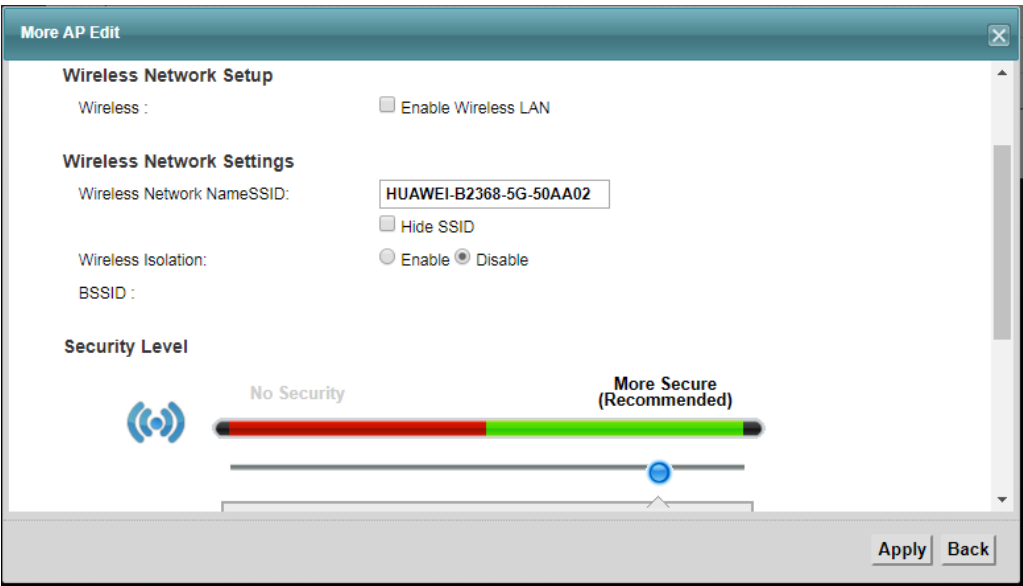
Figure 5-7 Wireless > More AP: Edit

Figure 5-8 Wireless 5G > More AP: Edit



The following table describes the fields in this screen.

Table 5-5 Wireless > More AP: Edit

Label	Description
Wireless Network Setup	
Wireless	Select the Enable Wireless LAN check box to activate the wireless LAN.
Wireless Network Settings	
Wireless Network NameSSID	The SSID (Service Set Identity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Wireless Isolation	Select this to keep the wireless clients in this SSID from communicating with each other directly through the Router.
BSSID	This shows the MAC address of the wireless interface on the LTE Device when wireless LAN is enabled.
Security Level	

Label	Description
Security Mode	Select More Secure (WPA(2)-PSK) to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the LTE Device. After you select to use a security, additional options appears in this screen. Or you can select No Security to allow any client to associate this network without any data encryption or authentication. See 5.2.1 More Secure (WPA(2)-PSK) for more details about this field.
Apply	Click Apply to save your changes.
Back	Click Back to exit this screen without saving.

5.4 The WPS Screen

Use this screen to configure WiFi Protected Setup (WPS) on your LTE Device.

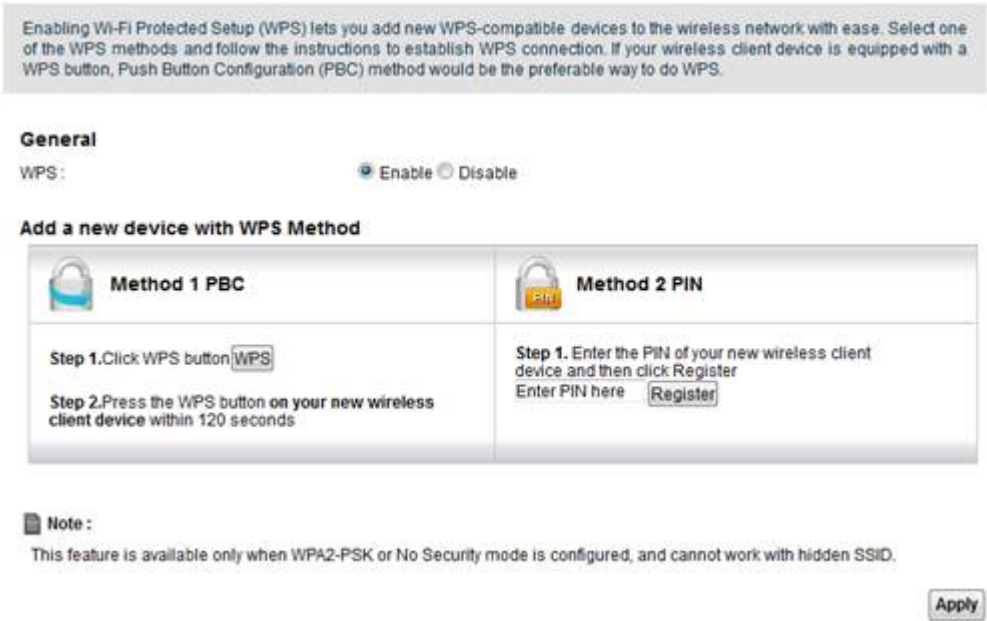
WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Set up each WPS connection between two devices. Both devices must support WPS. See [5.5.5 WiFi Protected Setup \(WPS\)](#) for more information about WPS.

NOTE

The LTE Device applies the security settings of the **SSID1** profile (see [5.1.2 Before You Begin](#)). If you want to use the WPS feature, make sure you have set the security mode of **SSID1** to **WPA2-PSK** or **No Security**. Also, do not hide **SSID1**.

Click **Network Setting > Wireless** (or **Wireless 5G**) > **WPS**. The following screen displays. Select **Enable** and click **Apply** to activate the WPS function. Then you can configure the WPS settings in this screen.

Figure 5-9 Network Setting > Wireless > WPS



The following table describes the Labels in this screen.

Table 5-6 Network Setting > Wireless > WPS

Label	Description
Enable WPS	Select Enable to activate WPS on the LTE Device.
Add a new device with WPS Method	
Method 1 PBC	Use this section to set up a WPS wireless network using Push Button Configuration (PBC).
WPS	Click this button to add another WPS-enabled wireless device (within wireless range of the LTE Device) to your wireless network. This button may either be a physical button on the outside of device, or a menu button similar to the WPS button on this screen. Note: You must press the other wireless device's WPS button within two minutes of pressing this button.
Method 2 PIN	Use this section to set up a WPS wireless network by entering the PIN (Personal Identification Number) of the client into the LTE Device.
Register	Enter the PIN of the device that you are setting up a WPS connection with and click Register to authenticate and add the wireless device to your wireless network. You can find the PIN either on the outside of the device, or by checking the device's settings. Note: You must also activate WPS on that device within two minutes to have it present its PIN to the LTE Device.

Label	Description
Apply	Click Apply to save your changes.

5.5 Technical Reference

This section discusses wireless LANs in depth.

5.5.1 Wireless Security Overview

By their nature, radio communications are simple to intercept. For wireless data networks, this means that anyone within range of a wireless network without security can not only read the data passing over the airwaves, but also join the network. Once an unauthorized person has access to the network, he or she can steal information or introduce malware (malicious software) intended to compromise the network. For these reasons, a variety of security systems have been developed to ensure that only authorized people can use a wireless data network, or understand the data carried on it.

These security standards do two things. First, they authenticate. This means that only people presenting the right credentials (often a username and password, or a "key" phrase) can access the network. Second, they encrypt. This means that the information sent over the air is encoded. Only people with the code key can understand the information, and only people who have been authenticated are given the code key.

These security standards vary in effectiveness. Some security standards are secure in themselves but can be broken if a user does not use them properly. For example, the WPA-PSK security standard is very secure if you use a long key which is difficult for an attacker's software to guess - for example, a twenty-letter long string of apparently random numbers and letters - but it is not very secure if you use a short key which is very easy to guess - for example, a three-letter word from the dictionary.

Because of the damage that can be done by a malicious attacker, it's not just people who have sensitive information on their network who should use security. Everybody who uses any wireless network should ensure that effective security is in place.

A good way to come up with effective security keys, passwords and so on is to use obscure information that you personally will easily remember, and to enter it in a way that appears random and does not include real words. For example, if your mother owns a 1970 Dodge Challenger and her favorite movie is Vanishing Point (which you know was made in 1971) you could use "70dodchal71vanpoi" as your security key.

The following sections introduce different types of wireless security you can set up in the wireless network.

SSID

Normally, the LTE Device acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the LTE Device does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized wireless devices to get the SSID. In addition, unauthorized wireless devices can still see the information that is sent in the wireless network.

MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.¹ A MAC address is usually written using twelve hexadecimal characters²; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the wireless network, see the device's User's Guide or other documentation.

You can use the MAC address filter to tell the LTE Device which devices are allowed or not allowed to use the wireless network. If a device is allowed to use the wireless network, it still has to have the correct information (SSID, channel, and security). If a device is not allowed to use the wireless network, it does not matter if it has the correct information.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized wireless devices to get the MAC address of an authorized device. Then, they can use that MAC address to use the wireless network.

1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
2. Hexadecimal characters are 0-9, A-F, and a-f.

User Authentication

Authentication is the process of verifying whether a wireless device is allowed to use the wireless network. You can make every user log in to the wireless network before using it. However, every device in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, you can store the user names and passwords for each user in a RADIUS server. This is a server used in businesses more than in homes. If you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized wireless devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

The types of encryption you can choose depend on the type of authentication.

Figure 5-10 Types of Encryption for Each Type of Authentication

Weakest	No Security
↕	WPA-PSK
Strongest	WPA2-PSK

You can choose no encryption, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every device in the wireless network supports. Suppose the wireless network has two devices. Device A only supports WPA-PSK,

and device B supports WPA-PSK and WPA2-PSK. Therefore, you should set up **WPA-PSK** in the wireless network.

 NOTE

It is recommended that wireless networks use **WPA-PSK** or **WPA2-PSK** encryption. The other types of encryption are better than none at all, but it is still possible for unauthorized wireless devices to figure out the original information pretty quickly.

When you select **WPA2-PSK** in your LTE Device, you can also select an option (**WPA compatible**) to support WPA-PSK as well. In this case, if some of the devices support WPA-PSK and some support WPA2-PSK, you should set up **WPA2-PSK** and select the **WPA compatible** option in the LTE Device.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every device in the wireless network must have the same key.

5.5.2 Signal Problems

Because wireless networks are radio networks, their signals are subject to limitations of distance, interference and absorption.

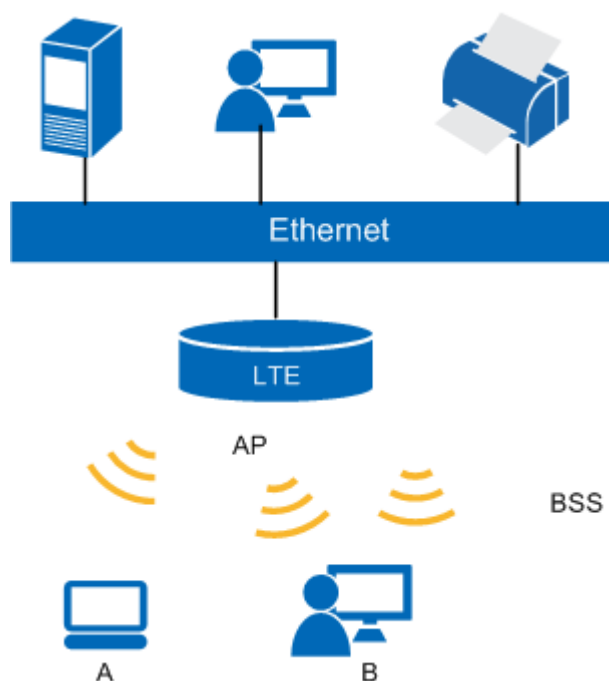
Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters such as electric motors or microwaves. Problems with absorption occur when physical objects (such as thick walls) are between the two radios, muffling the signal.

5.5.3 BSS

A Basic Service Set (BSS) exists when all communications between wireless stations or between a wireless station and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS traffic blocking is disabled, wireless station A and B can access the wired network and communicate with each other. When Intra-BSS traffic blocking is enabled, wireless station A and B can still access the wired network but cannot communicate with each other.

Figure 5-11 Basic Service set



5.5.4 MBSSID

Traditionally, you need to use different APs to configure different Basic Service Sets (BSSs). As well as the cost of buying extra APs, there is also the possibility of channel interference. The LTE Device's MBSSID (Multiple Basic Service Set Identifier) function allows you to use one access point to provide several BSSs simultaneously. You can then assign varying QoS priorities and/or security modes to different SSIDs.

Wireless devices can use different BSSIDs to associate with the same AP.

Notes on Multiple BSSs

- A maximum of eight BSSs are allowed on one AP simultaneously.
- You must use different keys for different BSSs. If two wireless devices have different BSSIDs (they are in different BSSs), but have the same keys, they may hear each other's communications (but not communicate with each other).
- MBSSID should not replace but rather be used in conjunction with 802.1x security.

5.5.5 WiFi Protected Setup (WPS)

Your LTE Device supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows

one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

5.5.5.1 Push Button Configuration

WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button. Take the following steps to set up WPS using the button.

- Step 1** Ensure that the two devices you want to set up are within wireless range of one another.
- Step 2** Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the LTE Device, see [5.4 The WPS Screen](#)).
- Step 3** Press the button on one of the devices (it doesn't matter which). For the LTE Device you must press the WPS button for more than ten seconds.
- Step 4** Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through a secure connection to the enrollee.

If you need to make sure that WPS worked, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

----End

5.5.5.2 PIN Configuration

The PIN method ensures that the connection is established between the devices you specify, not just the first two devices to activate WPS in range of each other. You need to log into the configuration interfaces of both devices to use the PIN method.

When you use the PIN method, you must enter the PIN the wireless client into the LTE Device. Then, when WPS is activated on the first device, it presents its PIN to the second device. If the PIN matches, one device sends the network and security information to the other, allowing it to join the network.

Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

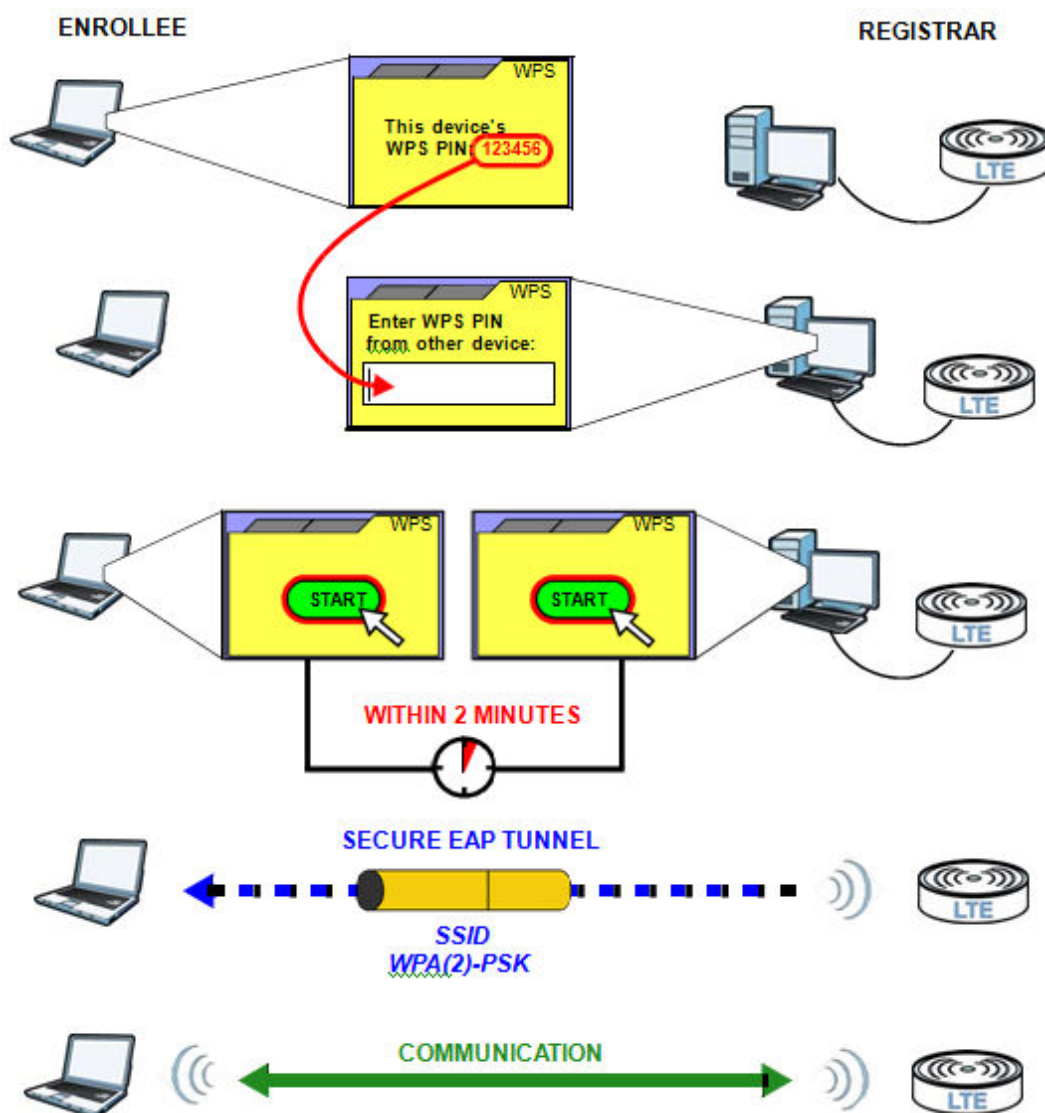
- Step 1** Ensure WPS is enabled on both devices.
- Step 2** Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this.
- Step 3** Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface.
- Step 4** Enter the client's PIN in the AP's configuration interface.
- Step 5** Start WPS on both devices within two minutes.
- Step 6** Use the configuration utility to activate WPS, not the push-button on the device itself.

Step 7 On a computer connected to the wireless client, try to connect to the Internet. If you can connect, WPS was successful.

If you cannot connect, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful

The following figure shows a WPS-enabled wireless client (installed in a notebook computer) connecting to the WPS-enabled AP via the PIN method.

Figure 5-12 Example WPS Process: PIN Method



----End

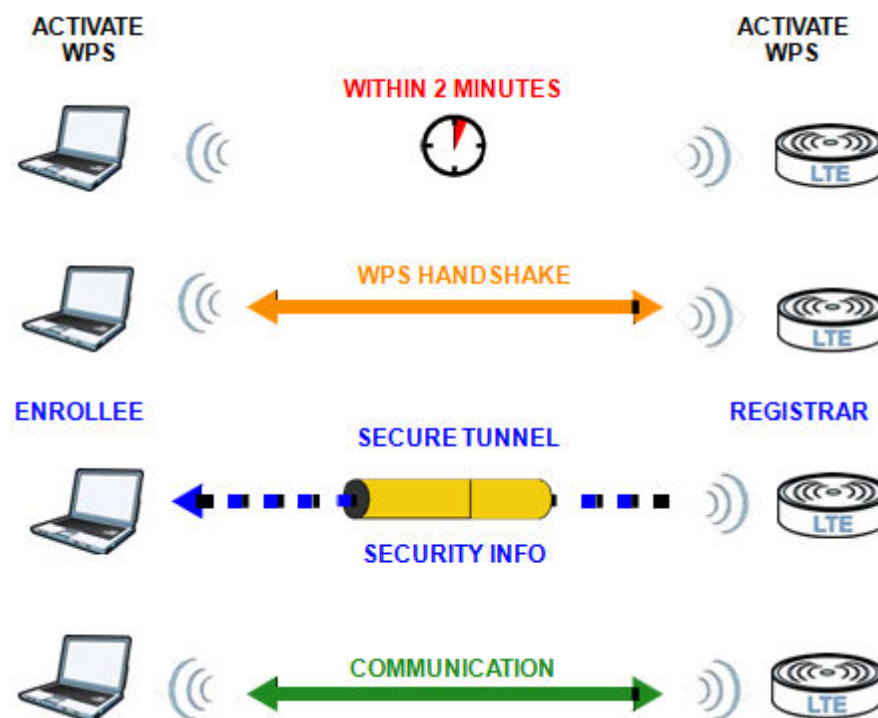
5.5.5.3 How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings). The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the

network name (SSID) and the WPA-PSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. WPS 2.0 does not allow the use of WPA-PSK. If the registrar is already part of a network, it sends the existing information. If not, it generates the SSID and WPA(2)-PSK randomly.

The following figure shows a WPS-enabled client (installed in a notebook computer) connecting to a WPS-enabled access point.

Figure 5-13 Example WPS Process: PIN Method



The roles of registrar and enrollee last only as long as the WPS setup process is active (two minutes). The next time you use WPS, a different device can be the registrar if necessary.

The WPS connection process is like a handshake; only two devices participate in each WPS transaction. If you want to add more devices you should repeat the process with one of the existing networked devices and the new device.

Note that the access point (AP) is not always the registrar, and the wireless client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled wireless clients.

5.5.5.4 Limitations of WPS

WPS has some limitations of which you should be aware.

- WPS works in Infrastructure networks only (where an AP and a wireless client communicate). It does not work in Ad-Hoc networks (where there is no AP).
- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously; you must enroll one after the other.

For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way.

- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices. Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).

- WPS 2.0 does not allow the use of WPA-PSK.
- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the "correct" enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

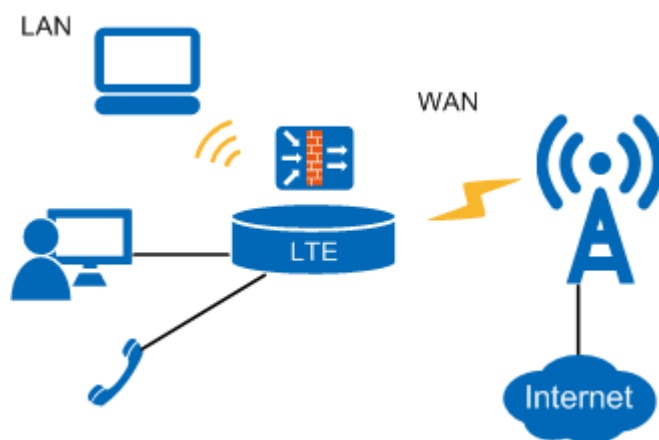
You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point's configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the access point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a Label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.

6 Home Networking

6.1 Overview

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is usually located in one immediate area such as a building or floor of a building.

The LAN screens can help you configure a LAN DHCP server and manage IP addresses.



6.1.1 What You Need To Know

The following terms and concepts may help as you read this chapter.

6.1.1.1 About LAN IP Address

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number. This is known as an Internet Protocol address.

Subnet Mask

The subnet mask specifies the network number portion of an IP address. Your LTE Device will compute the subnet mask automatically based on the IP address that you entered. You

don't need to change the subnet mask computed by the LTE Device unless you are instructed to do otherwise.

DHCP

DHCP (Dynamic Host Configuration Protocol) allows clients to obtain TCP/IP configuration at start-up from a server. This LTE Device has a built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

DNS

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The DNS server addresses you enter when you set up DHCP are passed to the client machines along with the assigned IP address and subnet mask.

6.1.1.2 About UPnP

How do I know if I'm using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the LTE Device allows multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

6.2 The LAN Setup Screen

Click **Network Setting > Home Networking** to open the **LAN Setup** screen. Use this screen to set the Local Area Network IP address and subnet mask of your LTE Device and configure the DNS server information that the LTE Device sends to the DHCP client devices on the LAN.

Figure 6-1 Network Setting > Home Networking > LAN Setup (DHCP Enabled)

The LAN IP address here is the IP address for you to login the configuration interface. The DHCP Server settings decides the rules how it assigns IP addresses to the LAN clients on your network.

LAN IP Setup

IP Address :

192.168.1.1

Subnet Mask :

255.255.255.0

DHCP Server State

DHCP :

☒ Enable

☐ Disable

DHCP Lease Time:

0

Day

12

Hour

0

Min (2 minutes to 31 days)

IP Addressing Values

IP Pool Starting Address :

192.168.1.33

Pool Size :

32

DNS Values

DNS Server 1 :

DNS Proxy

192.168.1.1

DNS Server 2 :

None

DNS Server 3 :

None

Apply

Cancel

Figure 6-2 Network Setting > Home Networking > LAN Setup (DHCP Disabled)

LAN IP Setup

IP Address :

192.168.1.1

Subnet Mask :

255.255.255.0

DHCP Server State

DHCP :

☐ Enable

☒ Disable

DHCP Relay State

DHCP Relay

☐ Enable

☒ Disable

DHCP Relay Server :

Apply

Cancel

The following table describes the fields in this screen.

Table 6-1 Network Setting > Home Networking > LAN Setup

Label	Description
LAN IP Setup	

Issue 03 (2019-01-31)

Copyright © Huawei Technologies Co., Ltd.

59

Label	Description
IP Address	Enter the LAN IP address you want to assign to your LTE Device in dotted decimal notation, for example, 192.168.1.1 (factory default).
Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your LTE Device automatically computes the subnet mask based on the IP address you enter, so do not change this field unless you are instructed to do so.
DHCP Server State	
DHCP	Select Enable to have your LTE Device assign IP addresses, an IP default gateway and DNS servers to LAN computers and other devices that are DHCP clients. If you select Disable, you need to manually configure the IP addresses of the computers and other devices on your LAN. When DHCP is used, the following fields need to be set.
DHCP Lease Time	Set how long DHCP clients will own the IP address obtained from the DHCP server. For example, 0 Day 12 hour 0 Min (factory default). The minimum DHCP Lease Time is 2 minutes, and the maximum DHCP Lease Time is 31 Days.
IP Addressing Values	
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
DNS Values	
DNS Server 1-3	Select From ISP if your ISP dynamically assigns DNS server information (and the LTE Device's WAN IP address). Select DNS-Proxy to have the LTE Device send its own address to the LAN clients for them to use as the DNS server. Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose User-Defined, but leave the IP address set to 0.0.0.0, User-Defined changes to None after you click Apply. If you set a second choice to User-Defined, and enter the same IP address, the second User-Defined changes to None after you click Apply. Select None if you do not want to configure DNS servers. You must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
DHCP Relay State	

Label	Description
DHCP Relay	DHCP relay fields display when you disable DHCP. Select Enable if you have the IP address of a DHCP server to use. Select Disable if you do not have the IP address of a DHCP server to use. When DHCP relay is used, the following field needs to be set.
DHCP Relay Server	Enter the IP address of the DHCP server to use.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

6.3 The Static DHCP Screen

This table allows you to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

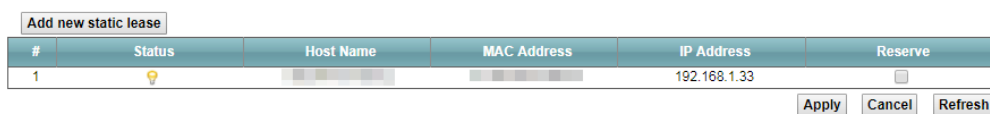
Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

6.3.1 Before You Begin

Find out the MAC addresses of your network devices if you intend to add them to the **Static DHCP** screen.

