

# User's Guide

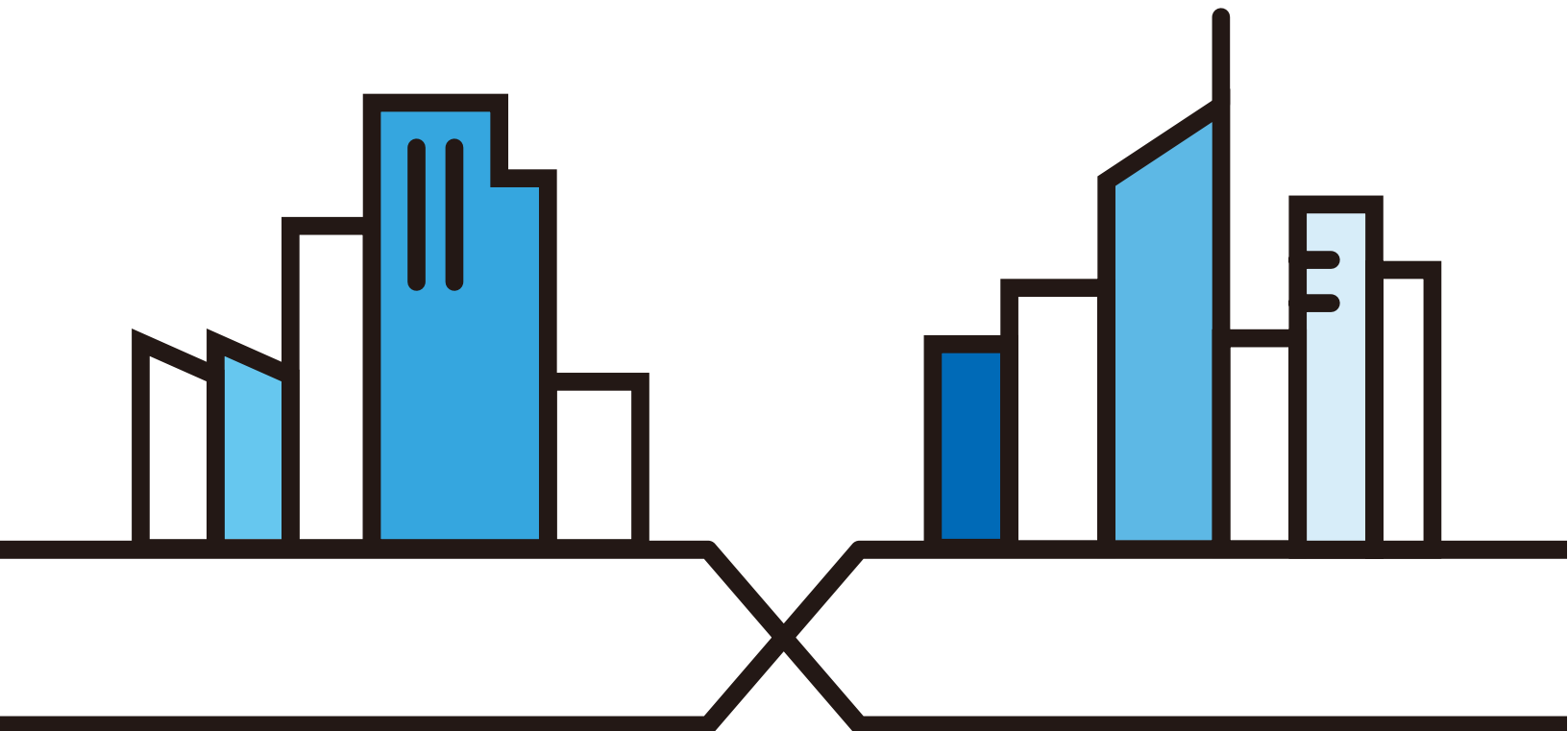
## LTE3316-M604

4G LTE-A Indoor IAD

### Default Login Details

LAN IP Address	http://192.168.1.1
User Name	admin
Password	1234

Version 1.00 Edition 3, 06/2020



---

**IMPORTANT!**

**READ CAREFULLY BEFORE USE.**

**KEEP THIS GUIDE FOR FUTURE REFERENCE.**

Screenshots and graphics in this book may differ slightly from what you see due to differences in release versions or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

### **Related Documentation**

- Quick Start Guide

The Quick Start Guide shows how to connect the managed device.