Use this screen to change your LTE Device's static DHCP settings. Click **Network Setting > Home Networking > Static DHCP** to open the following screen.

Figure 6-3 Network Setting > Home Networking > Static DHCP



Add new static lease					
#	Status	Host Name	MAC Address	IP Address	Reserve
1				192.168.1.33	☐

Apply Cancel Refresh

The following table describes the Labels in this screen.

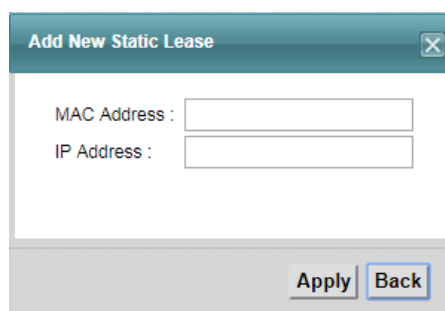
Table 6-2 Network Setting > Home Networking > Static DHCP

Label	Description
Add new static lease	Click this to add a new static DHCP entry.
#	This is the index number of the entry.

Label	Description
Status	This field displays whether the client is connected to the LTE Device.
Host Name	This field displays the client host name.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
IP Address	This field displays the IP address relative to the # field listed above.
Reserve	Select the check box in the heading row to automatically select all check boxes or select the check boxes in each entry to have the LTE Device always assign the selected entries' IP addresses to the corresponding MAC addresses (and host names). You can select up to 128 entries in this table.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.
Refresh	Click Refresh to reload the DHCP table.

If you click **Add new static lease** in the **Static DHCP** screen, the following screen displays.

Figure 6-4 Static DHCP: Add



The following table describes the Labels in this screen.

Table 6-3 Static DHCP: Add

Label	Description
MAC Address	Enter the MAC address of a computer on your LAN.
IP Address	Enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify.

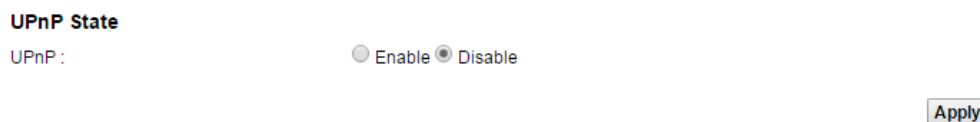
Label	Description
Apply	Click Apply to save your changes.
Back	Click Back to exit this screen without saving.

6.4 The UPnP Screen

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

Use the following screen to configure the UPnP settings on your LTE Device. Click **Network Setting > Home Networking > UPnP** to display the screen shown next.

Figure 6-5 Network Setting > Home Networking > UPnP



The following table describes the Labels in this screen.

Table 6-4 Network Settings > Home Networking > UPnP

Label	Description
UPnP	Select Enable to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the LTE Device's IP address (although you must still enter the password to access the web configurator).
Apply	Click Apply to save your changes.

6.5 The UPnP List Screen

When you enable UPnP, this screen lists the UPnP-enabled devices and/or software the LTE Device finds on your network.

Click **Network Setting > Home Networking > UPnP List** to display the screen shown next.

Figure 6-6 Network Setting > Home Networking > UPnP List

#	Protocol	Destination IP Address	External Port	Internal Port
Refresh				

The following table describes the Labels in this screen.

Table 6-5 Network Settings > Home Networking > UPnP List

Label	Description
#	The index number of the entry in the list.
Protocol	The IP protocol the particular UPnP-enabled device or software is using on your network.
Destination IP Address	The IP address of the UPnP-enabled device or software.
External Port	The external (WAN) port that the LTE Device uses for the application.
Internal Port	The internal (LAN) port that the LTE Device uses for the application.
Refresh	Click Refresh to save your changes.

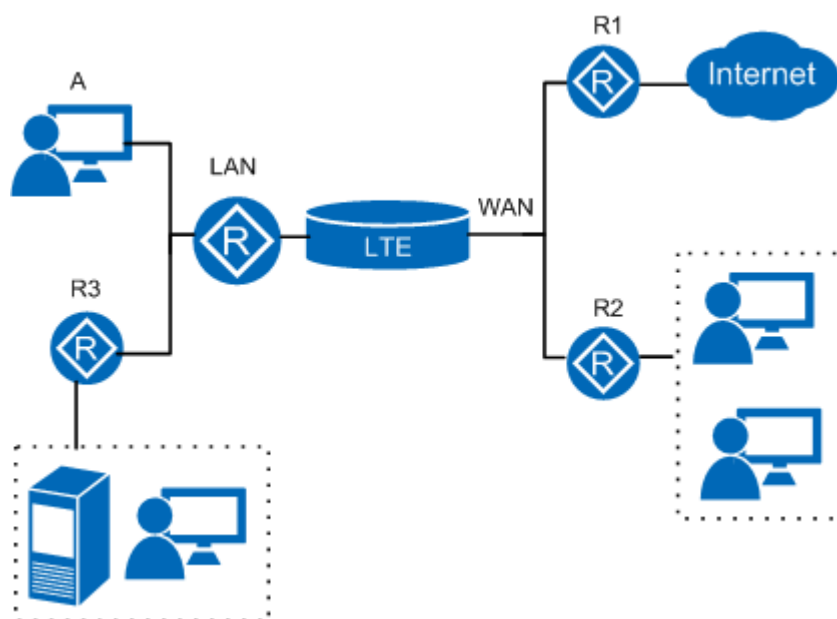
7 Static Route

7.1 Overview

The LTE Device usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the LTE Device send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the LTE Device's LAN interface. The LTE Device routes most traffic from **A** to the Internet through the LTE Device's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the LAN.

Figure 7-1 Example of Static Routing Topology



7.2 Configuring Static Route

Use this screen to view and configure IPv4 static routes on the LTE Device. Click **Network Setting** > **Static Route** to open the following screen.

Figure 7-2 Network Setting > Static Route

Add New Static Route								
#	Active	Status	Name	Destination IP	Gateway	Subnet Mask	Interface	Modify

The following table describes the Labels in this screen.

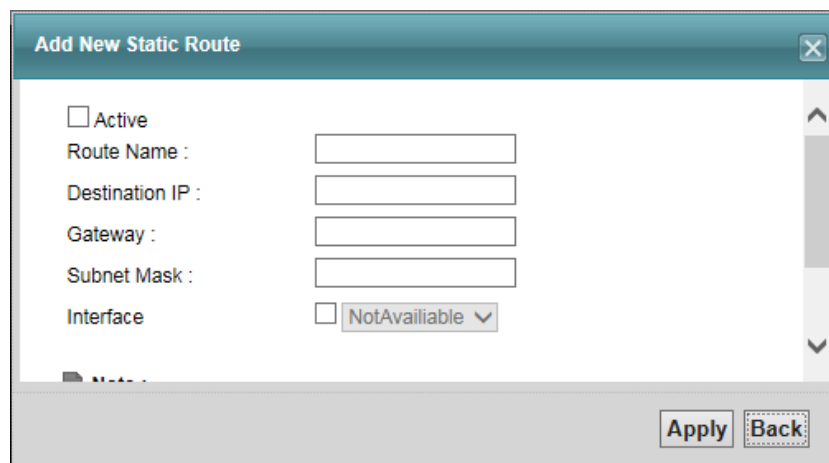
Table 7-1 Network Setting > Static Route

Label	Description
Add New Static Route	Click this to set up a new IPv4 static route on the LTE Device.
#	This is the number of an individual static route.
Active	This indicates whether the route is active or not. A yellow bulb signifies that this static route is active. A gray bulb signifies that this static route is not active.
Status	This shows whether the static route is currently in use or not. A yellow bulb signifies that this static route is in use. A gray bulb signifies that this static route is not in use.
Route Name	This is the name that describes or identifies this route.
Destination IP	This parameter specifies the IPv4 IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IPv4 IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Subnet Mask	This parameter specifies the IP network subnet mask of the final destination.
Interface	This indicates which interface handles the traffic forwarded by this route.
Modify	Click the Edit icon to go to the screen where you can set up a static route on the LTE Device. Click the Delete icon to remove a static route from the LTE Device.

7.2.1 Add/Edit Static Route

Click **Add New Static Route** in the **Static Route** screen or click the **Edit** icon next to a rule. The following screen appears. Use this screen to configure the required information for a static route.

Figure 7-3 Static Route: Add/Edit



The following table describes the Labels in this screen.

Table 7-2 Static Route: Add/Edit

Label	Description
Active	Click this to activate this static route.
Route Name	Enter the name of the IP static route.
Destination IP	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
Gateway	You can decide if you want to forward packets to a gateway IP address or a bound interface. If you want to configure a gateway IP address, enter the IP address of the next-hop gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Subnet Mask	Enter the subnet mask here.
Interface	You can decide if you want to forward packets to a gateway IP address or a specific interface. If you want to select an individual interface, select the check box and choose an interface through which the traffic is sent.

Label	Description
Apply	Click Apply to save your changes.
Back	Click Back to exit this screen without saving.

8 Network Address Translation (NAT)

8.1 Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

8.1.1 What You Need To Know

The following terms and concepts may help as you read this chapter.

Inside/Outside and Global/Local

Inside/outside denotes where a host is located relative to the LTE Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

NAT

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host.

Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

Finding Out More

See Section [8.6 Technical Reference](#) for advanced technical information on NAT.

8.2 The Port Forwarding Screen

Use the **Port Forwarding** screen to forward incoming service requests to the server(s) on your local network.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

Please refer to RFC 1700 for further information about port numbers.

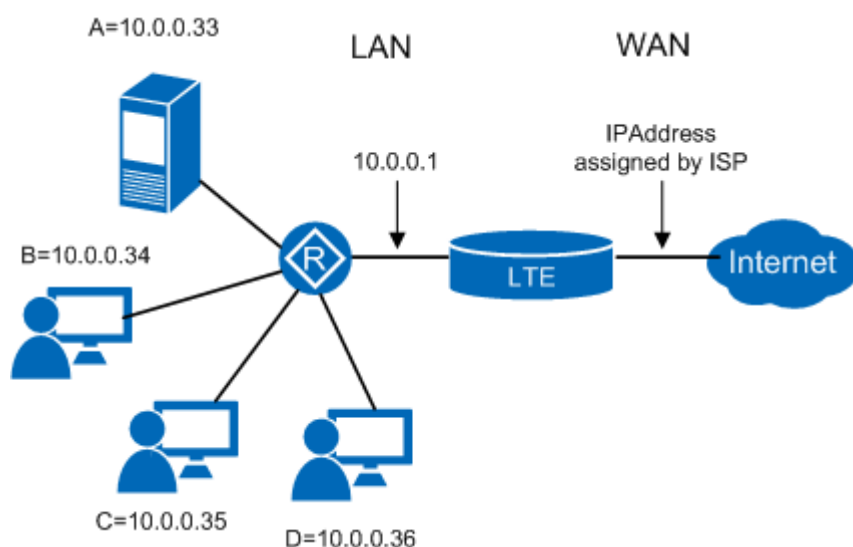
NOTE

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Configuring Servers Behind Port Forwarding (Example)

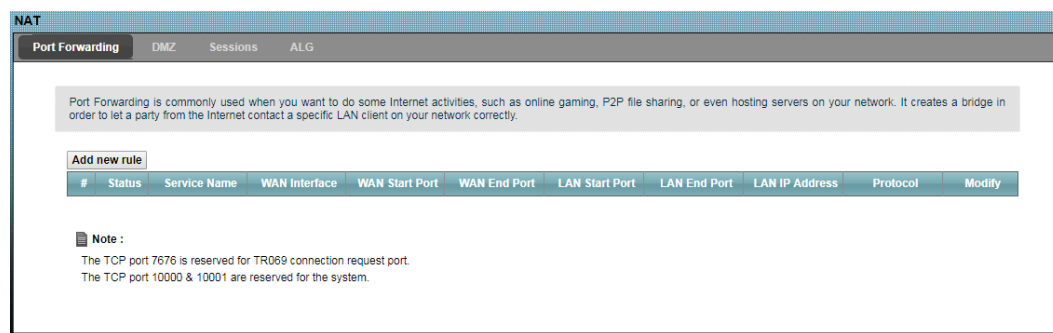
Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 10.0.0.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 8-1 Multiple Servers Behind NAT Example



8.2.1 The Port Forwarding Screen

Click **Network Setting > NAT** to open the **Port Forwarding** screen.

Figure 8-2 Network Setting > NAT > Port Forwarding

The following table describes the fields in this screen.

Table 8-1 Network Setting > NAT > Port Forwarding

Label	Description
Add new rule	Click this to add a new port forwarding rule.
#	This is the index number of the entry.
Status	This field indicates whether the rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Service Name	This is the service's name. This shows User Defined if you manually added a service. You can change this by clicking the edit icon.
WAN Interface	This shows the WAN interface through which the service is forwarded.
WAN Start Port	This is the first external port number that identifies a service.
WAN End Port	This is the last external port number that identifies a service.
LAN Start Port	This is the first internal port number that identifies a service.
LAN End Port	This is the last internal port number that identifies a service.
LAN IP Address	This is the server's IP address.
Protocol	This shows the IP protocol supported by this virtual server, whether it is TCP, UDP, or TCP/UDP.
Modify	Click the Edit icon to edit the port forwarding rule. Click the Delete icon to delete an existing port forwarding rule. Note that subsequent address mapping rules move up by one when you take this action.

8.2.2 The Port Forwarding Edit Screen

This screen lets you create or edit a port forwarding rule. Click **Add new rule** in the **Port Forwarding** screen or the **Edit** icon next to an existing rule to open the following screen.

Figure 8-3 Port Forwarding: Add/Edit

Add new rule

Service Name :

User Defined

WAN Interface :

Data

WAN Start Port :

WAN End Port :

LAN Start Port :

LAN End Port :

LAN IP Address :

Protocol :

TCP

Note :

To translate the port to internal server, enter the translated port number of

Apply

Back

The following table describes the Labels in this screen.

Table 8-2 Port Forwarding: Add/Edit

Label	Description
Service Name	Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on).
WAN Interface	This is the WAN interface through which the service is forwarded.
WAN Start Port	Enter the original destination port for the packets. To forward only one port, enter the port number again in the External End Port field. To forward a series of ports, enter the start port number here and the end port number in the External End Port field.
WAN End Port	Enter the last port of the original destination port range. To forward only one port, enter the port number in the External Start Port field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the External Start Port field above.

Label	Description
LAN Start Port	This shows the port number to which you want the LTE Device to translate the incoming port. For a range of ports, enter the first number of the range to which you want the incoming ports translated.
LAN End Port	This shows the last port of the translated port range.
LAN IP Address	Enter the inside IP address of the virtual server here.
Protocol	Select the protocol supported by this virtual server. Choices are TCP , UDP , or TCP/UDP .
Apply	Click Apply to save your changes.
Back	Click Back to return to the previous screen without saving.

8.3 The DMZ Screen

Use this page to set the IP address of your network DMZ (if you have one) for the LTE Device. All incoming packets received by this LTE Device's WAN interface will be forwarded to the default server you set.

Click **Network Setting > NAT > DMZ** to display the following screen.

NOTE

The configuration you set in this screen takes priority than the **Network Setting > NAT > Port Forwarding** screen.

Figure 8-4 Network Setting > NAT > DMZ

The following table describes the fields in this screen.

Table 8-3 Network Setting > NAT > DMZ

Label	Description
Default Server Address	Enter the IP address of your network DMZ host, if you have one. 0.0.0.0 means this feature is disabled.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

8.4 The Sessions Screen

Use the **Sessions** screen to limit the number of concurrent NAT sessions each client can use. Click **Network Setting > NAT > Sessions** to display the following screen.

Figure 8-5 Network Setting > NAT > Sessions



The following table describes the fields in this screen.

Table 8-4 Network Setting > NAT > Sessions

Label	Description
MAX NAT Sessions Per Host	Use this field to set a common limit to the number of concurrent NAT sessions each client computer can have. If only a few clients use peer to peer applications, you can raise this number to improve their performance. With heavy peer to peer application use, lower this number to ensure no single client uses too many of the available NAT sessions.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

8.5 The ALG Screen

Use the **ALG** screen to enable or disable SIP Application Layer Gateway (ALG) on the LTE Device. Click **Apply** to save your change.

The SIP ALG allows SIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream. When the LTE Device registers with the SIP register server, the SIP ALG translates the LTE Device's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if you enable the SIP ALG.

For the LTE environment, the LTE interface may experience heavy overhead when sending SIP re-registration requests due to SIP server NAT session timeout. This default NAT session timeout value (3600 seconds) helps to decrease the chance of this happening.

Figure 8-6 Network Setting > NAT > ALG

8.6 Technical Reference

This section provides some technical background information about the topics covered in this chapter.

8.6.1 NAT Definitions

Inside/outside denotes where a host is located relative to the LTE Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 8-5 NAT Definitions

ITEM	Description
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

NAT never changes the IP address (either local or global) of an outside host.

8.6.2 What NAT Does

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination

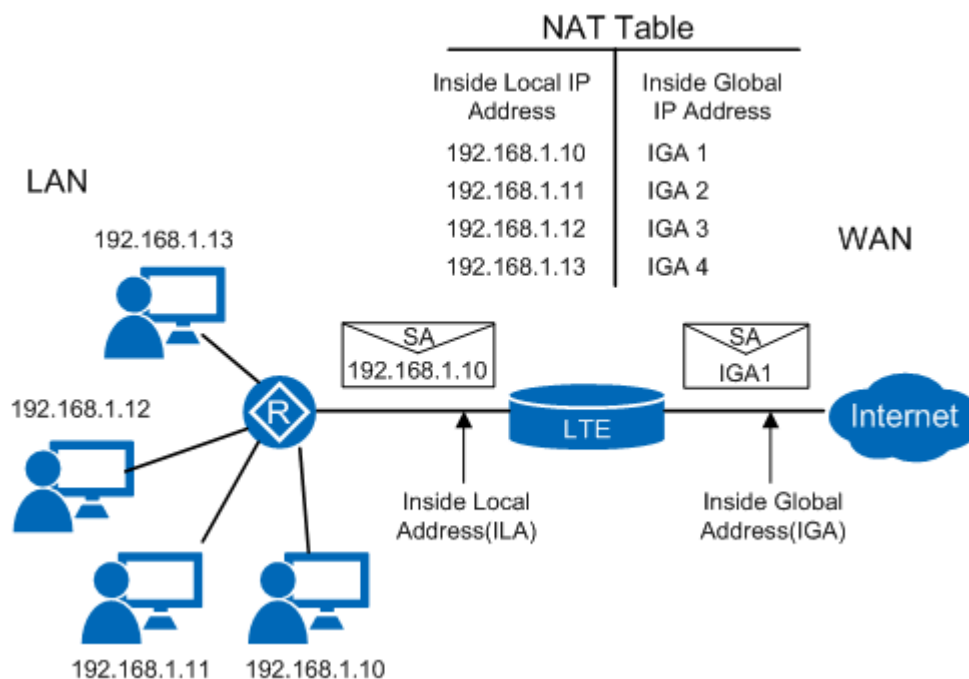
address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a Telnet server, on your local network and make them accessible to the outside world. If you do not define any servers, NAT offers the additional benefit of firewall protection. With no servers defined, your LTE Device filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631, The IP Network Address Translator (NAT)*.

8.6.3 How NAT Works

Each packet has two addresses—a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The LTE Device keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

Figure 8-7 How NAT Works



9 Dynamic DNS

9.1 Overview

This chapter discusses how to configure your LTE Device to use Dynamic DNS. Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in applications such as NetMeeting and CU-SeeMe). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org or www.no-ip.com. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

9.1.1 What You Need To Know

DYNDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

9.2 The Dynamic DNS Screen

10 Firewall

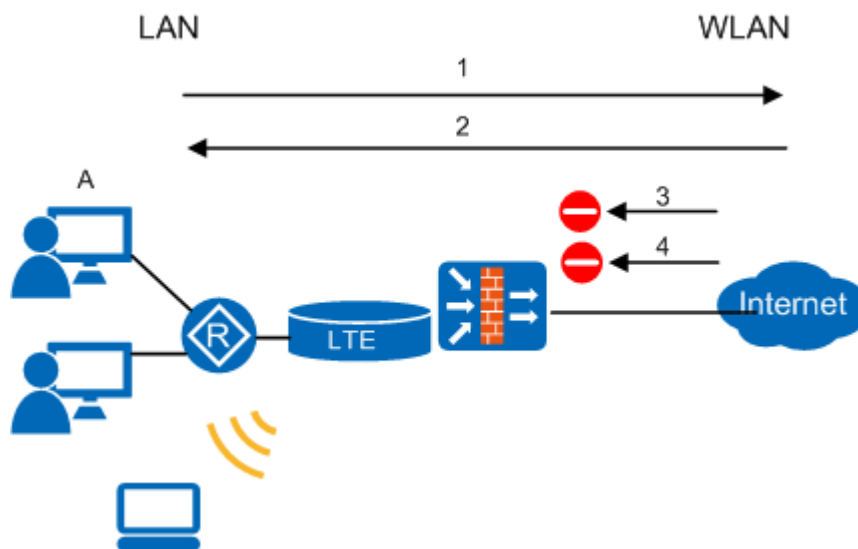
10.1 Overview

Use the LTE Device firewall screens to enable and configure the firewall that protects your LTE Device and network from attacks by hackers on the Internet and control access to it. By default the firewall:

- Allows traffic that originates from your LAN and WLAN computers to go to all other networks.
- Blocks traffic that originates on other networks from going to the LAN and WLAN.

The following figure illustrates the default firewall action. User A can initiate an IM (Instant Messaging) session from the LAN to the WAN (1). Return traffic for this session is also allowed (2). However other traffic initiated from the WAN is blocked (3 and 4).

Figure 10-1 Default Firewall Action



10.1.1 What You Need to Know

DoS

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The LTE Device is pre-configured to automatically detect and thwart all known DoS attacks.

Firewall

The LTE Device's firewall feature physically separates the LAN/WLAN and the WAN and acts as a secure gateway for all data passing between the networks.

It is designed to protect against Denial of Service (DoS) attacks when activated. The LTE Device's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The LTE Device can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network.

The LTE Device is installed between the LAN/WLAN and the connection to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN..

The LTE Device's PoE (Power over Ethernet) Ethernet WAN port and Ethernet LAN ports physically separate the network into two areas. The WAN (Wide Area Network) port attaches to the ODU for the Internet connection.

The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP and the World Wide Web. However, "inbound access" is not allowed (by default) unless the remote host is authorized to use a specific service.

NOTE

Enabling the firewall may impact the system performance.

ICMP

Internet Control Message Protocol (ICMP) is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.

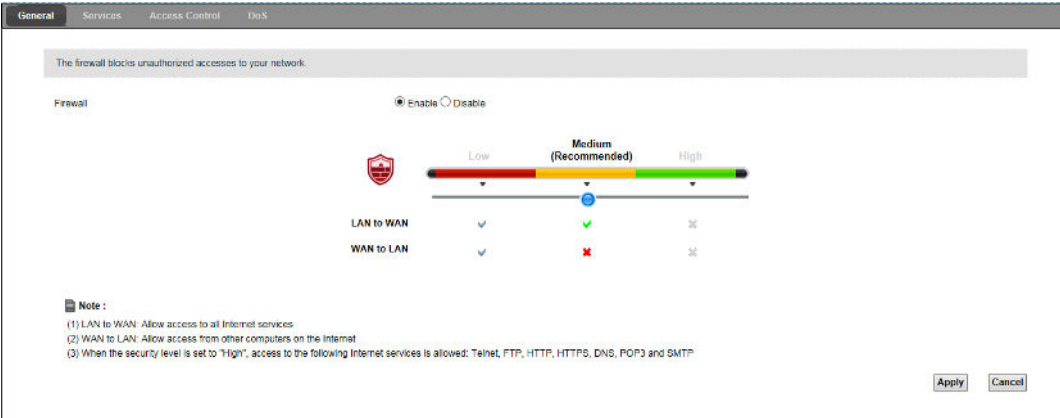
Finding Out More

See Section [10.6 Firewall Technical Reference](#) for more information on firewall.

10.2 The General Screen

Use this screen to enable or disable the LTE Device's firewall. Click **Security > Firewall** to open the **General** screen.

Figure 10-2 Security > Firewall > General



The following table describes the Labels in this screen.

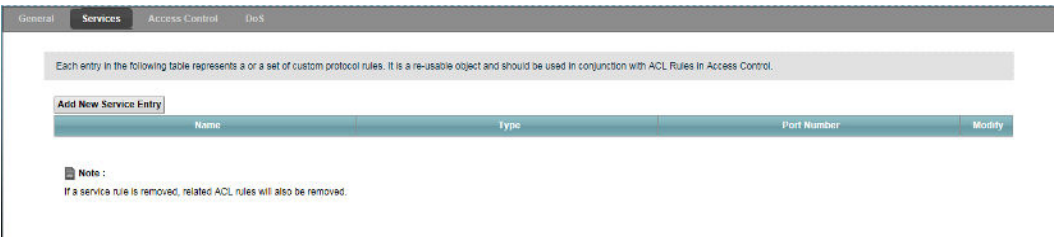
Table 10-1 Security > Firewall > General

Label	Description
Firewall	Select Enable to activate the firewall. The LTE Device performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Low Medium, High	Select Low to have the firewall allow both LAN-to-WAN and WAN-to- LAN traffic to flow through the LTE Device. Select Medium to have the firewall only allow traffic sent from the LAN to the WAN. All traffic sent or access from the WAN will be blocked. Select High to have the firewall only allow Telnet, FTP, HTTP, HTTPS, DNS, POP3, and SMTP traffic sent from the LAN to the WAN. Other traffic will be blocked.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

10.3 The Services Screen

Use this screen to view the configured service list. To access this screen, click **Security > Firewall > Services**. You have to configure at least one service in this screen before configuring the **Security > Firewall > Access Control > Add New ACL Rule/Edit** screen.

Figure 10-3 Security > Firewall > Services



Each field is described in the following table.

Table 10-2 Security > Firewall > Services

Label	Description
Add New Service Entry	Click this to define a new service.
Name	This is the name of a configured service.
Type	This is the protocol type (TCP, UDP, ICMP or Others) of the service.
Port Number	This displays a range of port numbers that defines the service.
Modify	Click the Edit icon to edit the service. Click the Delete icon to delete the service. Note that subsequent rules move up by one when you take this action. Deleting a service rule also deletes the related ACL rules which are configured in the Security > Firewall > Access Control screen.