- More Information

Go to [support.zyxel.com](http://support.zyxel.com) to find other information on the LTE3316-M604.



# Document Conventions

## Warnings and Notes

These are how warnings and notes are shown in this guide.

**Warnings tell you about things that could harm you or your device.**








Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

## Syntax Conventions

- The LTE3316-M604 in this user's guide may be referred to as the "LTE" in this guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A right angle bracket ( > ) within a screen name denotes a mouse click. For example, **Configuration > Network > WAN > Management WAN** means you first click **Configuration** in the navigation panel, then **Network**, then the **WAN** sub menu and finally the **Management WAN** tab to get to that screen.

## Icons Used in Figures

Figures in this user guide may use the following generic icons. The LTE icon is not an exact representation of your device.

LTE 	Generic Router 	Switch 
Server 	Firewall 	Printer 
Antenna Tower 		

# Contents Overview

<b>User's Guide .....</b>	<b>12</b>
Introduction .....	13
Web Configurator .....	20
Setup Wizard .....	27
Tutorials .....	32
<b>Technical Reference .....</b>	<b>39</b>
Status .....	40
Monitor .....	43
WAN .....	51
Wireless LAN .....	64
LAN .....	86
DHCP Server .....	88
NAT .....	93
DDNS .....	102
Routing .....	104
Interface Group .....	107
Firewall .....	109
Content Filtering .....	114
IPv6 Firewall .....	117
VPN .....	119
SMS .....	129
Voice Call .....	132
MGMT Interface .....	135
Bandwidth Management .....	138
Universal Plug-and-Play (UPnP) .....	143
TR-069 .....	158
Maintenance .....	160
Troubleshooting .....	168

---

# Table of Contents

<b>Document Conventions</b> .....	<b>3</b>
<b>Contents Overview</b> .....	<b>4</b>
<b>Table of Contents</b> .....	<b>5</b>
<b>Part I: User's Guide</b> .....	<b>12</b>
<b>Chapter 1</b>	
<b>Introduction</b> .....	<b>13</b>
1.1 Overview .....	13
1.2 Applications .....	13
1.2.1 Wireless WAN (3G/4G/LTE) Connection .....	14
1.2.2 WAN Priority .....	14
1.2.3 Wireless LAN (WiFi) Connection .....	14
1.3 Ways to Manage the LTE .....	14
1.4 Good Habits for Managing the LTE .....	14
1.5 Hardware Connections .....	15
1.5.1 LEDs .....	15
1.5.2 Rear Panel .....	16
1.6 Wall Mounting .....	18
<b>Chapter 2</b>	
<b>Web Configurator</b> .....	<b>20</b>
2.1 Overview .....	20
2.2 Login Accounts .....	20
2.3 Accessing the Web Configurator .....	20
2.4 Navigating the Web Configurator .....	22
2.4.1 Title Bar .....	23
2.4.2 Navigation Panel .....	23
2.4.3 Dashboard .....	24
<b>Chapter 3</b>	
<b>Setup Wizard</b> .....	<b>27</b>
3.1 Overview .....	27
3.2 Accessing the Wizard .....	27
3.3 Wizard Setup .....	28

<b>Chapter 4</b>	
<b>Tutorials</b> .....	<b>32</b>
4.1 Overview .....	32
4.2 Connecting to the LTE Using WPS .....	32
4.2.1 Push Button Configuration (PBC) .....	32
4.2.2 PIN Configuration .....	33
4.3 Connect to LTE Wireless Network Without WPS .....	34
4.4 Using Multiple SSIDs on the LTE .....	36
4.4.1 Configuring Security Settings of Multiple SSIDs .....	36
<b>Part II: Technical Reference</b> .....	<b>39</b>
<b>Chapter 5</b>	
<b>Status</b> .....	<b>40</b>
5.1 Overview .....	40
5.2 Status .....	40
<b>Chapter 6</b>	
<b>Monitor</b> .....	<b>43</b>
6.1 Overview .....	43
6.2 What You Can Do .....	43
6.3 Log .....	43
6.3.1 View Log .....	43
6.4 DHCP Table .....	45
6.5 ARP Table .....	45
6.6 Packet Statistics .....	46
6.7 WLAN Station Status .....	47
6.8 LTE Modem Status .....	48
<b>Chapter 7</b>	
<b>WAN</b> .....	<b>51</b>
7.1 Overview .....	51
7.2 What You Can Do .....	51
7.3 What You Need To Know .....	52
7.4 WAN Management .....	54
7.4.1 WAN Management Edit 3G/4G .....	54
7.4.2 WAN Management Edit Ethernet .....	57
7.5 Network Scan .....	60
7.6 IPv6 .....	61
7.7 PIN Management .....	63

<b>Chapter 8</b>	
<b>Wireless LAN</b>	<b>64</b>
8.1 Overview	64
8.1.1 What You Can Do	64
8.1.2 What You Should Know	65
8.2 General Wireless LAN Settings	67
8.3 Wireless Security	70
8.3.1 No Security	70
8.3.2 WPA2-PSK	71
8.3.3 WPA/WPA2	73
8.4 More AP	75
8.4.1 More AP Edit	76
8.5 MAC Filter	77
8.6 Wireless LAN Advanced Settings	79
8.7 Quality of Service (QoS)	80
8.8 WPS	81
8.9 WPS Station	82
8.10 Scheduling	83
8.11 WDS	84
<b>Chapter 9</b>	
<b>LAN</b>	<b>86</b>
9.1 Overview	86
9.2 What You Can Do	86
9.3 What You Need To Know	86
9.4 LAN IP	87
<b>Chapter 10</b>	
<b>DHCP Server</b>	<b>88</b>
10.1 Overview	88
10.1.1 What You Can Do	88
10.1.2 What You Need To Know	88
10.2 DHCP Server General Settings	88
10.3 Advanced DHCP Server Setting	90
10.4 DHCP Client List	92
<b>Chapter 11</b>	
<b>NAT</b>	<b>93</b>
11.1 Overview	93
11.1.1 What You Can Do	93
11.2 General Settings	94
11.3 Port Forwarding	94
11.3.1 Edit Port Forwarding	96

---

11.4 Port Trigger .....	98
11.5 ALG .....	99
11.6 Technical Reference .....	99
11.6.1 NAT Port Forwarding: Services and Port Numbers .....	99
11.6.2 NAT Port Forwarding Example .....	100
11.6.3 Trigger Port Forwarding .....	100
11.6.4 Trigger Port Forwarding Example .....	101
11.6.5 Two Points To Remember About Trigger Ports .....	101
<b>Chapter 12</b>	
<b>DDNS .....</b>	<b>102</b>
12.1 Overview .....	102
12.2 General Settings .....	102
<b>Chapter 13</b>	
<b>Routing .....</b>	<b>104</b>
13.1 Overview .....	104
13.2 Static Route .....	104
13.2.1 Add/Edit Static Route .....	105
13.3 Dynamic Routing .....	106
<b>Chapter 14</b>	
<b>Interface Group .....</b>	<b>107</b>
14.1 Overview .....	107
14.2 Interface Group .....	107
14.2.1 Add Interface Group .....	108
<b>Chapter 15</b>	
<b>Firewall .....</b>	<b>109</b>
15.1 Overview .....	109
15.1.1 What You Can Do .....	109
15.1.2 What You Need To Know .....	109
15.2 General Settings .....	110
15.3 Firewall Services .....	111
<b>Chapter 16</b>	
<b>Content Filtering .....</b>	<b>114</b>
16.1 Overview .....	114
16.2 Content Filter .....	114
<b>Chapter 17</b>	
<b>IPv6 Firewall .....</b>	<b>117</b>
17.1 Overview .....	117