10.3.1 The Add New Services Entry Screen

Use this screen to configure a service that you want to use in an ACL rule in the **Security > Firewall > Access Control > Add New ACL Rule/Edit** screen. To access this screen, click **Security > Firewall > Services** and then the **Add New Service Entry** button.

Figure 10-4 Security > Firewall > Services > Add New Service Entry

Add New Service Entry

Name:

Type:

TCP

Protocol Number:

(0-255)

Source Port:

Single

-

Destination Port:

Single

-

Apply

Back

Each field is described in the following table.

Table 10-3 Security > Firewall > Services > Add New Service Entry

Label	Description
Name	Type a descriptive name for the service.
Type	Select the protocol type (TCP , UDP or ICMP or Others) of the service.
Protocol Number	Enter the protocol number of the service type.
Source Port, Destination Port	The source port defines from which port number(s) the service traffic is sent. The destination port defines the port number(s) the destination hosts use to receive the service traffic. Select Single if the service uses one and only one source or destination port, then enter the port number. Select Multiple if the service uses two or more source or destination ports, then enter a port range. For example, suppose you want to define the Gnutella service. Select TCP type and enter a port range of 6345-6349.
Apply	Click Apply to save your changes.
Back	Click Back to exit this screen without saving your changes.

10.4 The Access Control Screen

Click **Security > Firewall > Access Control** to display the following screen. This screen displays a list of the configured incoming or outgoing filtering rules.

Figure 10-5 Security > Firewall > Access Control

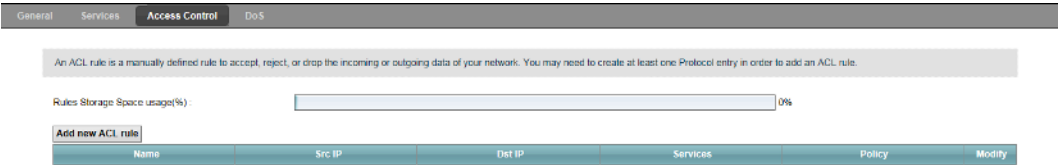
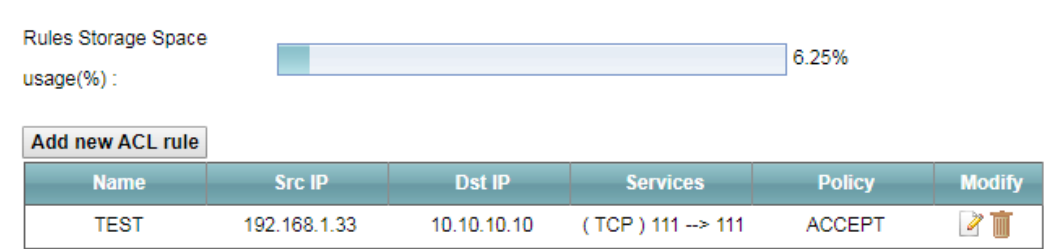


Figure 10-6 Security > Firewall > Access Control (After adding an ACL rule)



Each field is described in the following table.

Table 10-4 Security > Firewall > Access Control

Label	Description
Rules Storage Space usage(%)	This bar shows the percentage of the LTE Device's space has been used. If the usage is almost full, you may need to remove an existing filter rule before you create a new one.
Add new ACL rule	Click this to go to add a filter rule for incoming or outgoing IP traffic.
Name	This displays the name of the rule.
Src IP	This displays the source IP addresses to which this rule applies. Please note that a blank source address is equivalent to Any .
Dst IP	This displays the destination IP addresses to which this rule applies. Please note that a blank destination address is equivalent to Any .
Services	This displays the protocol type and a port range that define the service to which this rule applies.
Policy	This field displays whether the rule silently discards packets (DROP), discards packets and sends a TCP reset packet or an ICMP destination- unreachable message to the sender (REJECT) or allows the passage of packets (ACCEPT).
Modify	Click the Edit icon to edit the rule. Click the Delete icon to delete an existing rule. Note that subsequent rules move up by one when you take this action.

10.4.1 The Add New ACL Rule/Edit Screen

Click **Add New ACL Rule** or the **Edit** icon next to an existing ACL rule in the **Access Control** screen. The following screen displays.

Figure 10-7 Security > Firewall > Access Control > Add New ACL Rule/Edit

Add new ACL rule

Filter Name:

Source Address Type:

Single

Source IP Address Start:

Source IP Address End:

Destination Address Type:

Single

Destination IP Address Start:

Destination IP Address End:

Select Protocol:

Select Service

Protocol:

TCP

Protocol Number:

(0-255)

Source Port:

Single

-

Destination Port:

Single

-

Policy:

ACCEPT

Direction:

LAN to DEVICE

Apply

Back

Each field is described in the following table.

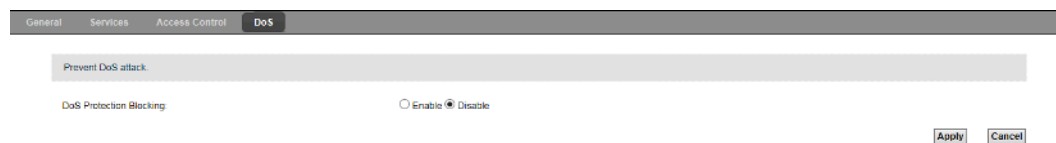
Table 10-5 Security > Firewall > Access Control > Add New ACL Rule/Edit

Label	Description
Filter Name	Enter a descriptive name of up to 16 alphanumeric characters, not including spaces, underscores, and dashes. You must enter the filter name to add an ACL rule. This field is read-only if you are editing the ACL rule.
Source Address Type	Select Single or Range depending on whether you want to enter a single or a range of source IP addresses to which the ACL rule applies. Select Any to indicate any source IP address.
Source IP Address Start	Enter an IP address or the starting IP address of the source IP range.
Source IP Address End	Enter the ending IP address of the source IP range.

Label	Description
Destination Address Type	Select Single or Range depending on whether you want to enter a single or a range of destination IP addresses to which the ACL rule applies. Select Any to indicate any destination IP address.
Destination IP Address Start	Enter an IP address or the starting IP address of the destination IP range.
Destination IP Address End	Enter the ending IP address of the destination IP range.
Select Protocol	Select the name of a configured service or Select Service to define a new service in this screen.
Protocol	This field is available when you Select Service in Select Protocol . Choose the protocol type (TCP , UDP , ICMP or Others) of the service.
Protocol Number	This field is available when you select Others in Protocol . Enter the protocol number of the service type to which this ACL rule applies.
Source Port	This field is displayed only when you Select Service in Select Protocol and TCP or UDP in Protocol . Select Single or Range and then enter a single port number or the range of port numbers of the source. Select Any to indicate any source port.
Destination Port	This field is displayed only when you Select Service in Select Protocol and TCP or UDP in Protocol . Select Single or Range and then enter a single port number or the range of port numbers of the destination. Select Any to indicate any destination port.
Policy	Use the drop-down list box to select whether to silently discard (DROP), deny and send an ICMP destination-unreachable message to the sender of (REJECT) or allow the passage of (ACCEPT) packets that match this rule.
Direction	Use the drop-down list box to select the direction of traffic to which this rule applies. The possible options are LAN to DEVICE , LAN to WAN , WAN to LAN , and WAN to DEVICE .
Apply	Click Apply to save your changes.
Back	Click Back to exit this screen without saving your changes.

10.5 The DoS Screen

Click **Security > Firewall > DoS** to display the following screen. Use this screen to enable or disable Denial of Service (DoS) protection.

Figure 10-8 Security > Firewall > DoS

Each field is described in the following table.

Table 10-6 Security > Firewall > DoS

Label	Description
DoS Protection Blocking	DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. Select Enable to enable protection against DoS attacks or Disable to disable it.
Apply	Click Apply to save the DoS Protection settings.
Cancel	Click Cancel to restore your previously saved settings.

10.6 Firewall Technical Reference

This section provides some technical background information about the topics covered in this chapter.

10.6.1 Guidelines For Enhancing Security With Your Firewall

- Step 1** Change the default password via web configurator.
- Step 2** Think about access control before you connect to the network in any way.
- Step 3** Limit who can access your LTE Device.
- Step 4** Don't enable any local service (such as Telnet or FTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
- Step 5** For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
- Step 6** Keep the firewall in a secured (locked) room.

----End

10.6.2 Security Considerations

NOTE

Incorrectly configuring the firewall may block valid access or introduce security risks to the LTE Device and your protected network. Use caution when creating or deleting firewall rules and test your rules after you configure them.

Consider these security ramifications before creating a rule:

- Step 1** Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
- Step 2** Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?
- Step 3** Does a rule that allows Internet users access to resources on the LAN create security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.
- Step 4** Does this rule conflict with any existing rules?

----End

Once these questions have been answered, adding rules is simply a matter of entering the information into the correct fields in the web configurator screens.

11 MAC Filter

11.1 Overview

This chapter discusses MAC address filtering.

You can configure the LTE Device to permit access to clients based on their MAC addresses in the **MAC Filter** screen. This applies to wired and wireless connections.

11.1.1 What You Need to Know

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

11.2 The MAC Filter Screen

Use the **MAC Filter** screen to allow wireless and LAN clients access to the LTE Device. Click **Security > MAC Filter** to change your LTE Device's MAC filter settings. Select **Allow** option to display the screen as shown next.

Figure 11-1 Security > MAC Filter

MAC Address Filter : ☒ Allow ☐ Deny ☐ Disable

Set	Allow	MAC Address
1	☐	DC:4A:3E:52:50:CE
2	☐	
3	☐	
4	☐	
5	☐	
6	☐	
7	☐	
8	☐	
9	☐	
10	☐	
11	☐	
12	☐	
13	☐	
14	☐	
15	☐	
16	☐	
17	☐	
18	☐	
19	☐	
20	☐	
21	☐	
22	☐	
23	☐	
24	☐	
25	☐	
26	☐	
27	☐	
28	☐	
29	☐	
30	☐	
31	☐	
32	☐	

 **Note :**
Only devices listed here are granted access to the network.

The following table describes the Labels in this menu.

Table 11-1 Security > MAC Filter

Label	Description
MAC Address Filter	Select Allow to permit only the devices with the MAC addresses you list and select as Allow to access the LTE Device. MAC addresses not listed will be denied access to the LTE Device. Select Deny to block the devices with the MAC addresses you list and select as Deny from accessing the LTE Device. MAC addresses not listed will be permitted to access the LTE Device. Select Disable to not filter traffic by the source MAC address.
Set	This is the index number of the MAC address.

Label	Description
Allow	Select Allow to permit access to the LTE Device from the MAC address in the entry.
Deny	Select Deny to block access to the LTE Device from the MAC address in the entry.
MAC Address	Enter the MAC addresses of the wireless station and LAN devices that are allowed or not allowed access to the LTE Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

12 Parental Control

12.1 Overview

Parental control allows you to block web sites with the specific URL. You can also define time periods and days during which the LTE Device performs parental control on a specific user.

12.2 The Parental Control Screen

Use this screen to enable parental control, view the parental control rules and schedules. Click **Security > Parental Control** to open the following screen.

Figure 12-1 Security > Parental Control

General

Parental Control : ☐ Enable ☒ Disable (settings are invalid when disabled)

[Add new PCP](#)

#	Status	PCP Name	Home Network User (MAC)	Internet Access Schedule	Network Service	Website Blocked	Modify
---	--------	----------	-------------------------	--------------------------	-----------------	-----------------	--------

[Apply](#) [Cancel](#)

Figure 12-2 Security > Parental Control (After adding a new PCP)

General

Parental Control : ☐ Enable ☒ Disable (settings are invalid when disabled)

[Add new PCP](#)

#	Status	PCP Name	Home Network User (MAC)	Internet Access Schedule	Network Service	Website Blocked	Modify
1		Morning	All	00:00-06:00	None	None	

[Apply](#) [Cancel](#)

The following table describes the fields in this screen.

Table 12-1 Parental Control > Parental Control

Label	Description
Parental Control	Select Enable to activate parental control.
Add new PCP	Click this if you want to configure a new parental control rule.
#	This shows the index number of the rule.
Status	This indicates whether the rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
PCP Name	This shows the name of the rule.
Home Network User (MAC)	This shows the MAC address of the LAN user's computer to which this rule applies.
Internet Access Schedule	This shows the day(s) and time on which parental control is enabled.
Network Service	This shows whether the network service is configured. If not, None will be shown.
Website Blocked	This shows whether the website block is configured. If not, None will be shown.
Modify	Click the Edit icon to go to the screen where you can edit the rule. Click the Delete icon to delete an existing rule.
Apply	Click Apply to save your changes back to the LTE Device.
Cancel	Click Cancel to restore your previously saved settings.

12.2.1 Add/Edit a Parental Control Rule

Click **Add new PCP** in the **Parental Control** screen to add a new rule or click the **Edit** icon next to an existing rule to edit it. Use this screen to configure a restricted access schedule and/or URL filtering settings to block the users on your network from accessing certain web sites.

Figure 12-3 Add/Edit Parental Control Rule

General

☐ Active

Parental Control Profile Name :

Home Network User :

All

Internet Access Schedule

Day :

☒ Everyday

☒ Monday

☒ Tuesday

☒ Wednesday

☒ Thursday

☒ Friday

☒ Saturday

☒ Sunday

Time (Start - End) :

00:00 - 24:00

00:00

24:00

☐ No access ☒ Authorized access

Network Service

Network Service Setting :

Block

selected service(s)

Add new service

#	☐	Service Name	Protocol:Port	Modify
1	☒	Example	TCP:5099	

Blocked Site/URL Keyword

AddDelete

The following table describes the fields in this screen.

Table 12-2 Add/Edit Parental Control Rule

Label	Description
General	
Active	Select the checkbox to activate this parental control rule.
Parental Control Profile Name	Enter a descriptive name for the rule.

Label	Description
Home Network User	Select the LAN user that you want to apply this rule to from the drop- down list box. If you select Custom , enter the LAN user's MAC address. If you select All , the rule applies to all LAN users.
Internet Access Schedule	
Day	Select check boxes for the days that you want the LTE Device to perform parental control.
Time (Start - End)	Enter the time period of each day, in 24-hour format, during which parental control will be enforced.
Time	Drag the time bar to define the time that the LAN user is allowed access.
Network Service	
Network Service Setting	If you select Block , the LTE Device prohibits the users from viewing the Web sites with the URLs listed below. If you select Access , the LTE Device blocks access to all URLs except ones listed below.
Add new service	Click this to show a screen in which you can add a new service rule. You can configure the Service Name , Protocol , and Port of the new rule.
#	This shows the index number of the rule. Select the checkbox next to the rule to activate it.
Service Name	This shows the name of the rule.
Protocol Port	This shows the protocol and the port of the rule.
Modify	Edit and Delete icons appear when you add a new service. Click the Edit icon to go to the screen where you can edit the rule. Click the Delete icon to delete an existing rule.
Blocked Site/URL Keyword	The field lists the blocked web sites and URL keywords. Click Add to show a screen to enter the URLs of web sites or URL keyword to which the LTE Device blocks access. Select an item in the list and click Delete to remove it.
Apply	Click this button to save your settings back to the LTE Device.
Back	Click this button to return to the previous screen without saving any changes.

13 L2TP VPN

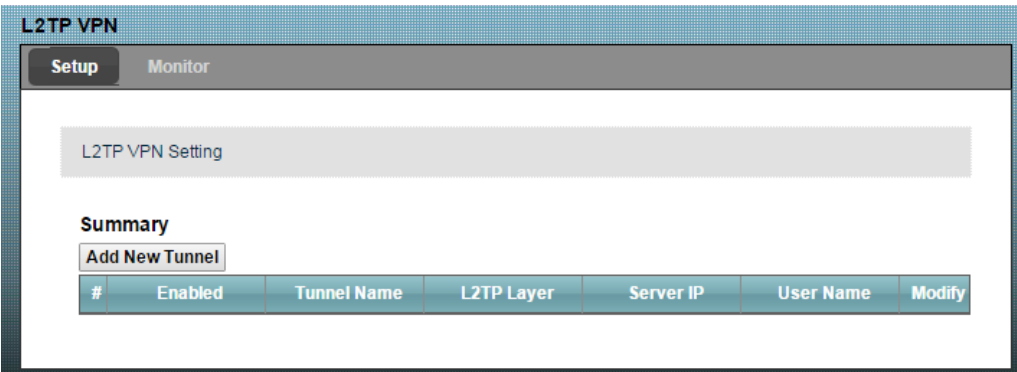
13.1 Overview

L2TP VPN tunnels network traffic between the LTE Device and a peer device or server over the Internet.

13.2 The Setup Screen

Use this screen to view and manage L2TP VPN tunnels. Click **Security > L2TP VPN** to open the following screen.

Figure 13-1 Security > L2TP VPN > Setup



The following table describes the fields in this screen.

Table 13-1 Security > L2TP VPN > Setup

Label	Description
Add New Tunnel	Click this button to create a new L2TP tunnel.
#	This shows the index number of an L2TP tunnel.

Label	Description
Enabled	This shows whether the L2TP tunnel is turned on or off.
Tunnel Name	This shows the name of this tunnel.
L2TP Layer	This shows the OSI layer protocol (Layer3) the L2TP tunnels over a network.
Server IP	This shows the IP address of the remote gateway with which the LTE Device establishes the L2TP tunnel.
User Name	The remote user must log into the LTE Device to use the L2TP VPN tunnel. This shows a user or user group that can use the L2TP VPN tunnel.
Modify	Click the Edit icon to go to the screen where you can edit the L2TP VPN tunnel. Click the Delete icon to delete an existing tunnel.

13.2.1 The Add/Edit L2TP Tunnel Screen

Use this screen to create or modify an L2TP VPN tunnel. Click the **Add New Tunnel** button or an **Edit** icon next to a VPN tunnel in the **Security > L2TP VPN** screen to open the following screen.

Figure 13-2 Add/Edit L2TP Tunnel

Add New Tunnel

L2TP Setup

Enabled

☐

Tunnel Name

L2TP Protocol Layer

Layer3 L2TP

Auth Protocol

☐ EAP

☐ MSCHAPv1

☐ MSCHAPv2

Server IP Address

User Name

Password

Note :

Warning: L2TP VPN and GRE VPN can't be used at the same time!

Warning: VPN feature and IP Pass Through feature can't be used at the same time!

Apply

Back

The following table describes the fields in this screen.

Table 13-2 Add/Edit L2TP Tunnel

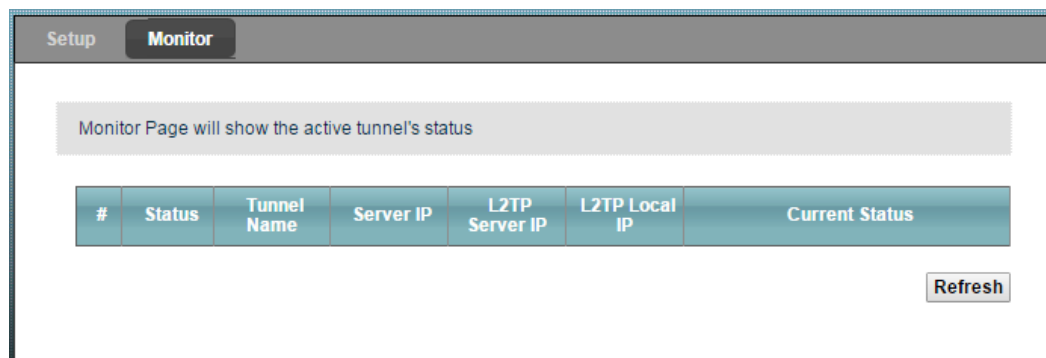
Label	Description
L2TP Setup	
Enabled	Select this to have the LTE Device use the L2TP tunnel. Clear it to configure the L2TP tunnel but not use it.
Tunnel Name	Enter a descriptive name for the L2TP tunnel.
L2TP Protocol Layer	Select Layer3 L2TP to have the LTE Device tunnel OSI layer 3 protocol over a network. Select Layer2 L2TP to have the LTE Device tunnel OSI layer 2 protocol (BCP tunnel) over a network.

Label	Description
Auth Protocol	Select the protocol (EAP, MSCHAPv1 or MSCHAPv2) the LTE Device uses for user authentication.
Server IP Address	Enter the IP address of the remote gateway.
User Name	Enter a user or user group that can use the L2TP VPN tunnel.
Password	Enter the password for the user.
Apply	Click this button to save your settings back to the LTE Device.
Back	Click this button to return to the previous screen without saving any changes.

13.3 The Monitor Screen

Use this screen to monitor L2TP VPN tunnel status. Click **Security > L2TP VPN > Monitor** to open the following screen.

Figure 13-3 Security > L2TP VPN > Monitor



The following table describes the fields in this screen.

Table 13-3 Security > L2TP VPN > Monitor

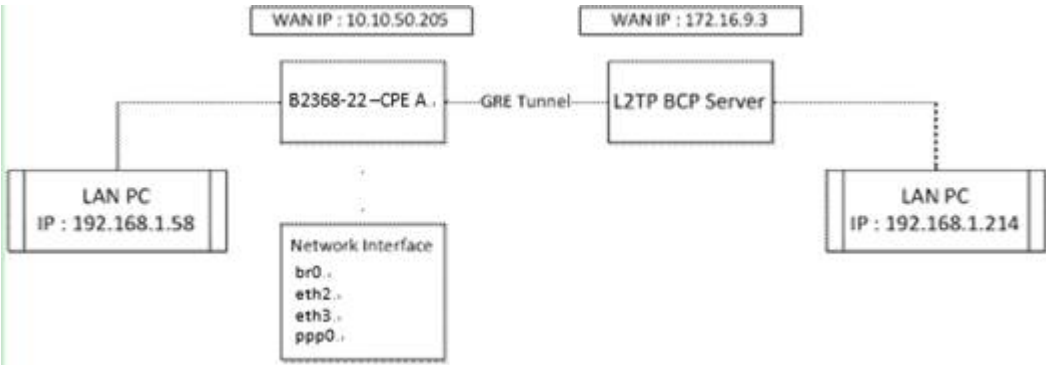
Label	Description
#	This shows the index number of the rule. Select the checkbox next to the rule to activate it.
Status	This shows the status of the L2TP VPN tunnel.
Tunnel Name	This shows the name of this tunnel.
Server IP	This shows the IP address of the remote gateway.
L2TP Server IP	This shows the IP address that the LTD Device assigned for the remote user's computer to use within the L2TP VPN tunnel.

Label	Description
L2TP Local IP	This shows the IP address of the computer that has this L2TP VPN connection with the LTE Device.
Current Status	This shows the current connection status of the L2TP VPN tunnel.
Refresh	Click this button to update this screen.

13.4 A Layer 3 L2TP VPN Configuration Example

This is the network structure used in this example:

Figure 13-4 Layer 3 L2TP VPN Network Structure Example



CPE A uses WAN IP 172.23.40.48 and has a LAN PC with IP 192.168.1.51 connected. The L2TP server uses WAN IP 172.23.40.25 and has a LAN PC with IP 192.168.2.2 connected. The LAN PC IPs must be in different subnet domains. User can set the Layer 3 L2TP VPN by L2TP Web GUI.

Figure 13-5 Layer 3 L2TP VPN Configuration Example, Add/Edit L2TP Tunnel

L2TP Setup

Enabled

☒

Tunnel Name

test

L2TP Protocol Layer

Layer3 L2TP

Auth Protocol

☐ EAP☐ MSCHAPv1☐ MSCHAPv2

Server IP Address

172.23.40.25

User Name

test

Password

●●●●

Both CPEs will bring up ppp0 interface and the L2TP server will provide a L2TP IP (192.168.3.2) for CPE A. After setting up the Layer 3 L2TP VPN, you also need to configure

static route (**Network > Static Route**, then click **Add New Static Route** or click the **Edit** icon next to an existing rule) in the Web Configurator to decide which Internet traffic goes through the L2TP tunnel. By default the CPE does not send traffic through the L2TP tunnel. For this example's network structure, set the static route to send all of the traffic destined for 192.168.2.0/24 through the tunnel (Gateway IP: 192.168.3.2).

Figure 13-6 Layer 3 L2TP VPN Configuration Example, Add Static Route

Add New Static Route

☒ Active

Route Name : L2TP

Destination IP : 192.168.2.0

Gateway : 192.168.3.2

Subnet Mask : 255.255.255.0

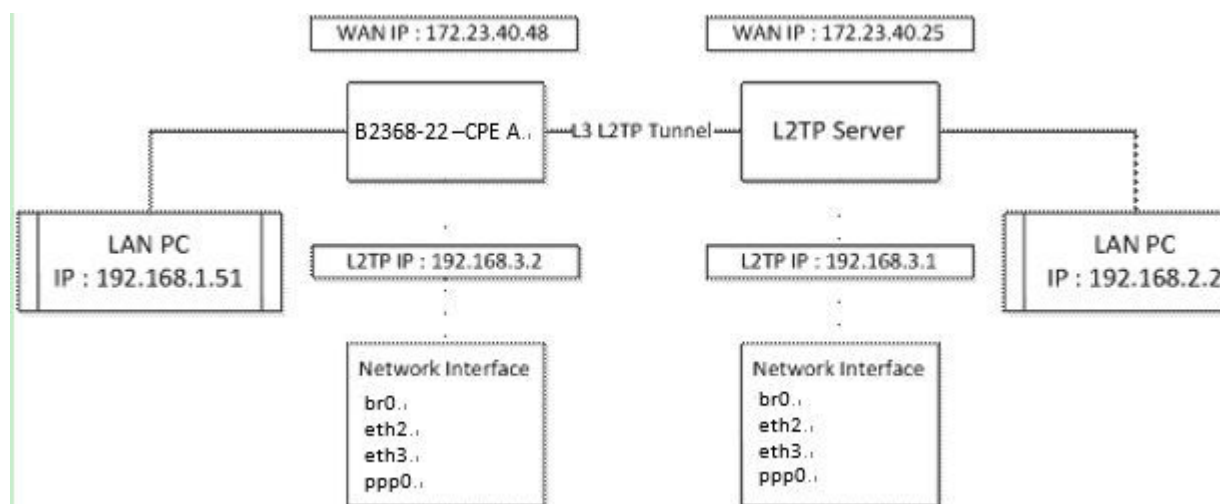
Interface : ☐ NotAvailable

Apply Back

13.5 A Layer 2 L2TP VPN Configuration Example

This is the network structure used in this example:

Figure 13-7 Layer 2 L2TP VPN Network Structure Example



CPE A has a WAN IP (10.10.50.205) and connects to a LAN PC with IP (192.168.1.58). In addition, L2TP BCP Server has a WAN IP (172.16.9.3) and connects to a LAN PC with IP (192.168.1.214). Both of the LAN PC IPs must be in the same subnet domain. You can set the Layer 2 L2TP VPN in the **L2TP VPN** screen.