17.2 IPv6 Firewall .....	117
<b>Chapter 18</b>	
<b>VPN.....</b>	<b>119</b>
18.1 Overview .....	119
18.1.1 What You Can Do in this Chapter .....	119
18.2 What You Need to Know .....	119
18.3 L2TP Server .....	120
18.4 L2TP Client .....	121
18.4.1 Add L2TP Client .....	122
18.5 GRE .....	124
18.5.1 Add GRE .....	126
18.6 VPN Passthrough .....	127
<b>Chapter 19</b>	
<b>SMS.....</b>	<b>129</b>
19.1 Overview .....	129
19.1.1 What You Can Do in this Chapter .....	129
19.2 SMS Configuration .....	129
<b>Chapter 20</b>	
<b>Voice Call.....</b>	<b>132</b>
20.1 Overview .....	132
20.1.1 What You Can Do in this Chapter .....	132
20.2 General Settings .....	132
20.3 Call Configuration .....	133
<b>Chapter 21</b>	
<b>MGMT Interface .....</b>	<b>135</b>
21.1 Overview .....	135
21.2 What You Can Do .....	135
21.3 What You Need To Know .....	135
21.3.1 System Timeout .....	135
21.4 Local MGMT .....	135
21.5 Remote MGMT .....	137
<b>Chapter 22</b>	
<b>Bandwidth Management .....</b>	<b>138</b>
22.1 Overview .....	138
22.2 What You Can Do .....	138
22.3 What You Need To Know .....	139
22.4 General Settings .....	139
22.4.1 Add Bandwidth Management Rule .....	140

---

<b>Chapter 23</b>	
<b>Universal Plug-and-Play (UPnP)</b> .....	<b>143</b>
23.1 Overview .....	143
23.2 What You Need to Know .....	143
23.2.1 NAT Traversal .....	143
23.2.2 Cautions With UPnP .....	143
23.3 UPnP Settings .....	144
23.4 Turn on UPnP in Windows 7 Example .....	144
23.4.1 Auto-discover Your UPnP-enabled Network Device .....	146
23.5 Turn on UPnP in Windows 10 Example .....	148
23.5.1 Auto-discover Your UPnP-enabled Network Device .....	150
23.6 Web Configurator Easy Access in Windows 7 .....	153
23.7 Web Configurator Easy Access in Windows 10 .....	155
<b>Chapter 24</b>	
<b>TR-069</b> .....	<b>158</b>
24.1 Overview .....	158
24.2 TR-069 Settings .....	158
<b>Chapter 25</b>	
<b>Maintenance</b> .....	<b>160</b>
25.1 Overview .....	160
25.1.1 What You Can Do in this Chapter .....	160
25.2 General Settings .....	160
25.3 User Account .....	161
25.3.1 Modify a User Account .....	162
25.4 Time Settings .....	162
25.5 Firmware Upgrade .....	164
25.6 Module Upgrade .....	165
25.7 Configuration Backup/Restore .....	166
25.8 System Reboot .....	167
<b>Chapter 26</b>	
<b>Troubleshooting</b> .....	<b>168</b>
26.1 Overview .....	168
26.2 Power, and Hardware Installation .....	168
26.3 LTE Access and Login .....	168
26.4 Internet Access .....	169
26.5 Wireless Connections .....	170
26.6 Getting More Troubleshooting Help .....	171
Appendix A Customer Support .....	172