After you set up the Layer 2 L2TP VPN, the LTE Device sends all of the packets from LAN PC (br0) through the L2TP BCP tunnel (bcp0). Users can send packets from one LAN PC to another (192.168.1.58 to 192.168.1.214).

Configuration:

Figure 13-8 Layer 2 L2TP VPN Configuration Example, Add/Edit L2TP Tunnel

L2TP Setup

Enabled	☒
Tunnel Name	test
L2TP Protocol Layer	Layer2 L2TP
Auth Protocol	☐ EAP ☐ MSCHAPv1 ☐ MSCHAPv2
Server IP Address	172.16.9.3
User Name	test
Password	••••

14 GRE VPN

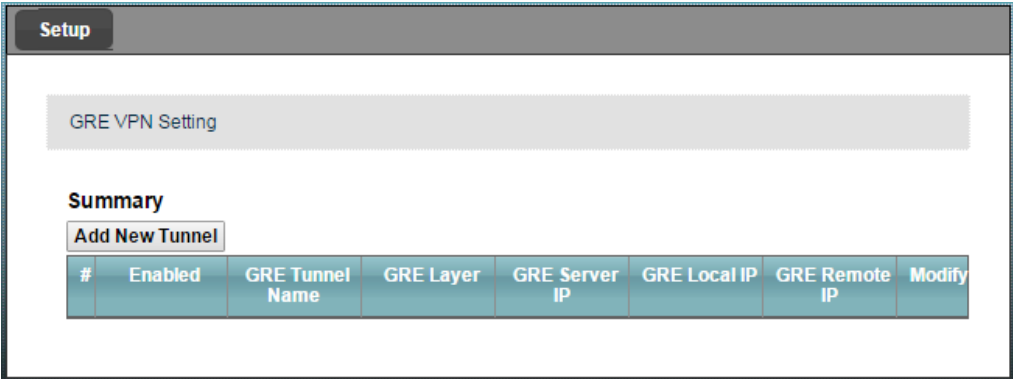
14.1 Overview

GRE (Generic Routing Encapsulation) tunnels encapsulate a wide variety of network layer protocol packet types inside IP tunnels. A GRE tunnel serves as a virtual point-to-point link between the LTE Device and another router over an IPv4 network. At the time of writing, the LTE Device only supports GRE tunneling in IPv4 networks.

14.2 The Setup Screen

Use this screen to view and manage GRE VPN tunnels. Click **Security > GRE VPN** to open the following screen.

Figure 14-1 Security > GRE VPN > Setup



The following table describes the fields in this screen.

Table 14-1 Security > GRE VPN > Setup

Label	Description
Add New Tunnel	Click this button to create a new GRE tunnel.
#	This shows the index number of the rule. Select the checkbox next to the rule to activate it.
Enabled	This shows whether the GRE tunnel is turned on or off.
GRE Tunnel Name	This shows the name of this tunnel.
GRE Layer	This shows either OSI layer 2 or layer 3 protocol the GRE tunnels over a network.
GRE Server IP	This is the IP address or domain name of the remote gateway to which the LTE Device's WAN interface tunnels traffic.
GRE Local IP	This is the local hosts' IP addresses for which the LTE Device tunnels traffic sent to the remote gateway.
GRE Remote IP	This is the remote hosts' IP addresses behind the remote gateway to which the LTE Device tunnels traffic.
Modify	Click the Edit icon to go to the screen where you can edit the tunnel. Click the Delete icon to delete an existing tunnel.

14.2.1 The Add/Edit GRE Tunnel Screen

Use this screen to create or modify a GRE VPN tunnel. Click the **Add New Tunnel** button or an **Edit** icon next to a VPN tunnel in the **Security > GRE VPN** screen to open the following screen.

Figure 14-2 Add/Edit GRE Tunnel

Add New Tunnel

GRE Setup

Enabled

☐

Tunnel Name

GRE Layer

Layer3 GRE

Server IP Address

GRE Local IP

GRE Remote IP

Note :

Warning: L2TP VPN and GRE VPN can't be used at the same time!

Warning: VPN feature and IP Pass Through feature can't be used at the same time!

Apply

Back

The following table describes the fields in this screen.

Table 14-2 Add/Edit GRE Tunnel

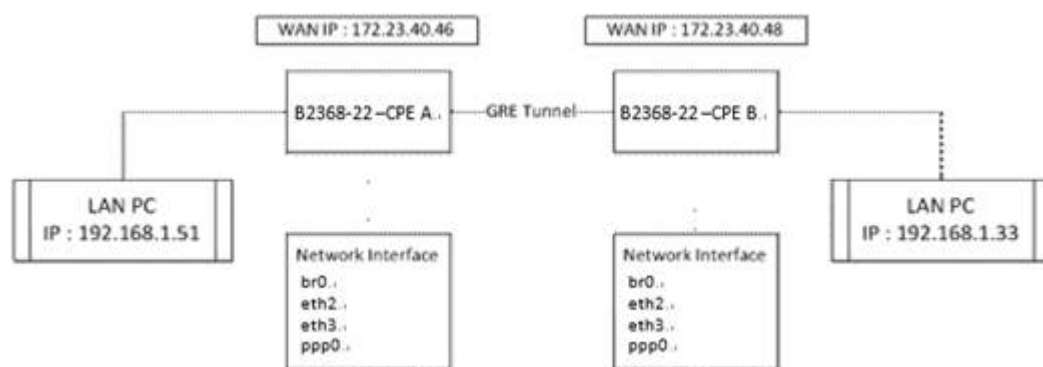
Label	Description
GRE Setup	
Enabled	Select this to have the LTE Device use the GRE tunnel. Clear it to configure the GRE tunnel but not use it.
Tunnel Name	Enter a descriptive name for the GRE tunnel.
GRE Layer	Select which OSI layer (Layer2 GRE or Layer3 GRE) protocol the GRE tunnels over a network. Use layer 2 when both of the LAN PC IPs are in the same subnet domain. Use layer 3 when the LAN PC IPs are in different subnet domains.
Server IP Address	Enter the IP address or domain name of the remote gateway to which the LTE Device's WAN interface tunnels traffic.
GRE Local IP	Enter a local host's IP address the LTE Device tunnels the traffic sent to the remote gateway.

Label	Description
GRE Remote IP	Enter a remote host's IP addresses behind the remote gateway, to which the LTE Device transmits traffic through this GRE tunnel.
Apply	Click this button to save your settings back to the LTE Device.
Back	Click this button to return to the previous screen without saving any changes.

14.3 A Layer 2 GRE VPN Configuration Example

This is the network structure used in this example:

Figure 14-3 Layer 2 GRE VPN Network Structure Example



CPE A uses WAN IP 172.23.40.46 and has a LAN PC with IP 192.168.1.51 connected. CPE B uses WAN IP 172.23.40.48 and has a LAN PC with IP 192.168.1.33 connected. Both of the LAN PC IPs must be in the same subnet domain. To configure CPE A, input a tunnel name, set the GRE Layer to Layer2 GRE, and set the WAN IP of CPE B (172.23.40.48) as the Server IP Address.

Configuration (**Security** > **GRE VPN**, and then click **Add New Tunnel**):

Figure 14-4 Layer 2 GRE VPN Configuration Example, Add/Edit GRE Tunnel

The screenshot shows the 'Add New Tunnel' configuration window. The 'GRE Setup' section is visible, with the following fields and values:

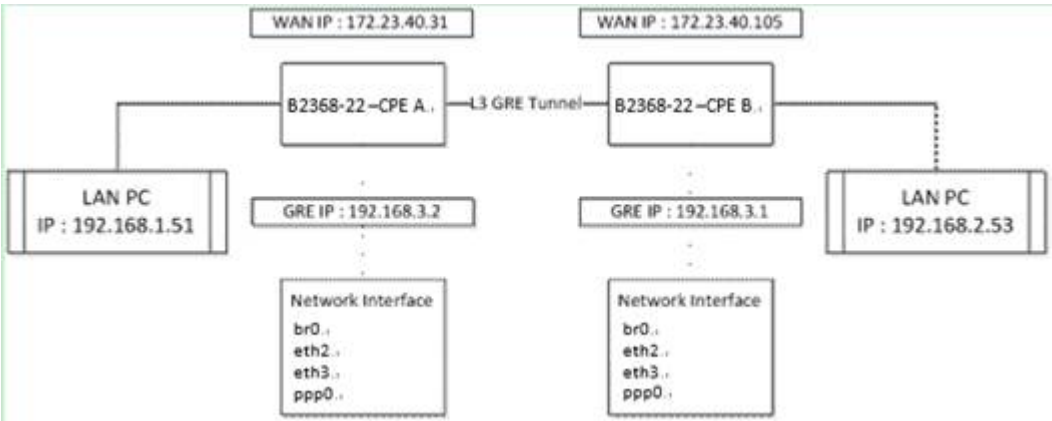
- Enabled: ☒
- Tunnel Name: GRE
- GRE Layer: Layer2 GRE
- Server IP Address: 172.23.40.48
- GRE Local IP: (empty)
- GRE Remote IP: (empty)

After setting up the Layer 2 GRE VPN, the CPEs send all of the packets from the LAN PCs through the GRE tunnel. Users can send packets from one LAN PC to the others via APN1.

14.4 A Layer 3 GRE VPN Configuration Example

This is the network structure used in this example:

Figure 14-5 Layer 3 GRE VPN Network Structure Example



CPE A uses WAN IP 172.23.40.31 and has a LAN PC with IP 192.168.1.51 connected. CPE B uses WAN IP 172.23.40.105 and has a LAN PC with IP 192.168.2.53 connected. The LAN PC IPs must be in different subnet domains. Configure CPE A as follows.

Figure 14-6 Layer 3 GRE VPN Configuration Example, Add/Edit GRE Tunnel

Add New Tunnel

GRE Setup

Enabled ☒

Tunnel Name

GRE Layer

Server IP Address

GRE Local IP

GRE Remote IP

Both CPEs will bring up the tunnel interface and set a GRE IP to the interface. After setting up the Layer 3 GRE VPN, you also need to configure static route in the Web Configurator to decide which Internet traffic goes through the GRE tunnel. By default the CPE does not send traffic through the GRE tunnel. For this example's network structure, set the static route to send all of the traffic destined for 192.168.2.0/24 through the tunnel (Gateway IP: 192.168.3.2).

Figure 14-7 Layer 3 GRE VPN Configuration Example, Add Static Route

Add New Static Route

☒ Active

Route Name :GRE

Destination IP :192.168.2.0

Gateway :192.168.3.2

Subnet Mask :255.255.255.0

Interface☐ NotAvailable

Apply

Back

15 VoIP

15.1 Overview

Use this chapter to:

- Connect an analog phone to the LTE Device.
- Make phone calls over the Internet, as well as the regular phone network.
- Configure settings such as speed dial.
- Configure network settings to optimize the voice quality of your phone calls.
- When using multiple APNs, you have to do the following actions to make sure the IAD devices or Softphone on the LAN can go through the correct routing path (second APN).

Add a static route that helps route traffic to the media server (ex. **204.11.12.32** in the example at the right) through the **Voice** interface in the **Network Setting > Static Route > Add New Static Route** screen (see **7.2.1 Add/Edit Static Route** for more information). After adding the static route, you can wait until the register retry interval timeout expires to let VoIP automatically connect to the server, or you can go to the **System Info** page and press the register button to have VoIP immediately connect to the server.

Figure 15-1 Static Route for Voice Example

Add New Static Route

☒ Active

Route Name : voice

Destination IP : 204.11.12.32

Gateway :

Subnet Mask : 255.255.255.255

Interface : ☒ Voice ▼

Apply Back

15.1.1 What You Need to Know

The following terms and concepts may help as you read this chapter.

VoIP

VoIP stands for Voice over IP. IP is the Internet Protocol, which is the message-carrying standard the Internet runs on. So, Voice over IP is the sending of voice signals (speech) over the Internet (or another network that uses the Internet Protocol).

SIP

SIP stands for Session Initiation Protocol. SIP is a signaling standard that lets one network device (like a computer or the LTE Device) send messages to another. In VoIP, these messages are about phone calls over the network. For example, when you dial a number on your LTE Device, it sends a SIP message over the network asking the other device (the number you dialed) to take part in the call.

SIP Accounts

A SIP account is a type of VoIP account. It is an arrangement with a service provider that lets you make phone calls over the Internet. When you set the LTE Device to use your SIP account to make calls, the LTE Device is able to send all the information about the phone call to your service provider on the Internet.

Strictly speaking, you don't need a SIP account. It is possible for one SIP device (like the LTE Device) to call another without involving a SIP service provider. However, the networking difficulties involved in doing this make it impractical under normal circumstances. Your SIP account provider removes these difficulties by taking care of the call routing and setup - figuring out how to get your call to the right place in a way that you and the other person can talk to one another.

Voice Activity Detection/Silence Suppression

Voice Activity Detection (VAD) detects whether or not speech is present. This lets the LTE Device reduce the bandwidth that a call uses by not transmitting "silent packets" when you are not speaking.

Comfort Noise Generation

When using VAD, the LTE Device generates comfort noise when the other party is not speaking. The comfort noise lets you know that the line is still connected as total silence could easily be mistaken for a lost connection.

Echo Cancellation

G.168 is an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.

How to Find Out More

See Section [15.6 Technical Reference](#) for more information on SIP.

15.1.2 Before You Begin

- Before you can use these screens, you need to have a VoIP account already set up. If you don't have one yet, you can sign up with a VoIP service provider over the Internet.
- You should have the information your VoIP service provider gave you ready, before you start to configure the LTE Device.

15.2 The SIP Service Provider Screen

Use this screen to configure the SIP server information, QoS for VoIP calls, and the numbers for certain phone functions. Click **VoIP > SIP** to open the **SIP Service Provider** screen.

NOTE

Click **more...** to see all the fields in the screen. You don't necessarily need to use all these fields to set up your account. Click **hide more** to see and configure only the fields needed for this feature.

Figure 15-2 VoIP > SIP > SIP Service Provider

SIP

SIP Service Provider SIP Account

SIP Service Provider offers services of making Internet calls using VoIP technology. You may need to consult your SIP Service Provider for the following settings. This configuration should be used in conjunction with SIP Account.

General

SIP Service Provider :☒ Enable SIP Service Provider

SIP Service Provider Name :

SIP Local Port : (1025-65535)

Main SIP Server Address :

SIP Server Port : (1025-65535)

REGISTER Server Address :

REGISTER Server Port : (1025-65535)

SIP Service Domain :

[hide more](#)

RFC Support

PRACK (RFC 3262) :

☐ DNS SRV Enabled (RFC 3263, When this option is selected, it takes about 30 seconds for the configuration to take effect.)

☒ Session Timer (RFC 4028)

VoIP IOP Flags

☒ Replace dial digit '#' to '%23' in SIP messages

☒ Remove ':5060' and 'transport=udp' from request-uri in SIP messages

☐ Remove the 'Route' header in SIP messages

☒ Don't send re-Invite to the remote party when there are multiple codecs answered in the SDP

☒ Remove the 'Authentication' header in SIP ACK message

☐ Using Bidirection RTP for SIP 183

☐ Support SDP for SIP 180

☐ Remove Early Media Header

RTP Port Range

Start Port : (1025-65535)

End Port : (1025-65535)

DTMF Mode

DTMF Mode : RFC 2833 ▼

Transport Type

Transport Type : UDP

Outbound Proxy

☐ Enable

Server Address :

Server Port :

(1025-65535)

QoS Tag

SIP TOS Priority Setting : 184 (0-255)

RTP TOS Priority Setting : 184 (0-255)

Timer Setting

Expiration Duration : 3600 (60-65535) second

Register Re-send timer : 512 (180-65535) second

Session Expires : 180 (100-3600) second

Min-SE : 90 (90-1800) second

Dialing Interval Selection

Dialing Interval Selection : 3 ▼ second

Phone Key Config

Caller Display Call *30#

Caller Hidden Call #30#

One Shot Caller Display Call #31#

One Shot Caller Hidden Call *31*

Call Waiting Enable *43#

Call Waiting Disable #43#

One Shot Call Waiting Enable *44#

One Shot Call Waiting Disable #44#

Call Transfer *98#

Unconditional Call Forward Enable *21*

Unconditional Call Forward Disable #21#

No Answer Call Forward Enable *61*

No Answer Call Forward Disable #61#

Call Forward When Busy Enable *67*

Call Forward When Busy Enable	*67*
Call Forward When Busy Disable	#67#
Do Not Disturb Enable	*95#
Do Not Disturb Disable	#95#

 NOTE

The configuration rule has restrictions. The configuration value cannot start with a digit and end with a number sign (#).

The following table describes the Labels in this screen.

Table 15-1 VoIP > SIP > SIP Service Provider

Label	Description
General	
SIP Service Provider	Select this if you want the LTE Device to use this SIP provider. Clear it if you do not want the LTE Device to use this SIP provider.
SIP Service Provider Name	Enter the name of your SIP service provider.
SIP Local Port	Enter the LTE Device's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value. NOTE To let both the FXS port and the IAD devices or SIP phones on the LAN work together, check the SIP port settings on your IADs and SIP phones and make sure they use different ports than the LTE Device's SIP local port.
Main SIP Server Address	Enter the IP address or domain name of the SIP server provided by your VoIP service provider. You can use up to 63 printable ASCII characters. It does not matter whether the SIP server is a proxy, redirect or register server.
SIP Server Port	Enter the SIP server's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
REGISTER Server Address	Enter the IP address or domain name of the SIP register server, if your VoIP service provider gave you one. Otherwise, enter the same address you entered in the SIP Server Address field. You can use up to 63 printable ASCII characters.
REGISTER Server Port	Enter the SIP register server's listening port number, if your VoIP service provider gave you one. Otherwise, enter the same port number you entered in the SIP Server Port field.

Label	Description
SIP Service Domain	Enter the SIP service domain name. In the full SIP URI, this is the part after the @ symbol. You can use up to 63 printable ASCII Extended set characters.
RFC Support	
PRACK (RFC 3262)	RFC 3262 defines a mechanism to provide reliable transmission of SIP provisional response messages, which convey information on the processing progress of the request. This uses the option tag 100rel and the Provisional Response ACKnowledgement (PRACK) method. Select Supported or Required to have the LTE Device include a SIP Require/Supported header field with the option tag 100rel in all INVITE requests. When the LTE Device receives a SIP response message indicating that the phone it called is ringing, the LTE Device sends a PRACK message to have both sides confirm the message is received. If you select Supported, the peer device supports the option tag 100rel to send provisional responses reliably. If you select Required, the peer device requires the option tag 100rel to send provisional responses reliably. Select Disabled to turn off this function.
DNS SRV Enabled (RFC 3263)	Select this to have the LTE Device query your ISP's DNS server for a list of any available SIP servers that it maintains. This is useful if your static SIP server experiences difficulties, making it hard for your IP phone users to make SIP calls.
Session Timer (RFC 4028)	Select this to have the LTE Device support RFC 4028. This makes sure that SIP sessions do not hang and the SIP line can always be available for use.
VoIP IOP Flags - Select VoIP inter-operability settings. Please select VoIP IOP Flag options according to information given by your Service Provider.	
RTP Port Range	

Label	Description
Start Port End Port	Enter the listening port number(s) for RTP traffic, if your VoIP service provider gave you this information. Otherwise, keep the default values. To enter one port number, enter the port number in the Start Port and End Port fields. To enter a range of ports, ● Enter the port number at the beginning of the range in the Start Port field. ● Enter the port number at the end of the range in the End Port field. NOTE The LTE Device uses the RTP ports starting from 50000 by default. NOTE Make sure your IADs'or SIP phones' RTP ports do NOT start from 50000 to avoid port conflict issues. For example, change them to 10000 or 30000 if they conflict with the LTE Device's RTP ports.
DTMF Mode	
DTMF Mode	Control how the LTE Device handles the tones that your telephone makes when you push its buttons. You should use the same mode your VoIP service provider uses. RFC2833 - send the DTMF tones in RTP packets. PCM - send the DTMF tones in the voice data stream. This method works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729 and G.726) can distort the tones. SIP INFO - send the DTMF tones in SIP messages.
Transport Type	
Transport Type	This read-only field displays the transport layer protocol the LTE Device uses for SIP (UDP).
Outbound Proxy	
Enable	Select this if your VoIP service provider has a SIP outbound server to handle voice calls. This allows the LTE Device to work with any type of NAT router and eliminates the need for STUN.
Server Address	Enter the IP address or domain name of the SIP outbound proxy server.
Server Port	Enter the SIP outbound proxy server's listening port, if your VoIP service provider gave you one. Otherwise, keep the default value.
QoS Tag	

Label	Description
SIP TOS Priority Setting	Enter the DSCP (DiffServ Code Point) number for SIP message transmissions. The LTE Device creates Class of Service (CoS) priority tags with this number to SIP traffic that it transmits.
RTP TOS Priority Setting	Enter the DSCP (DiffServ Code Point) number for RTP voice transmissions. The LTE Device creates Class of Service (CoS) priority tags with this number to RTP traffic that it transmits.
Timer Setting	
Expiration Duration	Enter the number of seconds your SIP account is registered with the SIP register server before it is deleted. The LTE Device automatically tries to re-register your SIP account when one-half of this time has passed. (The SIP register server might have a different expiration.)
Register Re- send timer	Enter the number of seconds the LTE Device waits before it tries again to register the SIP account, if the first try failed or if there is no response.
Session Expires	Enter the number of seconds the LTE Device lets a SIP session remain idle (without traffic) before it automatically disconnects the session.
Min-SE	Enter the minimum number of seconds the LTE Device lets a SIP session remain idle (without traffic) before it automatically disconnects the session. When two SIP devices start a SIP session, they must agree on an expiration time for idle sessions. This field is the shortest expiration time that the LTE Device accepts.
Dialing Interval Selection	
Dialing Interval Selection	Enter the number of seconds the LTE Device should wait after you stop dialing numbers before it makes the phone call. The value depends on how quickly you dial phone numbers.
Phone Key Config Use this section to customize the phone keypad combinations you use to access certain features on the LTE Device. If you dial the phone key which does not include the name with "one shot", you will hear a "single sound" tone. If not, it means the phone key you dialed is wrong. After hearing the "single sound" tone, hang up your phone and the corresponding feature will work. For the feature with the name "one shot", you must dial the phone number you're going to make after dial the phone key. You will not get any feedback from the device when you use the "one shot" feature.	
Caller Display Call	This code is used to display the caller ID for outgoing calls.
Caller Hidden Call	This code is used to hide the caller ID for outgoing calls.

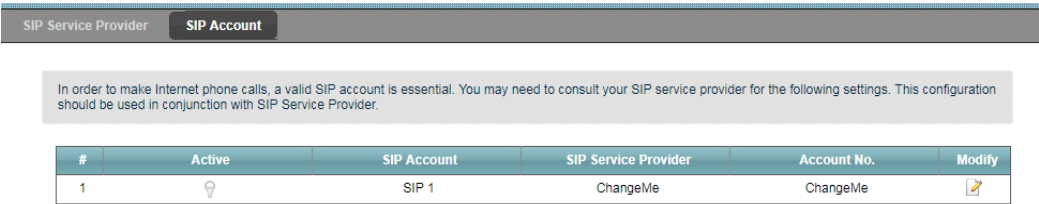
Label	Description
One Shot Caller Display Call	This code is used to display the caller ID only for the phone call you are going to make.
One Shot Caller Hidden Call	This code is used to hide the caller ID only for the phone call you are going to make.
Call Waiting Enable	This code is used to turn the Call Waiting feature on. With call waiting, you hear a special beep notifying another incoming call while you are answering a call. It allows you to place the first incoming call on hold and answer the second call so that you won't miss any important calls.
Call Waiting Disable	This code is used to turn the Call Waiting feature off.
One Shot Call Waiting Enable	This code is used to enable call waiting only for the phone call you are going to make. See the Description for the Call Waiting Enable field for more information.
One Shot Call Waiting Disable	This code is used to disable one shot call waiting.
Call Transfer	This code is used to enable call transfer that allows you to transfer an incoming call (that you have answered) to another phone.
Unconditional Call Forward Enable	This code is used to enable unconditional call forwarding. Incoming calls are always forwarded to a specified number without any condition.
Unconditional Call Forward Disable	This code is used to disable unconditional call forwarding.
No Answer Call Forward Enable	This code is used to enable call forwarding when there is no answer at a SIP number.
No Answer Call Forward Disable	This code is used to disable call forwarding when there is no answer at a SIP number.
Call Forward When Busy Enable	This code is used to enable call forwarding when the phone is busy.
Call Forward When Busy Disable	This code is used to disable call forwarding when the phone is busy.
Do Not Disturb Enable	This code is used to turn the Do Not Disturb feature on. This has the LTE Device not forward calls to the phone line.
Do Not Disturb Disable	This code is used to turn the Do Not Disturb feature off.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

15.3 The SIP Account Screen

The LTE Device uses a SIP account to make outgoing VoIP calls and check if an incoming call's destination number matches your SIP account's SIP number. In order to make or receive a VoIP call, you need to enable and configure a SIP account, and map it to a phone port. The SIP account contains information that allows your LTE Device to connect to your VoIP service provider.

To access the following screen, click **VoIP > SIP > SIP Account**.

Figure 15-3 VoIP > SIP > SIP Account



The following table describes the Labels in this screen.

Table 15-2 VoIP > SIP > SIP Account

Label	Description
#	This is the index number of the entry.
Active	This shows whether the SIP account is activated or not. A yellow bulb signifies that this SIP account is activated. A gray bulb signifies that this SIP account is activated.
SIP Account	This shows the name of the SIP account.
SIP Service Provider	This shows the name of the SIP service provider.
Account No.	This shows the SIP number.
Modify	Click the Edit icon to configure the SIP account.

15.3.1 Edit SIP Account

You can configure the SIP account. To access this screen, click **Edit** icon next to an existing account.

Figure 15-4 SIP Account: Edit

SIP Account Configuration

SIP Account :

☒ Active SIP Account

SIP Account Number :

ChangeMe x

Authentication

Username :

ChangeMe

Password :

URL Type

URL Type :

SIP v

Voice Features

Primary Compression Type :

G.711MuLaw v

Second Compression Type :

G.729 v

Third Compression Type :

G.711ALaw v

Speaking Volume Control :

Middle v

Listening Volume Control :

Middle v

☒ Active G.168(Echo Cancellation)

☐ Active VAD(Voice Active Detector)

Call Features

☒ Send Caller ID

☒ Active Call Transfer

☒ Active Call Waiting :

Active Call Waiting Reject Time :

24

(10~60) Seconds

☐ Active Unconditional Forward

To Number :

☐ Active Busy Forward

To Number :

☐ Active No Answer Forward

To Number :

No Answer Ring Time

10

(10~180) Seconds

☐ Active Anonymous Call Block

Flash Detect Interval Configuration

☐ Interval Configuration Enable

Hook Flash Detect Upper Bound :

500

(101~2000) Milliseconds

Hook Flash Detect Lower Bound :

100

(100~1999) Milliseconds

Apply

Back

The following table describes the Labels in this screen.

Table 15-3 SIP Account: Edit

Label	Description
General	
SIP Account	Select the Active SIP Account check box if you want to use this account. Clear it if you do not want to use this account.
SIP Account Number	Enter your SIP number. In the full SIP URI, this is the part before the @ symbol. You can use the "+" symbol and numbers.
Authentication	
Username	Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 128 printable ASCII characters.
Password	Enter the password for registering this SIP account, exactly as it was given to you. You can use up to 128 printable ASCII characters.
URL Type	
URL Type	Select whether or not to include the SIP service domain name when the LTE Device sends the SIP number. SIP - include the SIP service domain name. TEL - do not include the SIP service domain name.
Voice Features	
Primary Compression Type Secondary Compression Type Third Compression Type	Select the type of voice coder/decoder (codec) that you want the LTE Device to use. G.711 provides higher voice quality but requires more bandwidth (64 kbps). ● G.711MuLaw is typically used in North America and Japan. ● G.711ALaw is typically used in Europe. ● G.729 only requires 8 kbps. Select the LTE Device's first choice for voice coder/decoder. Select the LTE Device's second choice for voice coder/decoder. Select None if you only want the LTE Device to accept the first choice. Select the LTE Device's third choice for voice coder/decoder. Select None if you only want the LTE Device to accept the first or second choice.
Speaking Volume Control	Enter the loudness that the LTE Device uses for speech that it sends to the peer device. Minimum is the quietest, and Maximum is the loudest.
Listening Volume Control	Enter the loudness that the LTE Device uses for speech that it receives from the peer device. Minimum is the quietest, and Maximum is the loudest.

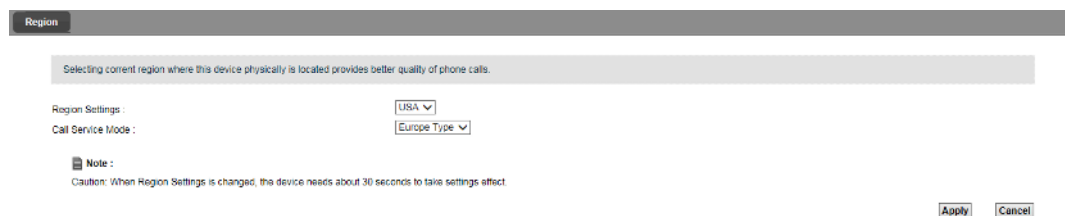
Label	Description
Active G.168 (Echo Cancellation)	Select this if you want to eliminate the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
Active VAD (Voice Active Detector)	Select this if the LTE Device should stop transmitting when you are not speaking. This reduces the bandwidth the LTE Device uses.
Call Features	
Send Caller ID	Select this if you want to send identification when you make VoIP phone calls. Clear this if you do not want to send identification.
Active Call Transfer	Select this to enable call transfer on the LTE Device. This allows you to transfer an incoming call (that you have answered) to another phone.
Active Call Waiting	Select this to enable call waiting on the LTE Device. This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.
Active Call Waiting Reject Time	Specify a time of seconds that the LTE Device waits before rejecting the second call if you do not answer it.
Active Unconditional Forward	Select this if you want the LTE Device to forward all incoming calls to the specified phone number. Specify the phone number in the To Number field on the right.
Active Busy Forward	Select this if you want the LTE Device to forward incoming calls to the specified phone number if the phone port is busy. Specify the phone number in the To Number field on the right. If you have call waiting, the incoming call is forwarded to the specified phone number if you reject or ignore the second incoming call.
Active No Answer Forward	Select this if you want the LTE Device to forward incoming calls to the specified phone number if the call is unanswered. (See No Answer Time .) Specify the phone number in the To Number field on the right.
No Answer Ring Time	This field is used by the Active No Answer Forward feature. Enter the number of seconds the LTE Device should wait for you to answer an incoming call before it considers the call is unanswered.
Active Anonymous Call Block	Select this if you do not want the phone to ring when someone tries to call you with caller ID deactivated.
Flash Detect Interval Configuration	

Label	Description
Interval Configuration Enable	You can tap the phone's hook to signal a flash in order to control certain functions. Select this to manually configure the flash detect interval (how long of a press on the phone's hook the LTE Device counts as a flash). If this configuration is disabled, the flash interval will be set according to the region selected in VoIP > Phone > Region Settings .
Hook Flash Detect Upper Bound	Specify the longest hook press to count as a flash. The LTE Device interprets a hook press longer than this as hanging up.
Hook Flash Detect Lower Bound	Specify the shortest hook press to count as a flash.
Apply	Click Apply to save your changes.
Back	Click Back to return to the previous screen without saving.

15.4 The Phone Region Screen

Use this screen to maintain settings that depend on which region of the world the LTE Device is in. To access this screen, click **VoIP > Phone > Region**.

Figure 15-5 VoIP> Phone > Region



Each field is described in the following table.

Table 15-4 VoIP > Phone > Region

Label	Description
Region Settings	Select the place in which the LTE Device is located.

Label	Description
Call Service Mode	Select the mode for supplementary phone services (call hold, call waiting, call transfer and three-way conference calls) that your VoIP service provider supports. ● Europe Type - use supplementary phone services in European mode. ● USA Type - use supplementary phone services American mode. You might have to subscribe to these services to use them. Contact your VoIP service provider.
Apply	Click this to save your changes and to apply them to the LTE Device.
Cancel	Click this to set every field in this screen to its last-saved value.

15.5 The Call Rule Screen

Use this screen to add, edit, or remove speed-dial numbers for outgoing calls. Speed dial provides shortcuts for dialing frequently-used (VoIP) phone numbers. You also have to create speed-dial entries if you want to call SIP numbers that contain letters. Once you have configured a speed dial rule, you can use a shortcut (the speed dial number, #01 for example) on your phone's keypad to call the phone number.

To access this screen, click **VoIP > Call Rule**.

Figure 15-6 VoIP > Call Rule

Speed Dial

When certain phone numbers are dialed on a regular basis, Speed Dial accelerates dialing process. The following rules apply to all the phone device connected to this device.

Speed Dial

#	Number	Description	SIPNumber
1			Add

Phone Book

#	Number	Description	Modify
#01			
#02			
#03			
#04			
#05			
#06			
#07			
#08			
#09			
#10			

Clear Cancel

Each field is described in the following table.

Table 15-5 VoIP > Call Rule

Label	Description
Speed Dial	Use this section to create or edit speed-dial entries.
#	Select the speed-dial number you want to use for this phone number.
Number	Enter the SIP number you want the LTE Device to call when you dial the speed-dial number.
Description	Enter a short Description to identify the party you call when you dial the speed- dial number. You can use up to 127 printable ASCII characters.
Add	Click this to use the information in the Speed Dial section to update the Phone Book section.
Phone Book	Use this section to look at all the speed-dial entries and to erase them.
#	This field displays the speed-dial number you should dial to use this entry.
Number	This field displays the SIP number the LTE Device calls when you dial the speed-dial number.
Description	This field displays a short Description of the party you call when you dial the speed-dial number.
Modify	Use this field to edit or erase the speed-dial entry. Click the Edit icon to copy the information for this speed-dial entry into the Speed Dial section, where you can change it. Click Add when you finish editing to change the configurations. Click the Delete icon to erase this speed-dial entry.
Clear	Click this to erase all the speed-dial entries.
Cancel	Click this to set every field in this screen to its last-saved value.

15.6 Technical Reference

This section contains background material relevant to the **VoIP** screens.

15.6.1 VoIP

VoIP is the sending of voice signals over Internet Protocol. This allows you to make phone calls over the Internet at a fraction of the cost of using the traditional circuit- switched telephone network. You can also use servers to run telephone service applications like PBX services and voice mail. Internet Telephony Service Provider (ITSP) companies provide VoIP service.

Circuit-switched telephone networks require 64 kilobits per second (Kbps) in each direction to handle a telephone call. VoIP can use advanced voice coding techniques with compression to reduce the required bandwidth.

15.6.2 SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet.

SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

SIP Identities

A SIP account uses an identity (sometimes referred to as a SIP address). A complete SIP identity is called a SIP URI (Uniform Resource Identifier). A SIP account's URI identifies the SIP account in a way similar to the way an e-mail address identifies an e-mail account. The format of a SIP identity is SIP-Number@SIP-Service-Domain.

SIP Number

The SIP number is the part of the SIP URI that comes before the "@" symbol. A SIP number can use letters like in an e-mail address (johndoe@your-ITSP.com for example) or numbers like a telephone number (1122334455@VoIP-provider.com for example).

SIP Service Domain

The SIP service domain of the VoIP service provider is the domain name in a SIP URI. For example, if the SIP address is 1122334455@VoIP-provider.com, then "VoIP-provider.com" is the SIP service domain.

SIP Registration

Each LTE Device is an individual SIP User Agent (UA). To provide voice service, it has a public IP address for SIP and RTP protocols to communicate with other servers.

A SIP user agent has to register with the SIP registrar and must provide information about the users it represents, as well as its current IP address (for the routing of incoming SIP requests). After successful registration, the SIP server knows that the users (identified by their dedicated SIP URIs) are represented by the UA, and knows the IP address to which the SIP requests and responses should be sent.

Registration is initiated by the User Agent Client (UAC) running in the VoIP gateway (the LTE Device). The gateway must be configured with information letting it know where to send the REGISTER message, as well as the relevant user and authorization data.

A SIP registration has a limited lifespan. The User Agent Client must renew its registration within this lifespan. If it does not do so, the registration data will be deleted from the SIP registrar's database and the connection broken.

The LTE Device attempts to register all enabled subscriber ports when it is switched on. When you enable a subscriber port that was previously disabled, the LTE Device attempts to register the port immediately.

Authorization Requirements

SIP registrations (and subsequent SIP requests) require a username and password for authorization. These credentials are validated via a challenge / response system using the HTTP digest mechanism (as detailed in RFC3261, "SIP: Session Initiation Protocol").

SIP Servers

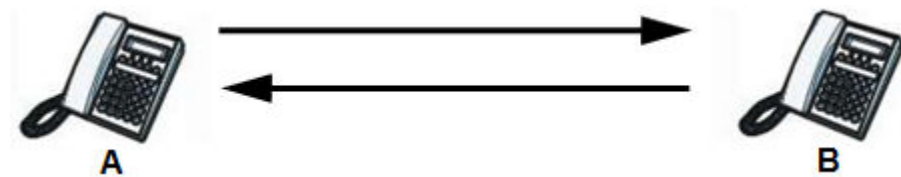
SIP is a client-server protocol. A SIP client is an application program or device that sends SIP requests. A SIP server responds to the SIP requests.

When you use SIP to make a VoIP call, it originates at a client and terminates at a server. A SIP client could be a computer or a SIP phone. One device can act as both a SIP client and a SIP server.

SIP User Agent

A SIP user agent can make and receive VoIP telephone calls. This means that SIP can be used for peer-to-peer communications even though it is a client-server protocol. In the following figure, either **A** or **B** can act as a SIP user agent client to initiate a call. **A** and **B** can also both act as a SIP user agent to receive the call.

Figure 15-7 SIP User Agent



SIP Proxy Server

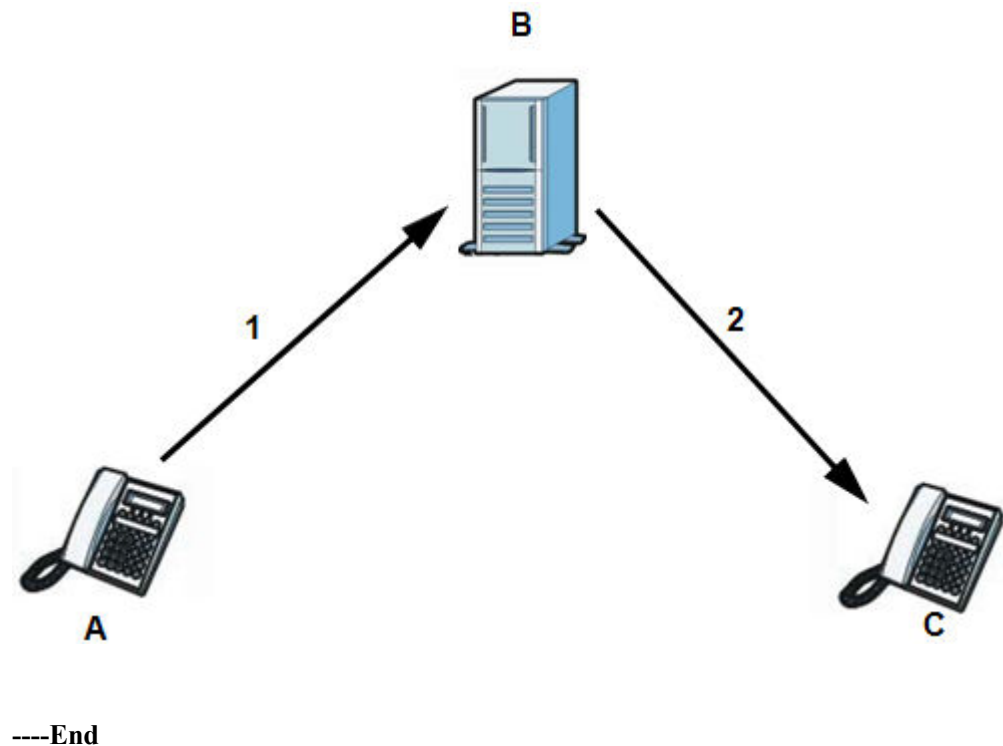
SIP Proxy Server

A SIP proxy server receives requests from clients and forwards them to another server.

In the following example, you want to use client device **A** to call someone who is using client device **C**.

- Step 1** The client device (**A** in the figure) sends a call invitation to the SIP proxy server **B**.
- Step 2** The SIP proxy server forwards the call invitation to **C**.

Figure 15-8 SIP Proxy Server



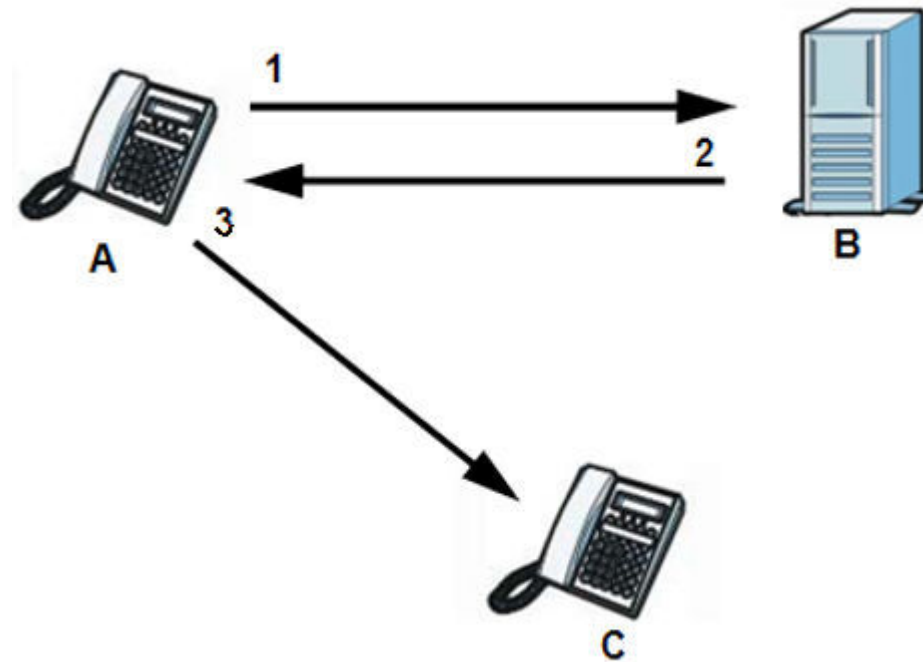
SIP Redirect Server

A SIP redirect server accepts SIP requests, translates the destination address to an IP address and sends the translated IP address back to the device that sent the request. Then the client device that originally sent the request can send requests to the IP address that it received back from the redirect server. Redirect servers do not initiate SIP requests.

In the following example, you want to use client device A to call someone who is using client device C.

- Step 1** Client device A sends a call invitation for C to the SIP redirect server B.
- Step 2** The SIP redirect server sends the invitation back to A with C's IP address (or domain name).
- Step 3** Client device A then sends the call invitation to client device C.

Figure 15-9 SIP Redirect Server



----End

SIP Register Server

A SIP register server maintains a database of SIP identity-to-IP address (or domain name) mapping. The register server checks your user name and password when you register.

RTP

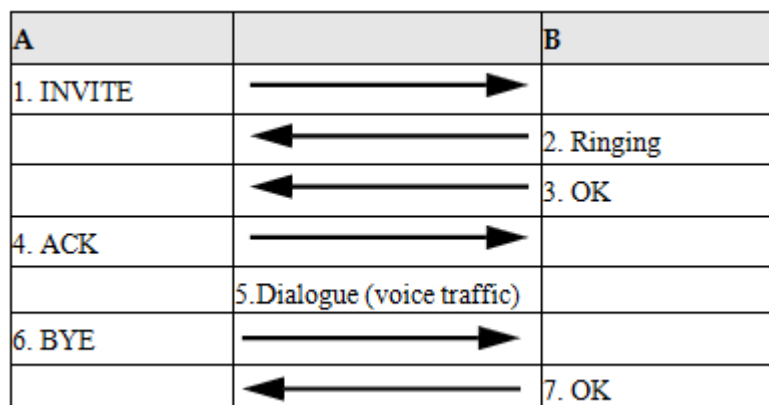
When you make a VoIP call using SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 3550 for details on RTP.

Pulse Code Modulation

Pulse Code Modulation (PCM) measures analog signal amplitudes at regular time intervals and converts them into bits.

SIP Call Progression

The following figures display the basic steps in the setup and tear down of a SIP call. A calls B.

Figure 15-10 SIP Call Progression

- Step 1** A sends a SIP INVITE request to B. This message is an invitation for B to participate in a SIP telephone call.
- Step 2** B sends a response indicating that the telephone is ringing.
- Step 3** B sends an OK response after the call is answered.
- Step 4** A then sends an ACK message to acknowledge that B has answered the call.
- Step 5** Now A and B exchange voice media (talk).
- Step 6** After talking, A hangs up and sends a BYE request.
- Step 7** B replies with an OK response confirming receipt of the BYE request and the call is terminated.

----End

Voice Coding

A codec (coder/decoder) codes analog voice signals into digital signals and decodes the digital signals back into analog voice signals. The LTE Device supports the following codecs.

- G.711 is a Pulse Code Modulation (PCM) waveform codec. PCM measures analog signal amplitudes at regular time intervals and converts them into digital samples. G.711 provides very good sound quality but requires 64 kbps of bandwidth.
- G.726 is an Adaptive Differential PCM (ADPCM) waveform codec that uses a lower bitrate than standard PCM conversion. ADPCM converts analog audio into digital signals based on the difference between each audio sample and a prediction based on previous samples. The more similar the audio sample is to the prediction, the less space needed to describe it. G.726 operates at 16, 24, 32 or 40 kbps.
- G.729 is an Analysis-by-Synthesis (AbS) hybrid waveform codec that uses a filter based on information about how the human vocal tract produces sounds. G.729 provides good sound quality and reduces the required bandwidth to 8 kbps.

MWI (Message Waiting Indication)

Enable Message Waiting Indication (MWI) enables your phone to give you a message-waiting (beeping) dial tone when you have a voice message(s). Your VoIP service provider must have a messaging system that sends message waiting status SIP packets as defined in RFC 3842.

15.6.3 Quality of Service (QoS)

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to provide bandwidth for real-time multimedia applications.

Type of Service (ToS)

Network traffic can be classified by setting the ToS (Type of Service) values at the data source (for example, at the LTE Device) so a server can decide the best method of delivery, that is the least cost, fastest route and so on.

15.6.4 Phone Services Overview

Supplementary services such as call hold, call waiting, and call transfer, are generally available from your VoIP service provider. The LTE Device supports the following services:

- Call Hold
- Call Waiting
- Making a Second Call
- Call Transfer
- Three-Way Conference
- Do not Disturb

NOTE

To take full advantage of the supplementary phone services available through the LTE Device's phone ports, you may need to subscribe to the services from your VoIP service provider.

The Flash Key

Flashing means to press the hook for a short period of time (a few hundred milliseconds) before releasing it. On newer telephones, there should be a "flash" key (button) that generates the signal electronically. If the flash key is not available, you can tap (press and immediately release) the hook by hand to achieve the same effect. However, using the flash key is preferred since the timing is much more precise. With manual tapping, if the duration is too long, it may be interpreted as hanging up by the LTE Device.

You can invoke all the supplementary services by using the flash key.

Europe Type Supplementary Phone Services

This section describes how to use supplementary phone services with the **Europe Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-Command before the default sub-Command time-out (2 seconds) expires or issue an invalid sub-Command, the current operation will be aborted.

Table 15-6 European Flash Key Commands

Command	Sub-command	Description
Flash	NA	Put a current call on hold to place a second call. Switch back to the call (if there is no second call).
Flash	0	Drop the call presently on hold or reject an incoming call which is waiting for answer.
Flash	1	Disconnect the current phone connection and answer the incoming call or resume with caller presently on hold.
Flash	2	1. Switch back and forth between two calls. 2. Put a current call on hold to answer an incoming call. 3. Separate the current three-way conference call into two individual calls (one is on-line, the other is on hold).
Flash	3	Create three-way conference connection.
Flash	*98#	Transfer the call to another phone.

European Call Hold

Call hold allows you to put a call (A) on hold by pressing the flash key.

If you have another call, press the flash key and then "2" to switch back and forth between caller A and B by putting either one on hold.

Press the flash key and then "0" to disconnect the call presently on hold and keep the current call on line.

Press the flash key and then "1" to disconnect the current call and resume the call on hold. If you hang up the phone but a caller is still on hold, there will be a remind ring.

European Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to a telephone number, you will hear a call waiting tone. Take one of the following actions.

- Reject the second call.
Press the flash key and then press "0".
- Disconnect the first call and answer the second call.
Either press the flash key and press "1", or just hang up the phone and then answer the phone after it rings.
- Put the first call on hold and answer the second call.
Press the flash key and then "2".

European Call Transfer

Do the following to transfer a call (that you have answered) to another phone number.

- Step 1** Press the flash key to put the caller on hold.
 - Step 2** When you hear the dial tone, dial "*98#" followed by the number to which you want to transfer the call.
 - Step 3** After you hear the ring signal or the second party answers it, hang up the phone.
- End

European Three-Way Conference

Use the following steps to make three-way conference calls.

- Step 1** When you are on the phone talking to someone, press the flash key to put the call on hold and get a dial tone.
 - Step 2** Dial a phone number directly to make another call.
 - Step 3** When the second call is answered, press the flash key and press "3" to create a three-way conversation.
 - Step 4** Hang up the phone to drop the connection.
 - Step 5** If you want to separate the activated three-way conference into two individual connections (one is on-line, the other is on hold), press the flash key and press "2".
- End

USA Type Supplementary Phone Services

This section describes how to use supplementary phone services with the **USA Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-Command before the default sub-Command time-out (2 seconds) expires or issue an invalid sub-Command, the current operation will be aborted.

Table 15-7 USA Flash Key Commands

Command	SUB- Command	Description
Flash	-	Put a current call on hold to place a second call. After the second call is successful, press the flash key again to have a three-way conference call. Put a current call on hold to answer an incoming call.
Flash	*98#	Transfer the call to another phone.

USA Call Hold

Call hold allows you to put a call (A) on hold by pressing the flash key.

If you have another call, press the flash key to switch back and forth between caller A and B by putting either one on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

USA Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to a telephone number, you will hear a call waiting tone.

Press the flash key to put the first call on hold and answer the second call.

USA Call Transfer

Do the following to transfer a call (that you have answered) to another phone.

- Step 1** Press the flash key to put the caller on hold.
- Step 2** When you hear the dial tone, dial "*98#" followed by the number to which you want to transfer the call.
- Step 3** After you hear the ring signal or the second party answers it, hang up the phone.

----End

USA Three-Way Conference

Use the following steps to make three-way conference calls.

- Step 1** When you are on the phone talking to someone (party A), press the flash key to put the caller on hold and get a dial tone.
- Step 2** Dial a phone number directly to make another call (to party B).
- Step 3** When party B answers the second call, press the flash key to create a three-way conversation.
- Step 4** Hang up the phone to drop the connection.
- Step 5** If you want to separate the activated three-way conference into two individual connections (with party A on-line and party B on hold), press the flash key.
- Step 6** If you want to go back to the three-way conversation, press the flash key again.
- Step 7** If you want to separate the activated three-way conference into two individual connections again, press the flash key. This time the party B is on-line and party A is on hold.

----End

16 LTE Status

16.1 Overview

Use the **LTE Status** screens to look at LTE related signaling status.

Figure 16-1 System Monitor > LTE Status

The page shows the present LTE Status in detail.

Refresh Interval: 5 seconds

Device Status			
Software Version	B2368_V1.00R001C00SPC1.009020	Device IMEI	35988053040480
Module Software Version	11.620.15.20.00	SIM Card IMSI	4600000602****
LTE Status			
Status	LTE	Connection Up Time	0 Day(s), 0 Hour(s), 3 Minute(s), 2 Second(s)
Service Provider	46000	ICCID	89860101234567890128
Signal Strength	-51 dBm	SINR	40 dB
RSRP	-69 dBm	RSRQ	-3 dB
Frequency Band	band 7	DL EARFCN	3151
Duplexing Mode	FDD	APN	Auto
RANK	2	Bandwidth	20MHz
Global Cell ID	4600000310EA0716	Physical Cell ID	22
CA Configuration Status	N/A	CA Activation Status	N/A
Data UL Packet Rate	0 kbps	Data DL Packet Rate	0 kbps
CQI	15 15	Data Roaming Status	Home Networking
ECGI	46000EA6715	ECI	0EA6715

17 Logs

17.1 Overview

The web configurator allows you to choose which categories of events and/or alerts to have the LTE Device log and then display the logs or have the LTE Device send them to an administrator (as e-mail) or to a syslog server.

17.1.1 What You Need To Know

The following terms and concepts may help as you read this chapter.

Alerts and Logs

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

Syslog Overview

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

Table 17-1 Syslog Severity Levels

CODE	SEVERITY
0	Emergency (EMERG): The system is unusable.
1	Alert (ALERT): Action must be taken immediately.