Appendix B Common Services ..... 178

Appendix C Legal Information ..... 181

**Index .....188**

---

# PART I

## User's Guide

---

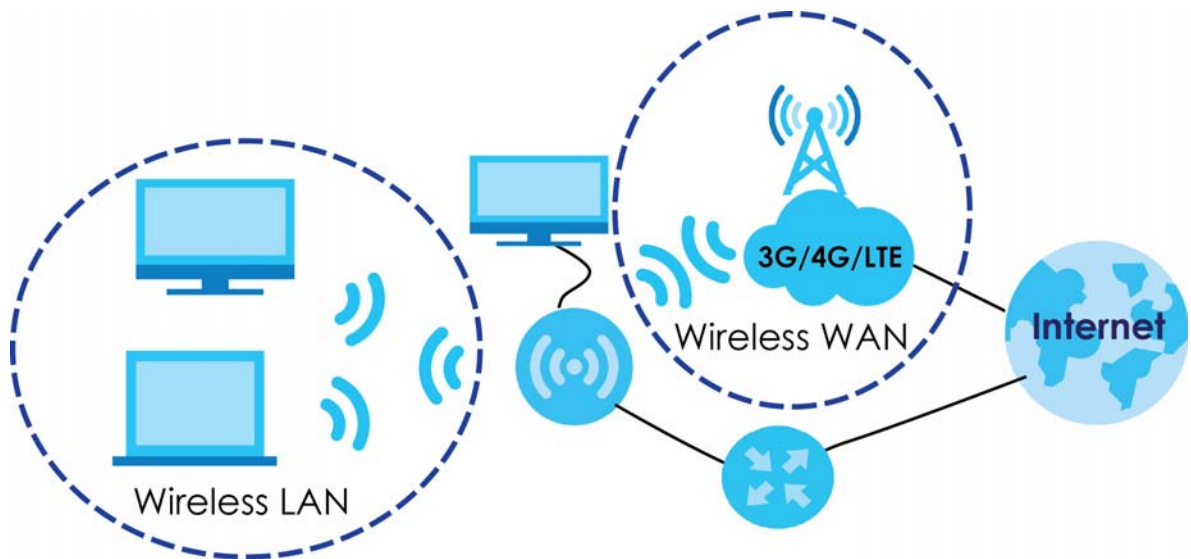
# CHAPTER 1

## Introduction

### 1.1 Overview

This chapter introduces the main features and applications of the LTE.

The LTE is a wireless router, which can connect to a mobile network and the Internet through a wireless WAN connection and provide easy network access to users without additional wiring. You can set up a 2.4G of IEEE 802.11b/g/n and 5G of 201.11a/n/ac wireless network.



A range of services such as a firewall are also available for secure Internet computing.

Your LTE is easy to install, configure and use. The embedded Web-based configurator enables simple, straightforward management and maintenance. See the Quick Start Guide for how to make hardware connections.

The LTE has two internal antennas for WAN connection. Additionally, you can install two external antennas to improve your wireless WAN signal strength. Note that external antennas are not provided. They are the default antennas for signal transmission when the LTE is starting up.

### 1.2 Applications

You can have the following networks with the LTE:

- **Wired LAN.** You can connect network devices via the Ethernet ports of the LTE so that they can communicate with each other and access the Internet.

- **Wireless LAN.** Wireless clients can wirelessly connect to the LTE to access network resources. You can use WPS (WiFi Protected Setup) to create an instant network connection with another WPS compatible device.

## 1.2.1 Wireless WAN (3G/4G/LTE) Connection

The LTE comes with a built-in 3G/4G module for 3G/4G connections. To set up a 3G/4G connection using the built-in 3G/4G module, just insert a 3G/4G SIM card into the SIM card slot at the back of the LTE.

Note: You must insert the 3G/4G SIM card into the card slot before turning on the LTE.

## 1.2.2 WAN Priority

The WAN connection priority is as follows:

- 3G/4G/Ethernet WAN

If you have a 3G/4G connection and Ethernet WAN connection at the same time, go to the **Status** screen to see which connection is up. Please see [Section 7.4 on page 54](#) for more information about WAN management.

## 1.2.3 Wireless LAN (WiFi) Connection

The LTE is a wireless Access Point (AP) for wireless clients, such as notebook computers or tablets and iPads. It allows them to connect to the Internet without having to rely on inconvenient Ethernet cables. By default, the wireless LAN (WLAN) is enabled on the LTE.

# 1.3 Ways to Manage the LTE

Use any of the following methods to manage the LTE.

- **Web Configurator.** This is recommended for everyday management of the LTE using a (supported) web browser.
- **WPS (WiFi Protected Setup).** You can use the WPS section of the Web Configurator to set up a wireless network with your LTE Device.
- **TR-069.** This is an auto-configuration server used to remotely configure your device.

# 1.4 Good Habits for Managing the LTE

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

- Change the password often. 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, you will have to reset the LTE to its factory default settings. If you backed up an earlier configuration file, you won't have to totally re-configure the LTE; you can simply restore your last configuration.

## 1.5 Hardware Connections

See your Quick Start Guide for information on making hardware connections. You need to insert a SIM card to the SIM card slot at the side of the LTE before you can use it.

### 1.5.1 LEDs

The following graphics display the front panel of the LTE. You can check the LED lights to see the 3G/4G/LTE connection status, signal strength, and the wireless connection status.