CODE	SEVERITY
2	Critical (CRIT): The system condition is critical.
3	Error (ERROR): There is an error condition on the system.
4	Warning (WARNING): There is a warning condition on the system.
5	Notice (NOTICE): There is a normal but significant condition on the system.
6	Informational (INFO): The syslog contains an informational message.
7	Debug (DEBUG): The message is intended for debug-level purposes.

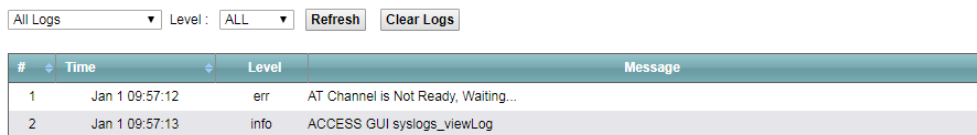
 NOTE

The LTE device supports sending ERROR, INFO, and DEBUG severity level logs.

17.2 The System Log Screen

Click **System Monitor > Log** to open the **System Log** screen. Use the **System Log** screen to see the system logs for the categories that you select in the upper left drop-down list box.

Figure 17-1 System Monitor > Log > System Log



All Logs	Level: ALL	Refresh	Clear Logs
#	Time	Level	Message
1	Jan 1 09:57:12	err	AT Channel is Not Ready, Waiting...
2	Jan 1 09:57:13	info	ACCESS GUI syslogs_viewLog

The following table describes the fields in this screen.

Table 17-2 System Monitor > Log > System Log

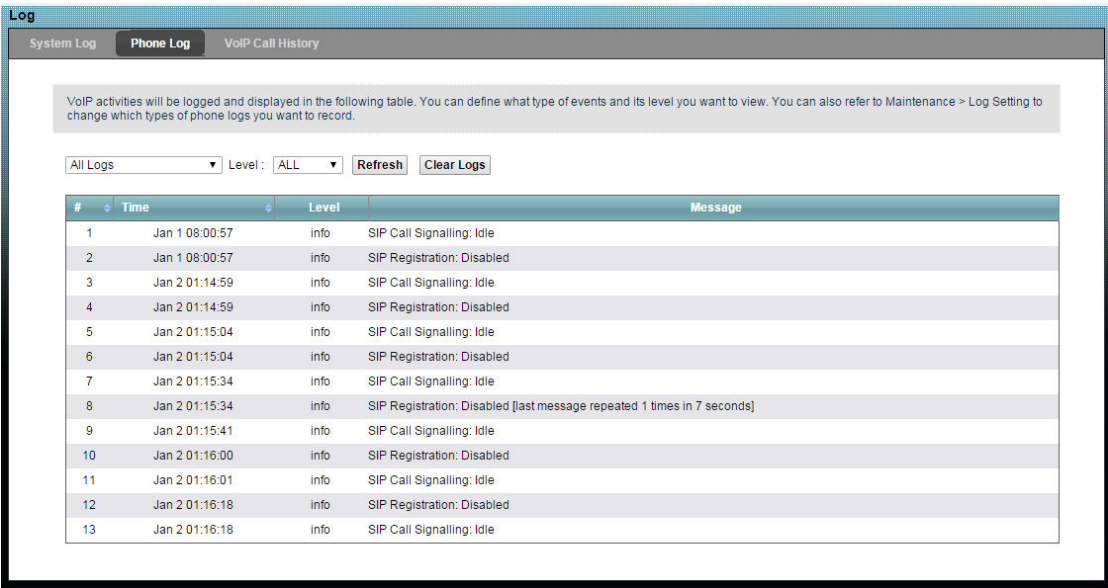
Label	Description
	Select the type of the logs that you want to search in the first drop-down list box. (Types: All Logs, WAN-DHCP, System Maintenance, Remote Management, TR-069, NTP, ETHER, DDNS, NAT, Attack, ACL, LTE)
Level	Select a severity level from this drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the LTE Device searches through all logs of that severity or higher. See Table 17-1 for more information about severity levels.
Refresh	Click this to renew the log screen.
Clear Logs	Click this to delete all the logs.

Label	Description
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the date and time the log was recorded.
Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Message	This field states the reason for the log.

17.3 The Phone Log Screen

Click **System Monitor > Log** to open the **Phone Log** screen. Use this screen to view phone logs and alert messages. You can select the type of log and level of severity to display.

Figure 17-2 System Monitor > Log > Phone Log



The following table describes the fields in this screen.

Table 17-3 System Monitor > Log > Phone Log

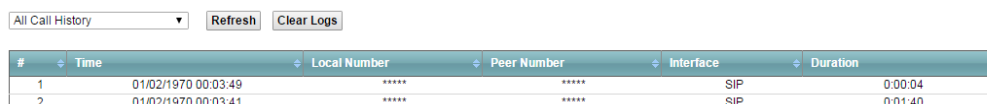
Label	Description
Select a category of logs to view from the drop-down list box. Select All Logs to view all logs.	
Level	Select the severity level that you want to view.
Refresh	Click this to renew the log screen.
Clear Logs	Click this to delete all the logs.

Label	Description
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Message	This field states the reason for the log.

17.4 The VoIP Call History Screen

Click **System Monitor > Log > VoIP Call History** to open the **VoIP Call History** screen. Use this screen to see the details of the calls performed on the LTE Device.

Figure 17-3 System Monitor > Log > VoIP Call History



#	Time	Local Number	Peer Number	Interface	Duration
1	01/02/1970 00:03:49	*****	*****	SIP	0:00:04
2	01/02/1970 00:03:41	*****	*****	SIP	0:01:40

The following table describes the fields in this screen.

Table 17-4 System Monitor > Log > VoIP Call History

Label	Description
Select a category of call records to view from the drop-down list box. Select All Call History to view all call records.	
Refresh	Click this to renew the log screen.
Clear Logs	Click this to delete all the logs.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the call was recorded.
Local Number	This field displays the phone number you used to make or receive this call.
Peer Number	This field displays the phone number you called or from which this call is made.
Interface	This field displays the type of the call.
Duration	This field displays how long the call lasted.

18 Traffic Status

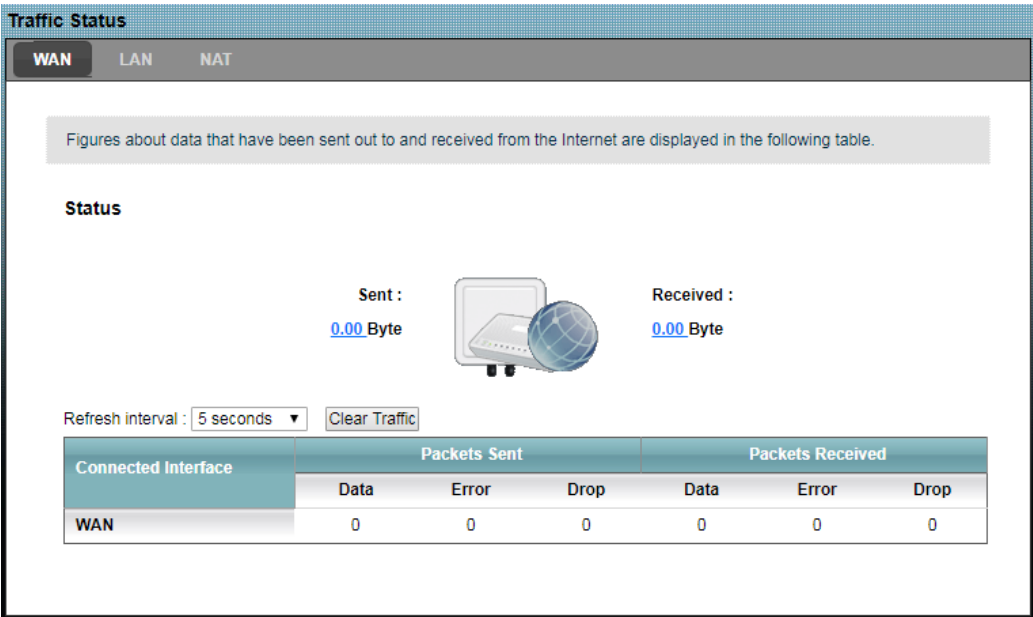
18.1 Overview

When using the administrator login, use the **Traffic Status** screens to look at network traffic status and statistics of the WAN, LAN interfaces and NAT.

18.2 The WAN Status Screen

Click **System Monitor > Traffic Status** to open the **WAN** screen. You can view the WAN traffic statistics in this screen. **WAN (VoIP)** displays when you enable dual APN.

Figure 18-1 System Monitor > Traffic Status > WAN



The following table describes the fields in this screen.

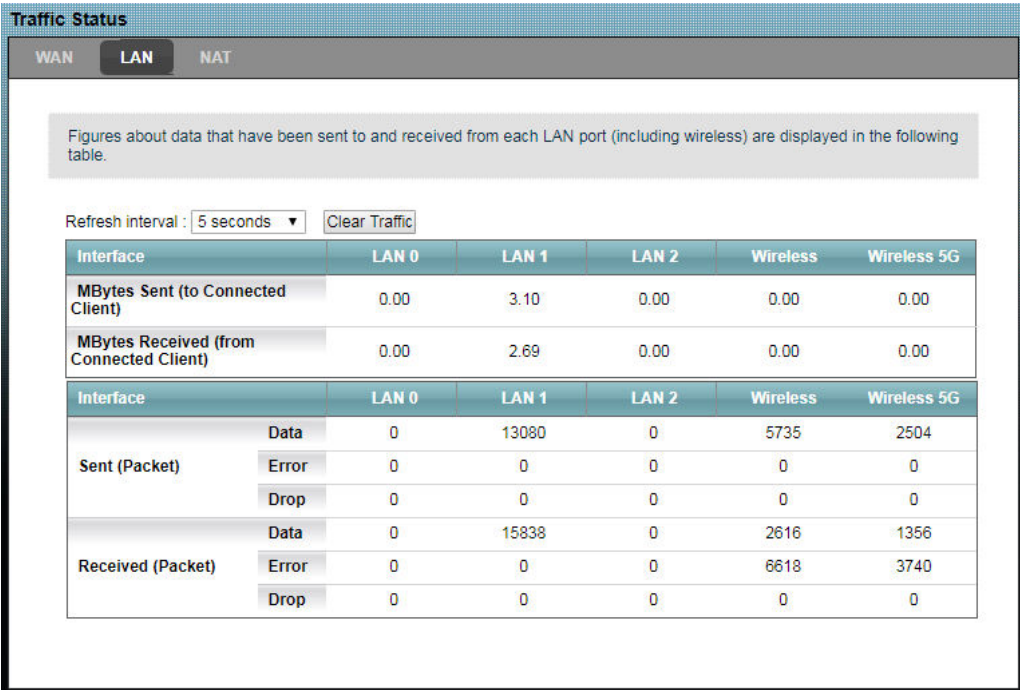
Table 18-1 System Monitor > Traffic Status > WAN

Label	Description
Status	This shows the number of bytes received and sent through the WAN interface of the LTE Device.
Refresh Interval	Select how often you want the LTE Device to update this screen from the drop-down list box.
Connected Interface	This shows the name of the WAN interface that is currently connected.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

18.3 The LAN Status Screen

Click **System Monitor > Traffic Status > LAN** to open the following screen. You can view the LAN traffic statistics in this screen.

Figure 18-2 System Monitor > Traffic Status > LAN



The following table describes the fields in this screen.

Table 18-2 System Monitor > Traffic Status > LAN

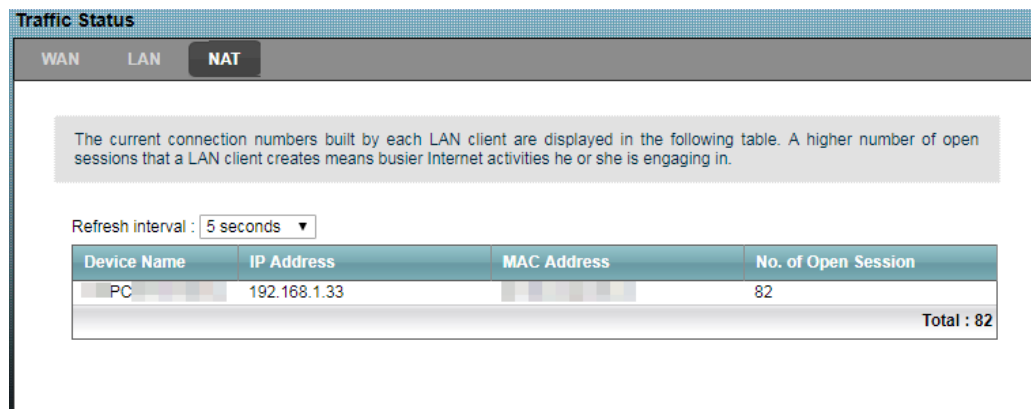
Label	Description
Refresh interval	Select how often you want the LTE Device to update this screen from the drop-down list box.
Interface	This shows the LAN or WLAN interface.
MBytes Sent	This indicates the number of megabytes transmitted on this interface.
MBytes Received	This indicates the number of megabytes received on this interface.
Interface	This shows the LAN or WLAN interface.
Sent (Packet)	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Received (Packet)	
Data	This indicates the number of received packets on this interface.

Label	Description
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

18.4 The NAT Status Screen

Click **System Monitor > Traffic Status > NAT** to open the following screen. You can view the NAT status of the LTE Device's client(s) in this screen.

Figure 18-3 System Monitor > Traffic Status > NAT



The following table describes the fields in this screen.

Table 18-3 System Monitor > Traffic Status > NAT

Label	Description
Refresh Interval	Select how often you want the LTE Device to update this screen from the drop-down list box.
Device Name	This shows the name of the client.
IP Address	This shows the IP address of the client.
MAC Address	This shows the MAC address of the client.
No. of Open Session	This shows the number of NAT sessions used by the client.

18.5 The VoIP Status Screen

Click **System Monitor > VoIP Status** to open the following screen. You can view the VoIP status in this screen.

Figure 18-4 System Monitor > VoIP Status

Information, such as whether a SIP account is registered and the total call volume made by a SIP account, can be viewed in the page.

Refresh interval: 5 seconds ▼

SIP Status

Account	Registration	URI	Message Waiting	Last Incoming Number	Last Outgoing Number
SIP 1	Up	+8613800034799@ims.mnc000.mcc460.3gppnetwork.org	NO	N/A	13800034799

Call Status

Account	Status	Codec	Peer Number
SIP 1	Idle	N/A	N/A

Phone Status

Phone No.	Outgoing Number	Incoming Number	Phone State
Phone 1	N/A	N/A	OFFHOOK

The following table describes the fields in this screen.

Table 18-4 System Monitor > VoIP Status

Label	Description
Refresh interval	Select how often you want the LTE Device to update this screen from the drop-down list box.
SIP Status	
Account	This column displays each SIP account in the LTE Device.
Registration	This field displays the current registration status of the SIP account. You can change this in the Status screen. Registered - The SIP account is registered with a SIP server. Not Registered - The last time the LTE Device tried to register the SIP account with the SIP server, the attempt failed. The LTE Device automatically tries to register the SIP account when you turn on the LTE Device or when you activate it. Inactive - The SIP account is not active. You can activate it in VoIP > SIP > SIP Account.
URI	This field displays the account number and service domain of the SIP account. You can change these in the VoIP > SIP screens.
Message Waiting	This field indicates whether or not there are any messages waiting for the SIP account.
Last Incoming Number	This field displays the last number that called the SIP account. The field is blank if no number has ever dialed the SIP account.
Last Outgoing Number	This field displays the last number the SIP account called. The field is blank if the SIP account has never dialed a number.
Call Status	
Account	This column displays the SIP account in the LTE Device.

Label	Description
Status	This field displays the current state of the phone call. Idle - There are no current VoIP calls, incoming calls or outgoing calls being made. Dial - The callee's phone is ringing. Ring - The phone is ringing for an incoming VoIP call. Process - There is a VoIP call in progress. DISC - The callee's line is busy, the callee hung up or your phone was left off the hook.
Codec	This field displays what voice codec is being used for a current VoIP call through a phone port.
Peer Number	This field displays the SIP number of the party that is currently engaged in a VoIP call through a phone port.
Phone Status	
Account	This field displays the phone accounts of the LTE Device.
Outgoing Number	This field displays the SIP number that you use to make calls on this phone port.
Incoming Number	This field displays the SIP number that you use to receive calls on this phone port.
Phone State	This field shows whether or the phone connected to the subscriber port is on-hook (ONHOOK) or off-hook (OFFHOOK).

19 User Account

19.1 Overview

You can configure system password for different user accounts in the **User Account** screen.
To enhance the security further, please change your password regularly.

19.2 The User Account Screen

Use the **User Account** screen to configure system password.
Click **Maintenance > User Account** to open the following screen.

Figure 19-1 Maintenance > User Account

Password that you use to log in the configuration interface can be changed in this page. Once a new password is given and saved, you need to use the new one next time when logging in the interface. The password length must be in the range of 8 to 15 characters. The password must be the mixture of following character types (at least three kinds): uppercase, lowercase, digit, other printable ASCII symbol code.

The password should not contain user name, or reversed user name, or more than two consecutive same characters.

To enhance the security further, please change your password regularly.

User Name :

admin ▼

Old Password :

New Password :

Retype to Confirm :

Apply

Cancel

The following table describes the Labels in this screen.

Table 19-1 Maintenance > User Account

Label	Description
User Name	You can configure the password for the user and admin accounts.
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays a dot (●) for each character you type. After you change the password, use the new password to access the LTE Device.
Retype to Confirm	Type the new password again for confirmation.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

20 Remote MGMT

20.1 Overview

These settings are available when you log in with the administrator username.

Remote MGMT allows you to manage your LTE Device from a remote location through the following interfaces:

- LAN and WLAN
- WAN only



The LTE Device is managed using the web configurator.

20.1.1 What You Need to Know

The following terms and concepts may help as you read this chapter.

20.2 The Remote MGMT Screen

Use this screen to decide what services you may use to access which LTE Device interface. Click **Maintenance > Remote MGMT** to open the following screen.



Only **admin** users can configure **Remote MGMT** when they log on. The **user** users do not have remote administrative authority and cannot configure **Remote MGMT**.

Figure 20-1 Maintenance > Remote MGMT

Remote MGMT enables various approaches to access this device remotely from a LAN/WAN connection.

Services	LAN/WLAN	WAN	Port
HTTPS	☒ Enable	☐ Enable	443
ICMP	☒ Enable	☐ Enable	N/A

Note :
Each service should not be set to the same port.
The TCP port 10000 & 10001 are reserved for the system.

The following table describes the fields in this screen.

Table 20-1 Maintenance > Remote MGMT

Label	Description
Services	This is the service you may use to access the LTE Device.
LAN/WLAN	Select the Enable check box for the corresponding services that you want to allow access to the LTE Device from the LAN and WLAN.
WAN	Select the Enable check box for the corresponding services that you want to allow access to the LTE Device from the WAN.
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

20.3 The TR069 Screen

TR-069 defines how Customer Premise Equipment (CPE), for example your LTE Device, can be managed over the WAN by an Auto Configuration Server (ACS). TR-069 is based on sending Remote Procedure Calls (RPCs) between an ACS and a client device. RPCs are sent in Extensible Markup Language (XML) format over HTTP or HTTPS.

An administrator can use an ACS to remotely set up the LTE Device, modify settings, perform firmware upgrades as well as monitor and diagnose the LTE Device. You have enable the device to be managed by the ACS and specify the ACS IP address or domain name and username and password.

Please refer to the TR-069 model tree for TR-069 settings and notice items.

Click **Maintenance > Remote MGMT > TR069** to open the following screen. Use this screen to configure your LTE Device to be managed by an ACS.

Figure 20-2 Maintenance > Remote MGMT > TR069

Remote Management

Remote Management TR069

TR069 offers remote management control service.

TR-069 : ☒ Active

ACS Server URL :

ACS Username :

ACS Password :

Periodic Inform : ☒ Enable

Periodic Inform Interval : sec (Min. 30 sec)

Connection Request Port : (1025 ~ 65535)

Connection Request Username :

Connection Request Password :

Apply Cancel

The following table describes the fields in this screen.

Table 20-2 Maintenance > Remote MGMT > TR069

Label	Description
TR-069	Select Active to activate remote management via TR-069 on the WAN.
ACS Server URL	Enter the URL or IP address of the auto-configuration server.
ACS Username	Select the Enable check box for the corresponding services that you want to allow access to the LTE Device from the WAN.
ACS Password	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Periodic Inform	Select this to set a time interval (in seconds) at which the LTE Device sends information to the auto-configuration server.
Periodic Inform Interval	Enter the time interval (in seconds) at which the LTE Device sends information to the auto-configuration server.
Connection Request Port	Specify the port number the ACS uses to request a connection to the LTE Device.
Connection Request Username	Enter the username for authenticating the ACS when it requests a connection to the LTE Device.
Connection Request Password	Enter the password for authenticating the ACS when it requests a connection to the LTE Device.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

21 System

21.1 Overview

Configure system settings, including the host name, domain name and the inactivity time-out interval in the **System** screen. Refresh the security key in the **Encryption Key** screen.

21.1.1 What You Need to Know

The following terms and concepts may help as you read this chapter.

Domain Name

This is a network address that identifies the owner of a network connection. For example, in the network address *www.example.com/support/files*, the domain name is *www.example.com*.

Encryption Key

The LTE Device has a preset encryption key for secure communication between the IDU and ODU. It is recommended to refresh the encryption key of the product, when the device is first used.

21.2 The System Screen

Use the **System** screen to configure the system's host name, domain name, and inactivity time-out interval.

The **Host Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name". Find the system name of your Windows computer.

In Windows 7, click **Start, Computer, Properties**. Note the entry in the **Full computer name** field and enter it as the LTE Device **System Name**.

Click **Maintenance > System** to open the following screen.

Figure 21-1 Maintenance > System

System

System Encryption Key

You can assign a unique name to this device so it can be recognized easily on your network. Besides, you can decide when to automatically sign out the administrator account after he or she is idle for a period of time.

Host Name: router

Domain Name: home

Administrator Inactivity Timer: 5 (minutes, range 1-15)

ODU LED Light Control: ☒ Light On ☐ Light Off

Apply Cancel

The following table describes the Labels in this screen.

Table 21-1 Maintenance > System

Label	Description
Host Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Administrator Inactivity Timer	Type how many minutes a management session (either via the web configurator) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks.
ODU LED Light Control	This switch turns the ODU's LED indicators on or off. Select Light On to turn on the ODU's LED indicators. Select Light Off to turn them off.
Apply	Click this to save your changes back to the LTE Device.
Cancel	Click this to begin configuring this screen afresh.

21.3 The Encryption Key Screen

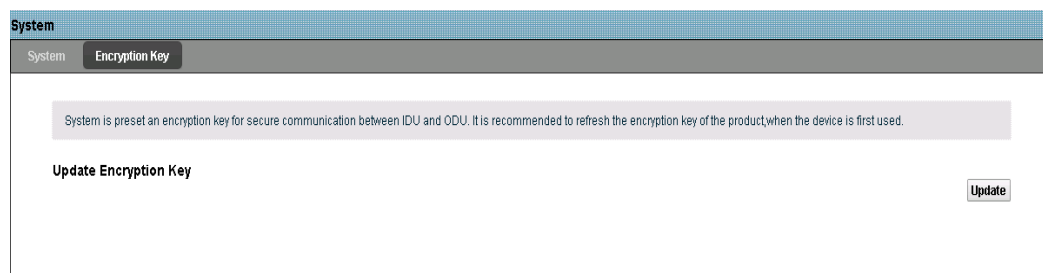
A preset encryption key secures communication between the IDU and ODU. It is recommended to refresh the encryption key of the product, when the device is first used.

There are three encryption key update scenarios to consider:

21.3.1 Normal: IDU and ODU Bundle

Step 1 Click **Maintenance > System > Encryption Key** to open the following screen.

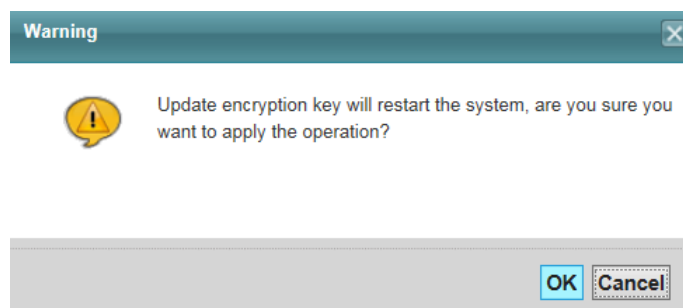
Figure 21-2 Maintenance > System > Encryption Key



Step 2 Click **Update** to update the encryption key.

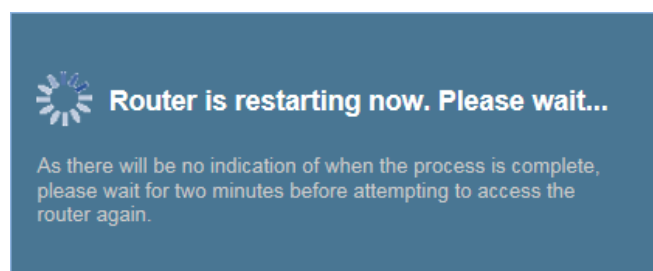
Step 3 A popup screen asks you to confirm. Click **OK**.

Figure 21-3 Maintenance > System > Encryption Key > Update



Step 4 Wait for the LTE Device to reboot.

Figure 21-4 Maintenance > System > Encryption Key > Update: Restarting



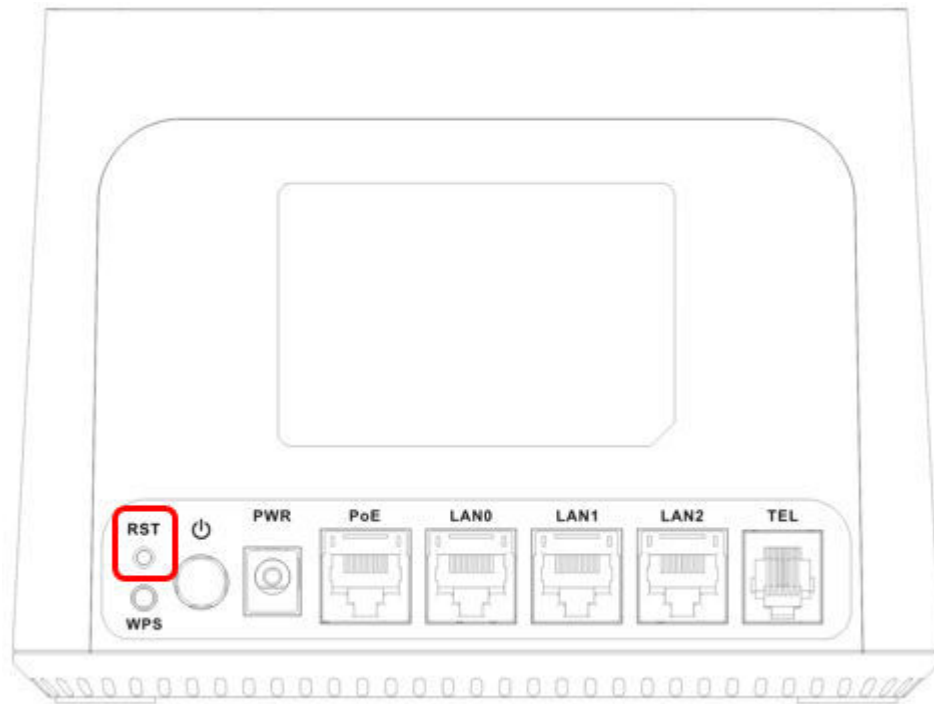
----End

21.3.2 New ODU with Old IDU

Do the following if you replace the ODU but still have the old IDU.