Figure 1 LTE Front Panel

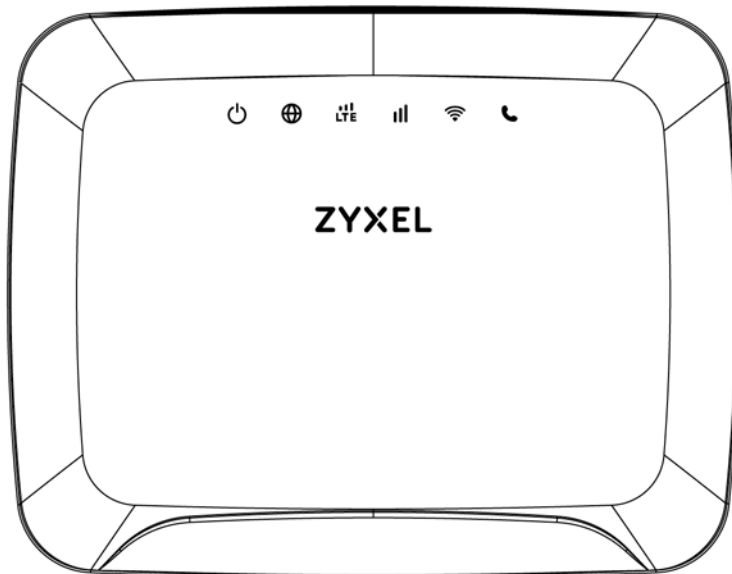
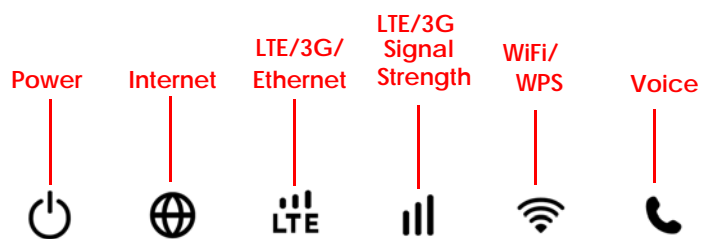








Figure 2 LEDs



The following table describes the LED lights.

Table 1 Front Panel LEDs

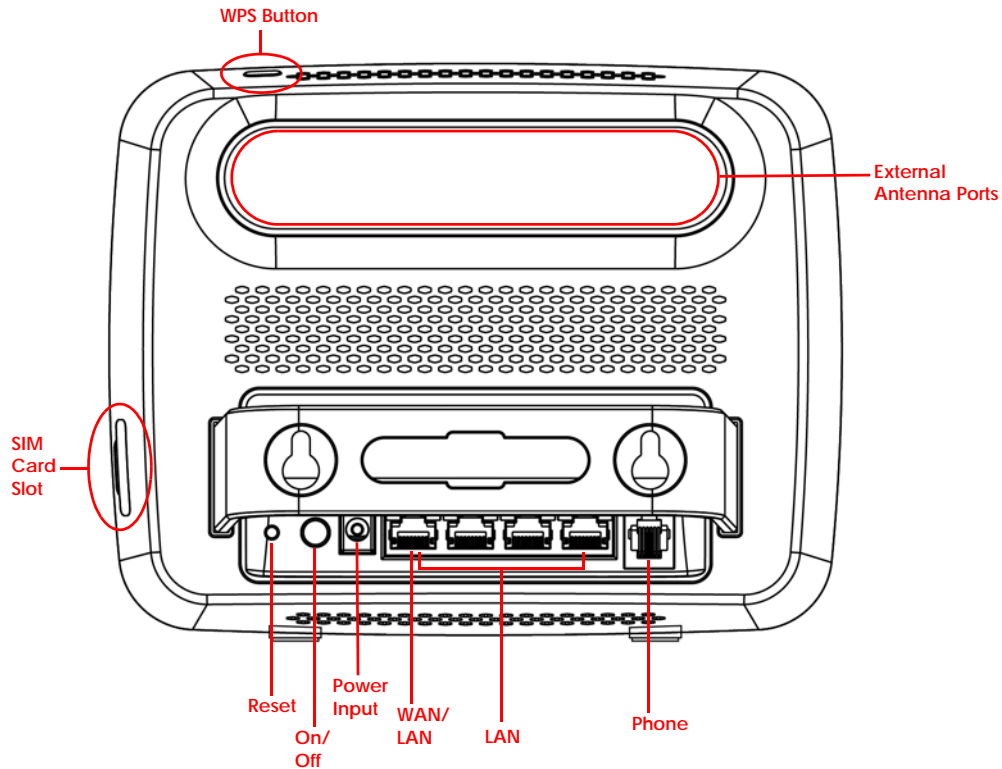
LED	COLOR	STATUS	DESCRIPTION	
Power 	White	On	The LTE is receiving power and functioning properly.	
		Blinking	The LTE is in the process of starting up or default restoring.	
		Off	The LTE is not receiving power.	
Internet 	White	On	The LTE's WAN connection is ready, but there is no traffic.	
		Blinking	The LTE is transmitting and receiving data through the WAN.	
		Off	The WAN connection is not ready, or has failed.	
LTE/3G/ Ethernet 	White	On	The LTE is successfully connected to a 4G or LTE network.	
		Blinking (slow)	The LTE is successfully connected to a 3G network.	
	Green	On	The LTE is successfully connected to an Ethernet WAN network.	
LTE/3G Signal Strength 	Green	On	A valid SIM card is inserted and the wireless WAN interface is enabled, this indicates the signal strength is good.	
		Amber	On	A valid SIM card is inserted and the wireless WAN interface is enabled, this indicates the signal strength is fair.
		Red	On	A valid SIM card is inserted and the wireless WAN interface is enabled, this indicates the signal strength is poor.
		Blinking	A valid SIM card is inserted, but no signal is detected.	
WiFi/WPS 	White	On	The LTE is ready and the 5G wireless LAN is on, but is not sending/receiving data through the wireless LAN.	
		Blinking (fast)	The LTE is sending/receiving data through the 5G wireless LAN.	
		Blinking (slow)	The LTE is connecting to a 5G WiFi-Connection via WPS.	
	Green	On	The LTE is ready and the 2.4G wireless LAN is on, but is not sending/receiving data through the wireless LAN.	
		Blinking (fast)	The LTE is sending/receiving data through the 2.4G wireless LAN.	
		Blinking (slow)	The LTE is connecting to a 2.4G WiFi-Connection via WPS.	
Voice 	White	On	A telephone connected to the <b>PHONE</b> port has its receiver on the hook.	
		Blinking	The LTE is receiving an incoming call.	
		Off	A telephone connected to the <b>PHONE</b> port has its receiver off the hook.	