Step 1 Press the IDU reset button over 10 seconds and release, and wait for the device to reboot.

Figure 21-5 IDU Reset Button



Step 2 After rebooting the IDU, the Wi-Fi user name and password can be found on the label of the old IDU.

----End

21.3.3 New IDU with Old ODU

Step 1 If you replace the IDU but still have the old ODU, refer to [21.3.1 Normal: IDU and ODU Bundle](#) to update the encryption key.

1. Click **Maintenance > System > Encryption Key** to open the **Encryption Key** screen.
2. Click **Update** to update the encryption key.
3. A popup screen asks you to confirm. Click **OK**.
4. Wait for the LTE Device to reboot.

Step 2 Log in to the web configurator, choose **Maintenance > Backup/Restore > Back to Factory Defaults**, select **Reset**, and wait for the IDU to reboot.

Step 3 After the restart, the Wi-Fi user name and password can be found on the label of the new IDU.

----End

22 Time Setting

22.1 Overview

You can configure the system's time and date in the **Time Setting** screen.

22.2 The Time Setting Screen

To change your LTE Device's time and date, click **Maintenance > Time Setting**. The screen appears as shown. Use this screen to configure the LTE Device's time based on your local time zone.

Figure 22-1 Maintenance > Time Setting

In order to get a correct time for the device, fill in a time server address, select the time zone where this device is physically located, and complete the daylight saving settings if needed.

Current Date/Time

Current Time : 08:16:44
Current Date : 2017-01-01

Time and Date Setup

NTP : ☒ Enable ☐ Disable

Time Protocol : NTP

Time Server Address :

Manual Time : (HHMMSS)

Manual Date : (YYYYMMDD)

Time Zone

Time Zone : (GMT+01:00) Berlin, Stockholm, Rome, Bern, Brussels, Vienna ▼

☐ Daylight Savings

Start Date : ▼ ▼ Of ▼ (2008-01-01) at o'clock

End Date : ▼ ▼ Of ▼ (2008-01-01) at o'clock

The following table describes the fields in this screen.

Table 22-1 Maintenance > Time Setting

Label	Description
Current Date/Time	

Label	Description
Current Time	This field displays the time of your LTE Device.
Current Date	This field displays the date of your LTE Device.
Time and Date Setup	
NTP	Select Enable to have the LTE Device get the time from the NTP server you specify. Select Disable to enter the LTE Device's time manually.
Time Protocol	This shows the time service protocol that your time server sends when you turn on the LTE Device.
Time Server Address	Enter the IP address or URL (up to 31 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Manual Time	Use these fields to manually set the time in hours, minutes, and seconds format.
Manual Date	Use these fields to manually set the date in year, month, and day format.
Time Zone	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected Daylight Savings . The o'clock field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select Second, Sunday, March and type 2 in the o'clock field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, March . The time you type in the o'clock field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).

Label	Description
End Date	Configure the day and time when Daylight Saving Time ends if you selected Daylight Savings. The o'clock field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select First, Sunday, November and type 2 in the o'clock field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, October. The time you type in the o'clock field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click Apply to save your changes.

23 Log Setting

23.1 Overview

You can configure which logs and/or immediate alerts the LTE Device records in the **Log Setting** screen.

23.2 The Log Setting Screen

To change your LTE Device's log settings, click **Maintenance > Log Setting**. The screen appears as shown.

Figure 23-1 Maintenance > Log Setting

Active Log and Select Level

Log Category

VoIP

☐ VoIP-Call Statistics

☒ VoIP-SIP Call Signaling

☒ VoIP-SIP Registrations

☐ VoIP-Phone Event

☐ VoIP-Misc

System

☒ LTE

☒ DHCP

☒ System Maintenance

☒ Remote Management

☒ TR-069

☐ NTP

☐ DDNS

☐ NAT

☐ Attack

☐ ACL

Log Level

ALL

ALL

ALL

ALL

ALL

ALL

ALL

ALL

ALL

ALL

ALL

ALL

ALL

ALL

ALL

Apply

Cancel

The following table describes the fields in this screen.

Table 23-1 Maintenance > Log Setting

Label	Description
Active Log and Select Level	
Log Category	Select the categories of logs that you want to record.
Log Level	Select the severity level of logs that you want to record. If you want to record all logs, select ALL .
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

24 Software Upgrade

24.1 Overview

This chapter explains how to upload new firmware (software) to your LTE Device.

CAUTION

Only use firmware for your device's specific model. Refer to the Label on the bottom of your LTE Device.

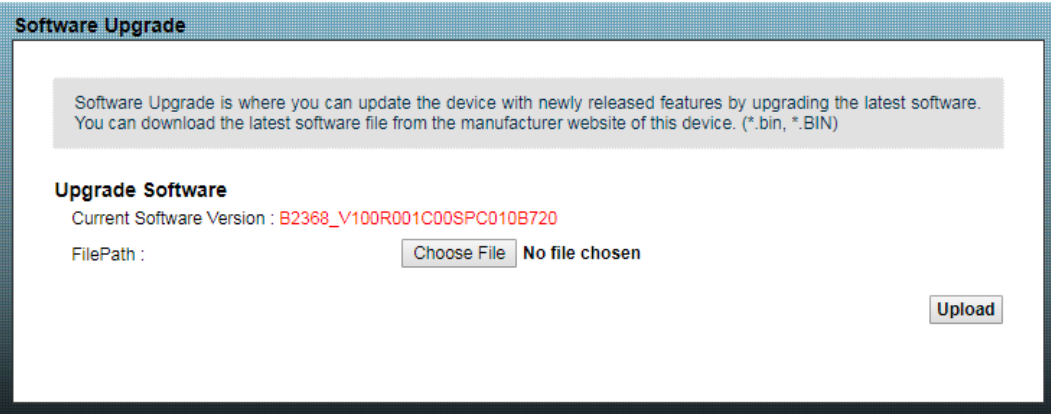
24.2 The Software Upgrade Screen

Click **Maintenance > Software Upgrade** to open the following screen. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to five minutes. After a successful upload, the system will reboot.

CAUTION

Do NOT turn off the LTE Device while firmware upload is in progress!

Figure 24-1 Maintenance > Software Upgrade



The following table describes the Labels in this screen.

Table 24-1 Maintenance > Software Upgrade

Label	Description
Upgrade Software	
Current Software Version	This is the present firmware version.
File Path	Click Choose File to browse to the location of the file you want to upload. Note: If both the modem and router need firmware upgrades, update the modem firmware first and then the router.
Upload	After you select the file, click Upload to begin the upload process. This process may take up to five minutes.

After you see the firmware updating screen, wait a few minutes before logging into the LTE Device again.

Figure 24-2 Firmware Upgrading Warning

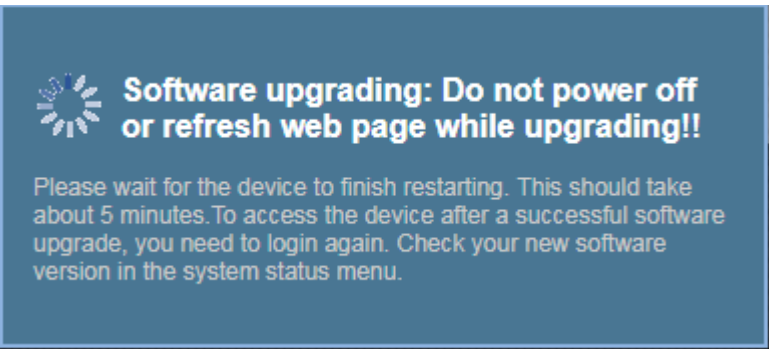


Figure 24-3 Firmware Upgrading Warning: Upgrading

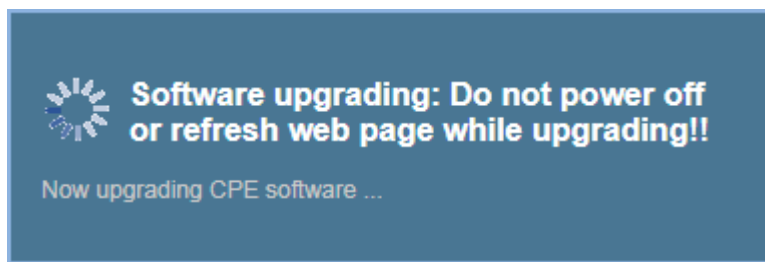
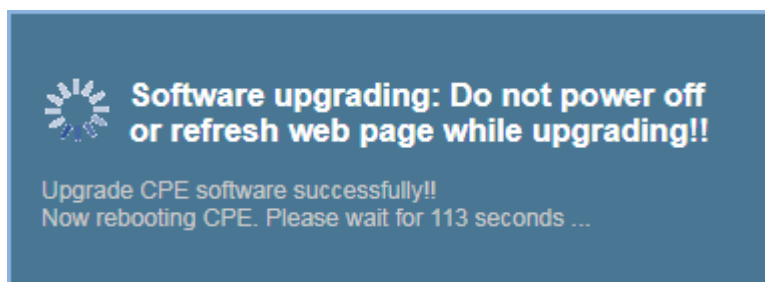
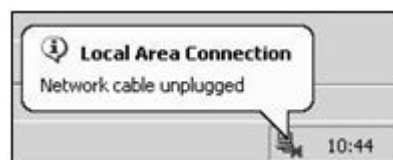


Figure 24-4 Firmware Upgrading Warning: Rebooting



The LTE Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 24-5 Network Temporarily Disconnected



After two minutes, log in again and check your new firmware version in the **System Info** screen.

If the upload was not successful, an error screen will appear. Click **OK** to go back to the **Software Upgrade** screen.

25 Online Upgrade

25.1 Overview

This chapter explains how to use the **Online Upgrade** screen to upload new firmware to your LTE Device or your LTE Device's LTE module.

CAUTION

Only use firmware for your device's specific model. Refer to the label on the bottom of your LTE Device.

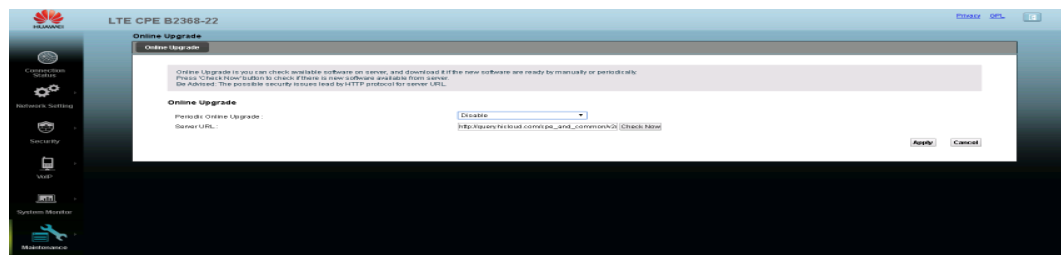
25.2 The Online Upgrade Screen

Click **Maintenance > Online Upgrade** to open the following screen. The upload process uses HTTPS (Hypertext Transfer Protocol Secure) or HTTP (Hypertext Transfer Protocol) and may take up to five minutes. After a successful upload, the system will reboot.

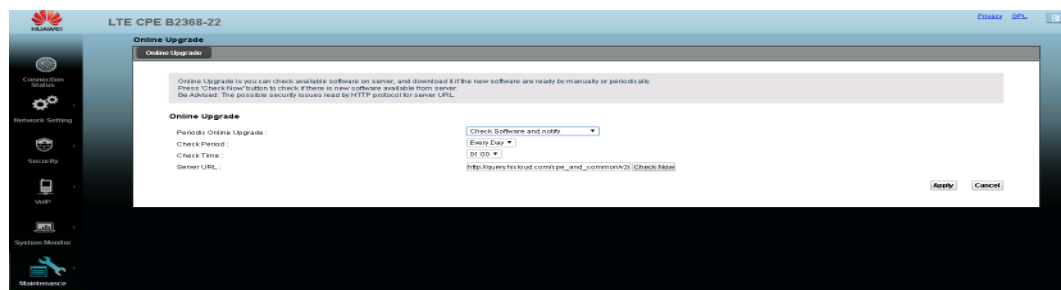
CAUTION

Do NOT turn off the LTE Device while firmware upload is in progress!

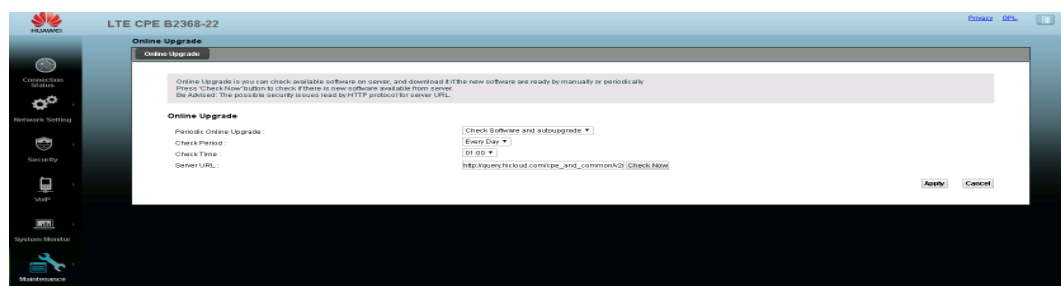
In the **Periodic Online Upgrade field**, select **Disable** to turn off remote automatic detection and automatic upgrade functions.

Figure 25-1 Maintenance > Online Upgrade: Disable

In the **Periodic Online Upgrade** field, select **Check Software and notify** to have the LTE Device periodically check the server and notify you when there is new software. When the LTE Device finds new firmware, it displays a popup when you go to the **Connection Status** screen or the **Online Upgrade** screen.

Figure 25-2 Maintenance > Online Upgrade: Check Software and notify

In the **Periodic Online Upgrade** field, select **Check Software and autoupgrade** to have the LTE Device periodically check the server and automatically upgrade when there is new software.

Figure 25-3 Maintenance > Online Upgrade: Check Software and autoupgrade

When you choose **Check Software and notify** or **Check Software and autoupgrade**; you can choose when to check (**Check Time**).



Use the server URL provided by your service provider for your LTE Device!

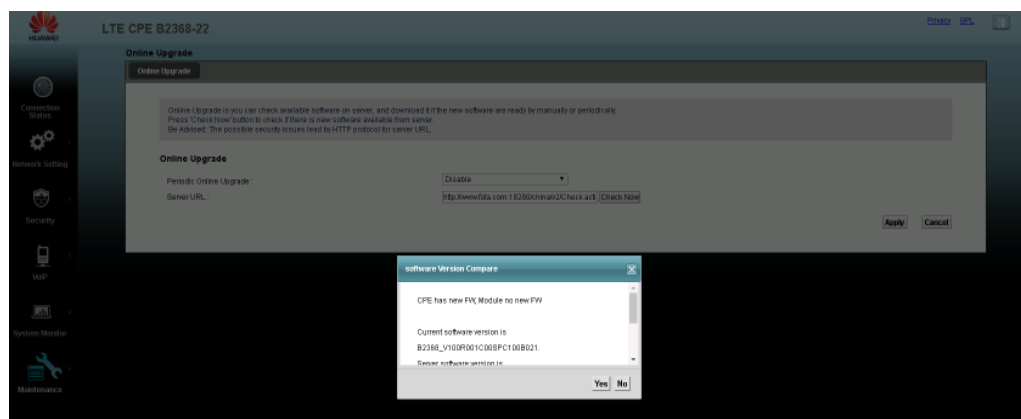
Enter the update server's address in the **Server URL** field and click the **Apply** button to check if new firmware is available from the server. It is recommended to use an HTTPS address although HTTP is also supported.

25.3 Online Upgrade Types

You can upgrade the firmware online when:

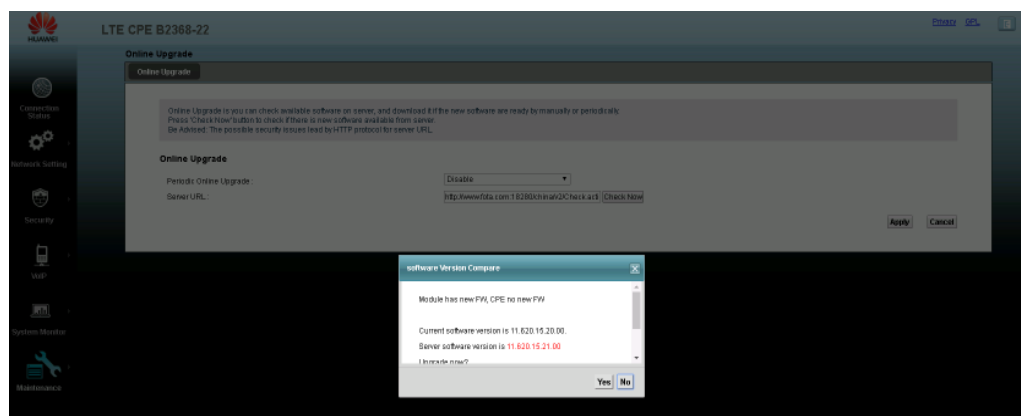
There is new firmware for the LTE Device (CPE) but not for the LTE module.

Figure 25-4 Maintenance > Online Upgrade: CPE Firmware Only



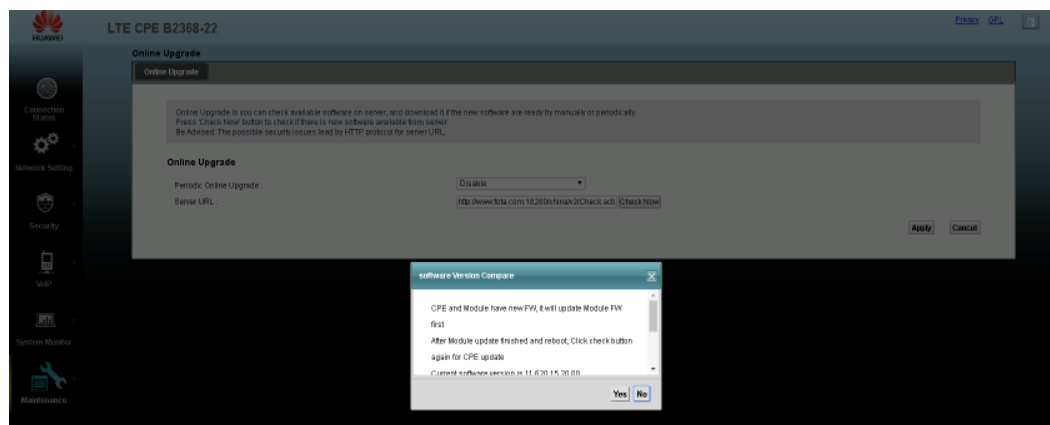
There is new firmware for the LTE module, but not for the LTE Device.

Figure 25-5 Maintenance > Online Upgrade: Module Firmware Only



There is new firmware for both the LTE Device and new firmware for the LTE module. In this situation, the LTE Device upgrades the LTE module's firmware first.

Figure 25-6 Maintenance > Online Upgrade: CPE and Module Firmware



25.4 Online Upgrade Procedures

To upgrade the LTE Device or LTE module firmware

- Step 1** Click **Maintenance > Online Upgrade**. Set **Periodic Online Upgrade** to **Disable**. Fill in the firmware server URL, click **Apply** and click **Check Now**.

Figure 25-7 Maintenance > Online Upgrade: Enter URL



- Step 2** A popup window shows if there is new firmware.

Figure 25-8 Maintenance > Online Upgrade: New Module Firmware Popup



Step 3 Click the **Yes** button to have the LTE Device upgrade the firmware. During the process, you will see a popup window to show the system is upgrading. If you don't need to upgrade the firmware, click **No** or the **X** button to close the popup window and skip the firmware upgrade.

Figure 25-9 Maintenance > Online Upgrade: Firmware Upgrading Warning

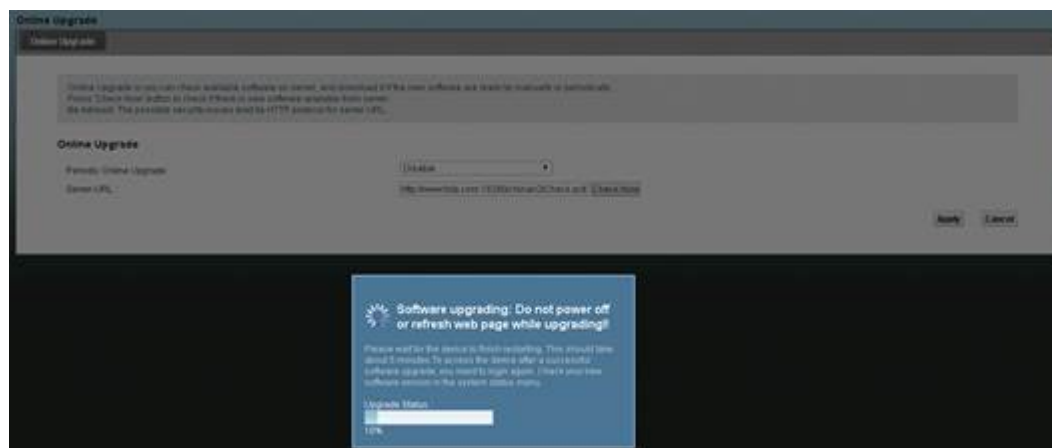


Figure 25-10 Maintenance > Online Upgrade: Firmware Upgrading 25%

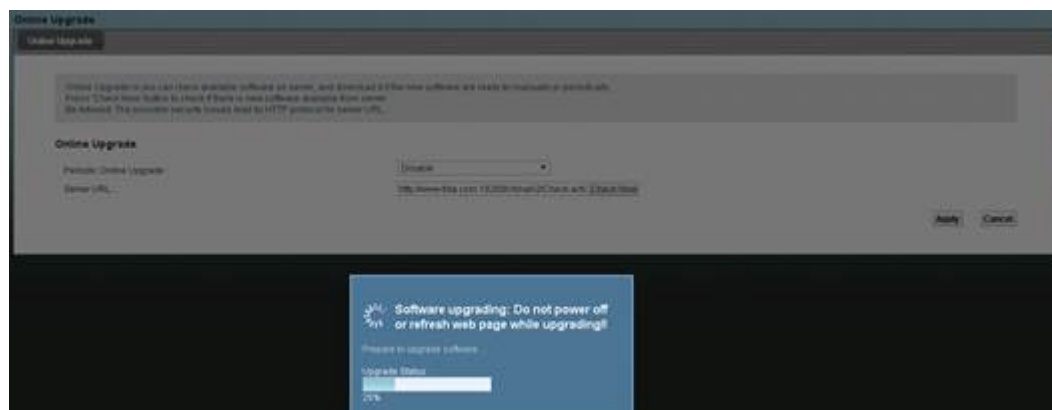
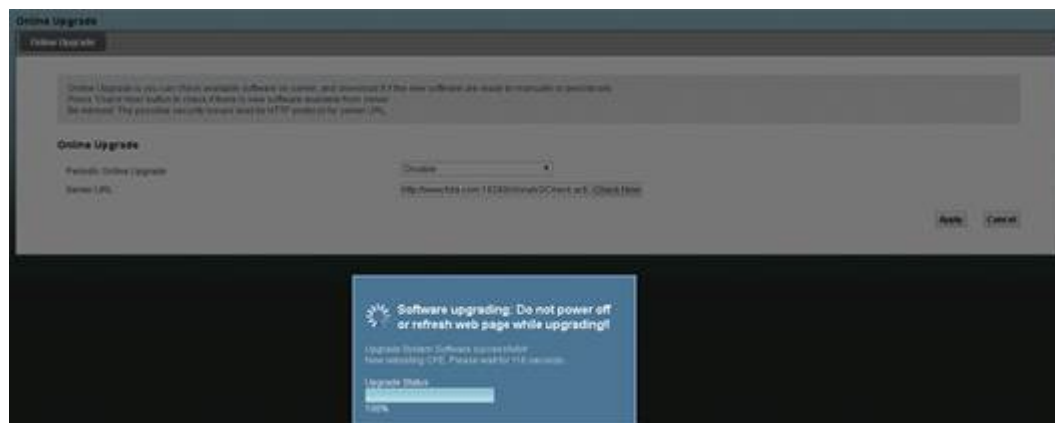


Figure 25-11 Maintenance > Online Upgrade: Firmware Upgrading 50%



Figure 25-12 Maintenance > Online Upgrade: Firmware Upgrading 100%



- Step 4** Normally, the upgrade process may take around five minutes. The login screen appears again after the upgrade is done.
- During the online upgrade process, you only need to confirm to update. You do not need to use other software update tools or hardware devices.
 - If the online upgrade process fails, the LTE Device will go back to the previous firmware version and state.
- Step 5** Log back into the LTE Device and use **System Monitor > LTE Status** to check if the module firmware version is correct.

Figure 25-13 System Monitor > LTE Status: Checking the Firmware Version

The screenshot shows the 'LTE Status' page. At the top, it says 'The page shows the present LTE Status in detail'. Below this, there's a 'Refresh interval' dropdown set to '5 seconds'. The main content is a table with two sections: 'Device Status' and 'LTE Status'.

Device Status		LTE Status	
Software Version	B2368_V100R001C00DFC010T	Device IMEI	0000000000000000
Module Software Version	H182015.21.00	Sim Card IMSI	4600000000000000
Status	Down off	Connection Up Time	0 Day(s), 0 Hour(s), 0 Minute(s), 0 Second(s)
Service Provider	N/A	ICCID	88880122012020130202
Signal Strength	N/A	SNR	N/A
RSCP	N/A	RSCQ	N/A
Frequency Band	N/A	UL EARFCN	N/A
Encoding Mode	N/A	APN	N/A
PARA	N/A	Bandwidth	N/A
Global Cell ID	N/A	Physical Cell ID	N/A
CA Configuration Status	N/A	CA Activation Status	N/A
Data UL Packet Rate	N/A	Data DL Packet Rate	N/A
CSK	N/A	Data Retaining Status	Home Networking
ECN	N/A	ECN	N/A

----End

To upgrade both the LTE Device and LTE module firmware

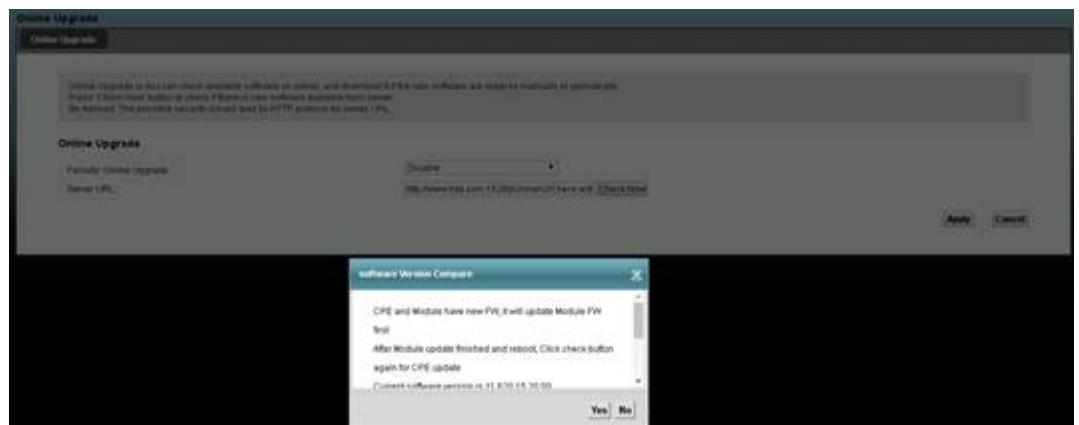
- Step 1** Click **Maintenance > Online Upgrade**. Set **Periodic Online Upgrade** to **Disable**. Fill in the firmware server URL and click **Check Now**.

Figure 25-14 Maintenance > Online Upgrade: Enter URL



Step 2 The popup window shows below if there is new firmware. The LTE Device will upgrade the module first if it detects new firmware for both the LTE Device and the LTE module. After it finishes upgrading the module, you can use the **Online Upgrade** screen again to upgrade the LTE Device firmware.

Figure 25-15 Maintenance > Online Upgrade: New CPE and Module Firmware Popup



Step 3 Click the **Yes** button to upgrade the firmware. During the process, you will see a popup window to show the system is upgrading. If you don't need to upgrade the firmware, click **No** or the **X** button to close the popup window and skip the firmware upgrade.

Figure 25-16 Maintenance > Online Upgrade: Firmware Upgrading Warning

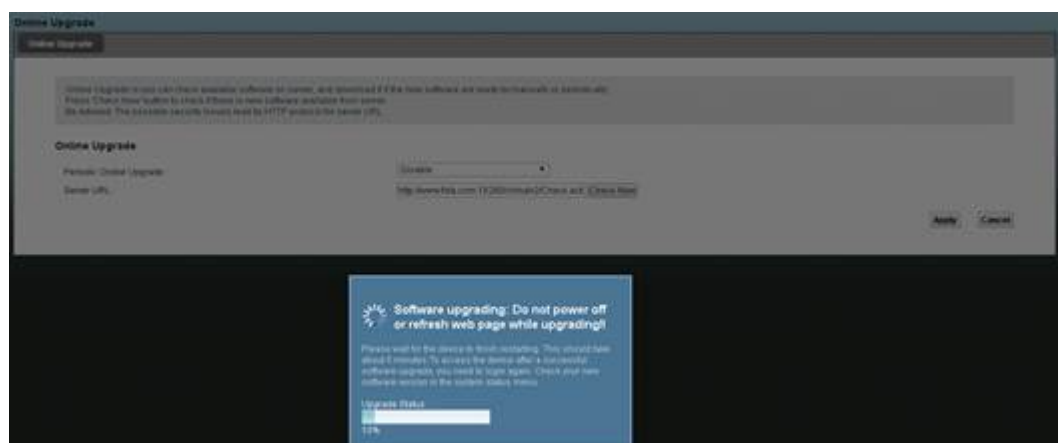


Figure 25-17 Maintenance > Online Upgrade: Firmware Upgrading 25%

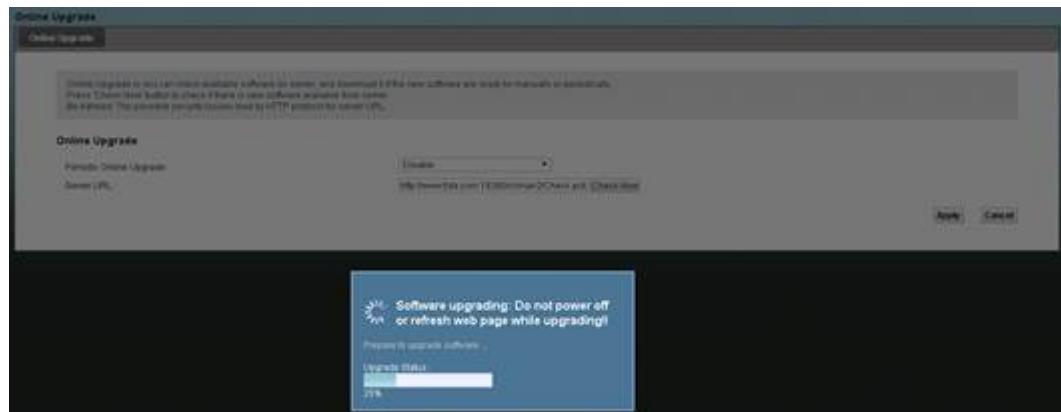


Figure 25-18 Maintenance > Online Upgrade: Firmware Upgrading 50%

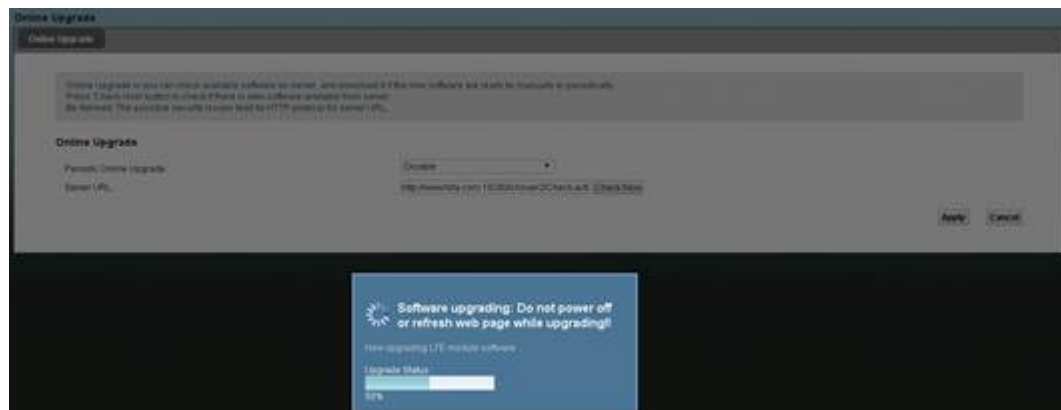
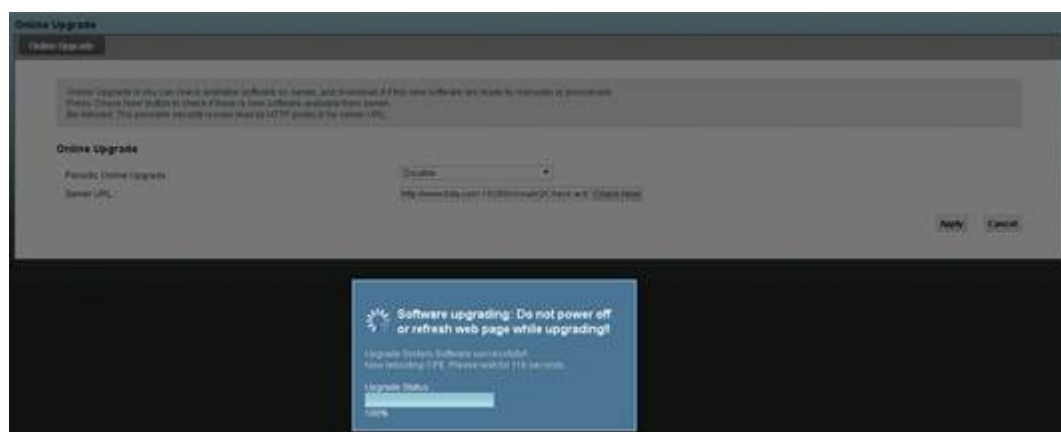


Figure 25-19 Maintenance > Online Upgrade: Firmware Upgrading 100%



Step 4 The login page appears again after the upgrade is complete. Log back into the LTE Device and use **System Monitor > LTE Status** to check if the module firmware version is correct.

Figure 25-20 System Monitor > LTE Status: Checking the Firmware Version



LTE Status			
This page shows the present LTE Status in detail.			
Refresh interval: 5 seconds			
Device Status		Device IMEI	
Software Version	B2368_V100R001C00SPC000T	Device IMEI	800000000000000
Module Software Version	V1.020.15.21.00	SIM Card IMEI	400000000000000
LTE Status		Connection Up Time	
Status	Down: all	Connection Up Time	0 Days, 0 Hours, 0 Minutes, 0 Seconds
Service Provider	HUA	ECGI	800000000000000
Signal Strength	HUA	SIMI	HUA
RSRP	HUA	RSRQ	HUA
Frequency Band	HUA	DL EARTH	HUA
Duplexing Mode	HUA	APN	HUA
RAN	HUA	Bandwidth	HUA
Global Cell ID	HUA	Physical Cell ID	HUA
CA Configuration Status	HUA	CA Activation Status	HUA
Data DL Packet Rate	HUA	Data DL Packet Rate	HUA
CQI	HUA	Data Roaming Status	HUA
ECGI	HUA	ECI	HUA

Step 5 Click **Maintenance > Online Upgrade** again and click **Check Now**. This time the popup window just shows that there is new LTE Device firmware. Click **Yes** to upgrade the LTE Device firmware.

Figure 25-21 Maintenance > Online Upgrade: New CPE Firmware Popup

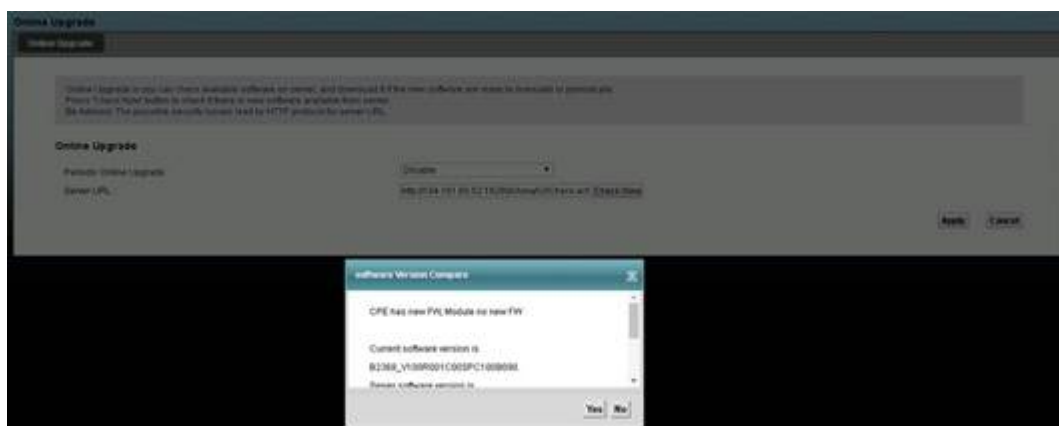
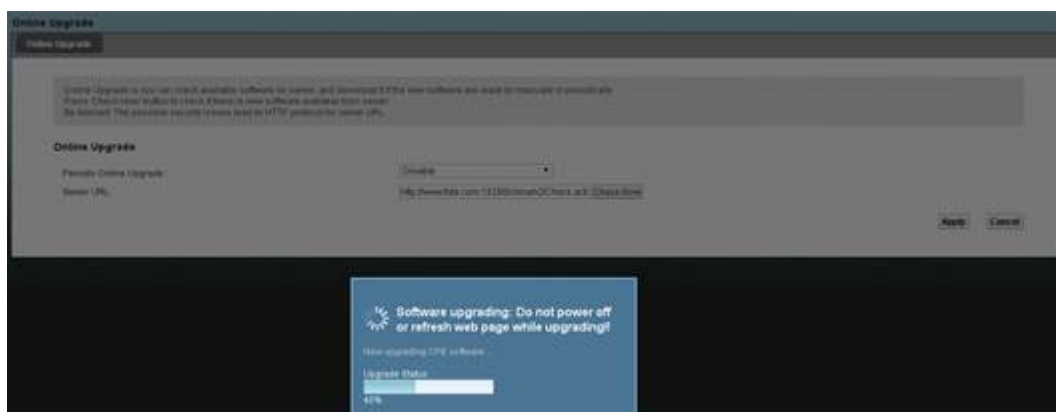


Figure 25-22 Maintenance > Online Upgrade: Firmware Upgrading 40%



Step 6 The login screen appears again after the upgrade is complete. Log back into the LTE Device and use **System Monitor > LTE Status** to check if the firmware version is correct.

Figure 25-23 System Monitor > LTE Status: Checking the Firmware Version

LTE Status

The page shows the present LTE Status in detail.

Refresh Interval: 5 seconds

Device Status	
Software Version	B2368_V100R001C00SPC100B091
Module Software Version	11.620.15.21.00
Device IMEI	355968053040480
SIM Card IMSI	46000000003****

LTE Status	
Status	LTE
Service Provider	46000
Signal Strength	-62 dBm
RSRP	-86 dBm
Frequency Band	band 41
Duplexing Mode	TDD
RANK	1
Global Cell ID	4600000010EA679B
CA Configuration Status	N/A
Data UL Packet Rate	0 kbps
COI	15
ECGI	460000EA679B
Connection Up Time	0 Day(s), 0 Hour(s), 0 Minute(s), 14 Second(s)
ICCID	89860101234567890128
SINR	22 dB
RSRQ	-3 dB
DL EARFCN	39750
APN	Auto / wtx
BandWidth	20MHz
Physical Cell ID	155
CA Activation Status	N/A
Data DL Packet Rate	0 kbps
Data Roaming Status	Home Networking
ECI	0EA679B

----End

26 Backup/Restore

26.1 Overview

The **Backup/Restore** screen allows you to backup and restore device configurations. You can also reset your device settings back to the factory default.

26.2 The Backup/Restore Screen

- Step 1** Click **Maintenance > Backup/Restore**. Information related to factory defaults, backup configuration, and restoring configuration appears in this screen, as shown in the following figure.

Figure 26-1 Maintenance > Backup/Restore

Backup Log
Click "Backup Log" to save the all logs of your system to your computer.

Backup Configuration
Click Backup to save the current configuration of your system to your computer.

Restore Configuration
To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.
(* .xml, *.XML, *.rom, *.ROM)
FilePath : No file chosen

Back to Factory Defaults
Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the LAN IP address will be 192.168.1.1 DHCP will be reset to server.

----End

Backup Log

- Step 1** Backup Log allows you to back up (save) the LTE Device's logs to a file on your computer. Once your LTE Device has unusual behavior, it is highly recommended that you back up your

log file before making any changes. The backup log file will be useful in case you need to ask the customer service.

Step 2 Click **Backup Log** to save the LTE Device's logs to your computer.

----End

Backup Configuration

Step 1 Backup Configuration allows you to back up (save) the LTE Device's current configuration to a file on your computer. Once your LTE Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Step 2 Click **Backup** to save the LTE Device's current configuration to your computer.

----End

Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your LTE Device.

Table 26-1 Restore Configuration

Label	Description
File Path	Type in the location of the file you want to upload in this field or click Browse ... to find it.
Browse...	Click this to find the file you want to upload.
Upload	Click this to begin the upload process.

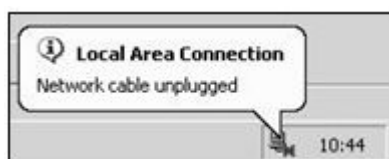
⚠ CAUTION

Do not turn off the LTE Device while configuration file upload is in progress.

After the LTE Device configuration has been restored successfully, the login screen appears. Login again to restart the LTE Device.

The LTE Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 26-2 Network Temporarily Disconnected



If you restore the default configuration, you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1).

If the upload was not successful, an error screen will appear. Click **OK** to go back to the Configuration screen.

Reset to Factory Defaults

- Click the **Reset** button to clear all user-entered configuration information and return the LTE Device to its factory defaults. The following warning screen appears.

Figure 26-3 Reset Warning Message

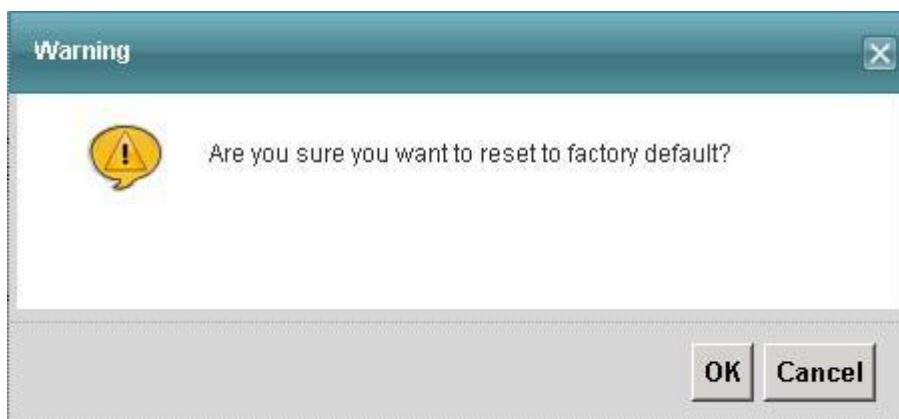
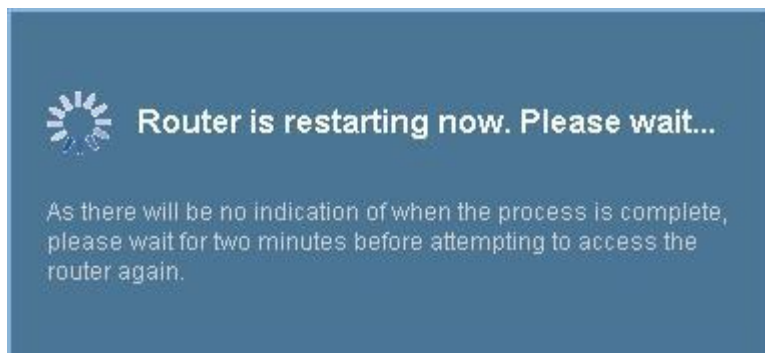


Figure 26-4 Reset In Progress Message



- You can also press the **RESET** button on the back panel to reset the factory defaults of your LTE Device. Refer to Section 1.7 on page 6 for more information on the **RESET** button.

27 The Reboot Screen

System restart allows you to reboot the LTE Device remotely without turning the power off. You may need to do this if the LTE Device hangs, for example.

Step 1 Click **Maintenance> Reboot**. Click the **Reboot** button to have the LTE Device reboot. This does not affect the LTE Device's configuration.

Figure 27-1 Reboot

System Reboot

Reboot

----End

28 Diagnostic

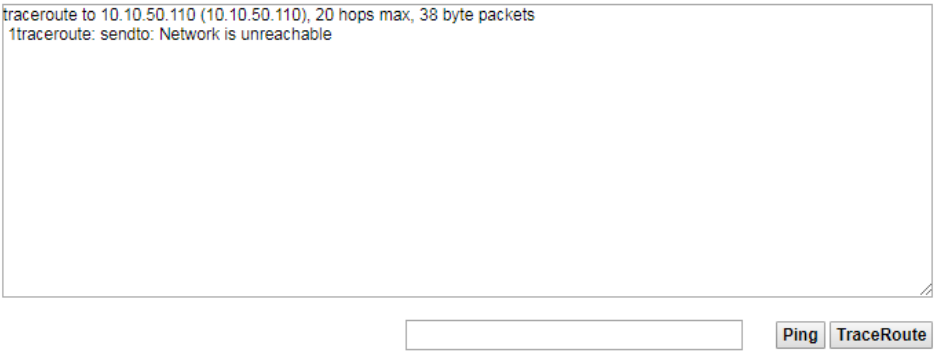
28.1 Overview

You can use different diagnostic methods to test a connection and see the detailed information. These read-only screens display information to help you identify problems with the LTE Device.

28.2 The Ping/TraceRoute Screen

Ping and traceroute help check availability of remote hosts and also help troubleshoot network or Internet connections. Click **Maintenance > Diagnostic** to open the **Ping/TraceRoute** screen shown next.

Figure 28-1 Maintenance > Diagnostic > Ping/TraceRoute



The following table describes the fields in this screen.

Table 28-1 Maintenance > Diagnostic > Ping/TraceRoute

Label	Description
Ping	Type the IP address of a computer that you want to ping in order to test a connection. Click Ping and the ping statistics will show in the diagnostic.
TraceRoute	Click this button to perform the traceroute function. This determines the path a packet takes to the specified host.

29 Troubleshooting

29.1 Overview

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- LTE Device Access and Login
- Internet Access
- Wireless Internet Access
- Phone Calls and VoIP
- UPnP

29.2 Power, Hardware Connections, and LEDs

29.3 LTE Device Access and Login

I forgot the IP address for the LTE Device.

Step 1 The default IP address is 192.168.1.1.

Step 2 If you changed the IP address and have forgotten it, you might get the IP address of the LTE Device by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the LTE Device (it depends on the network), so enter this IP address in your Internet browser.

Step 3 If this does not work, you have to reset the device to its factory defaults, see [1.5.3 The RESET Button](#).

----End

I forgot the password.

- If you can't remember the password, you have to reset the device to its factory defaults. See [1.5.3 The RESET Button](#).

I cannot see or access the *Login* screen in the web configurator.

Step 1 Make sure you are using the correct IP address.

The default IP address is 192.168.1.1.

If you changed the IP address, use the new IP address.

If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the LTE Device.

Step 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the *Quick Start Guide*.

Step 3 Check to make sure your computer does not have a static IP address.

Step 4 Check to make sure your web browser is not using proxy.

Step 5 Make sure your Internet browser does not block popup windows and has JavaScript and Java enabled.

Step 6 Reset the device to its factory defaults, and try to access the LTE Device with the default IP address. See [1.5.3 The RESET Button](#).

Step 7 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the LTE Device using another service, such as Telnet. If you can access the LTE Device, check the remote management settings and firewall rules to find out why the LTE Device does not respond to HTTP.
- If your computer is connected to the **WAN** port or is connected wirelessly, use a computer that is connected to an **ETHERNET** port.

----End

I can see the *Login* screen, but I cannot log in to the LTE Device.

Step 1 Make sure you have entered the user name and password correctly. The default user name is **user**. These fields are case-sensitive, so make sure [Caps Lock] is not on.

Step 2 You cannot log in to the web configurator while someone is using Telnet to access the LTE Device. Log out of the LTE Device in the other session, or ask the person who is logged in to log out.

Step 3 Turn the LTE Device off and on.

Step 4 If this does not work, you have to reset the device to its factory defaults. See [26.2 The Backup/Restore Screen](#).

----End

29.4 Internet Access

I cannot access the Internet.

- Step 1** Check the hardware connections, and make sure the LEDs are behaving as expected. See the *Quick Start Guide* and [1.5 Hardware](#).
- Step 2** Make sure you entered your service provider's LTE APN information correctly.
- Step 3** If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.
- Step 4** If you are trying to access the Internet wirelessly, make sure you have enabled the wireless LAN by the WPS/WLAN button or the Network Setting > Wireless > General screen.
- Step 5** Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
- Step 6** If the problem continues, contact your ISP.

----End

I cannot access the Internet anymore. I had access to the Internet (with the LTE Device), but my Internet connection is not available anymore.

- Step 1** Check the hardware connections, and make sure the LEDs are behaving as expected. See the *Quick Start Guide* and [1.5 Hardware](#).
- Step 2** Turn the LTE Device off and on.
- Step 3** If the problem continues, contact your ISP.

----End

The Internet connection is slow or intermittent.

- Step 1** There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.6. If the LTE Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
- Step 2** Turn the LTE Device off and on.
- Step 3** If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

Check the settings for QoS. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.

----End

29.5 Wireless Internet Access

What factors may cause intermittent or unstable wireless connection? How can I solve this problem?

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.
- Building Materials: metal doors, aluminum studs.
- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other wireless devices.

To optimize the speed and quality of your wireless connection, you can:

- Move your wireless device closer to the AP if the signal strength is low.
- Reduce wireless interference that may be caused by other wireless networks or surrounding wireless electronics such as cordless phones.
- Place the AP where there are minimum obstacles (such as walls and ceilings) between the AP and the wireless client.
- Reduce the number of wireless clients connecting to the same AP simultaneously, or add additional APs if necessary.
- Try closing some programs that use the Internet, especially peer-to-peer applications. If the wireless client is sending or receiving a lot of information, it may have too many programs open that use the Internet.

What wireless security modes does my LTE Device support?

Wireless security is vital to your network. It protects communications between wireless stations, access points and the wired network.

The available security modes in your device are as follows:

- **WPA2-PSK:** (recommended) this uses a pre-shared key with the WPA2 standard.
- **WPA-PSK:** This has the device use either WPA-PSK or WPA2-PSK depending on which security mode the wireless client uses.

29.6 Phone Calls and VoIP

The telephone port won't work or the telephone lacks a dial tone.

Step 1 Check the telephone connection and telephone wire.

----End

I can access the Internet, but cannot make VoIP calls.

Step 1 The **PHONE** light should come on. Make sure that your telephone is connected to the PHONE port.

Step 2 You can also check the VoIP status in the **System Info** screen.

Step 3 If the VoIP settings are correct, use speed dial to make peer-to-peer calls. If you can make a call using speed dial, there may be something wrong with the SIP server, contact your VoIP service provider.

----End

29.7 UPnP

When using UPnP and the LTE Device reboots, my computer cannot detect UPnP and refresh

My Network Places > Local Network.

Step 1 Disconnect the Ethernet cable from the LTE Device's LAN port or from your computer.

Step 2 Re-connect the Ethernet cable.

----End

The *Local Area Connection* icon for UPnP disappears in the screen. Restart your computer.

I cannot open special applications such as white board, file transfer and video when I use the MSN messenger.

Step 1 Wait more than three minutes.

Step 2 Restart the applications.

----End

30 Personal Data Description

LTE CPE B2368 Personal Data Description provides descriptions to the personal data collected by CPE. You must handle the personal data on the CPE according to the laws and regulations of your country, for example, GDPR(General Data Protection Regulation) of European Union.