## 1.5.2 Rear Panel

To turn on the device, press the power button.



Figure 3 LTE Power Button



### 1.5.2.1 SIM Card Slot

The LTE comes with a built-in 3G/4G/LTE module for mobile connections. To set up a mobile connection using the built-in 3G/4G/LTE module, just insert a SIM card into the SIM card slot at the back of the LTE.

Note: You must insert the SIM card into the card slot before turning on the LTE.

### 1.5.2.2 The WPS Button

Your LTE 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.

You can use the WPS button (  ) on the side panel of the LTE to activate WPS in order to quickly set up a wireless network with strong security.

- 1 Make sure the power LED is on (not blinking).

- 2 Press the WPS button for more than five seconds and release it. Press the WPS button on another WPS enabled device within range of the LTE.

Note: You must activate WPS in the LTE and in another wireless device within two minutes of each other.

Note: The LTE's WPS is disabled by default for security reasons. To use this feature you will need to enable WPS, for more information see [Section 4.2 on page 32](#).

### 1.5.2.3 The Reset Button

If you forget your password or IP address, or you cannot access the Web Configurator, you will need to use the physical **Reset** button to reload the factory-default configuration file. This means that you will lose all configurations that you had previously saved, the password will be reset to **1234** and the IP address will be reset to **192.168.1.1**.

#### Resetting the LTE to Factory-Default Settings

- 1 Press the **Reset** button on the rear panel for more than five seconds to set the LTE back to its factory default configurations.
- 2 Wait until the Power LED turns on steady white. This means the LTE is ready for use.

#### Restarting or Rebooting the LTE

- 1 Press the **Reset button** on the rear panel for two seconds to restart/reboot the LTE.
- 2 Wait until the Power LED turns on steady white. This means the LTE is ready for use.

## 1.6 Wall Mounting

You may need screw anchors if mounting on a concrete or brick wall.

Table 2 Wall Mounting Information

Distance between holes	100 mm
M4 Screws	Two
Screw anchors (optional)	Two

- 1 Select a position free of obstructions on a wall strong enough to hold the weight of the device.
- 2 Mark two holes on the wall at the appropriate distance apart for the screws.

**Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.**

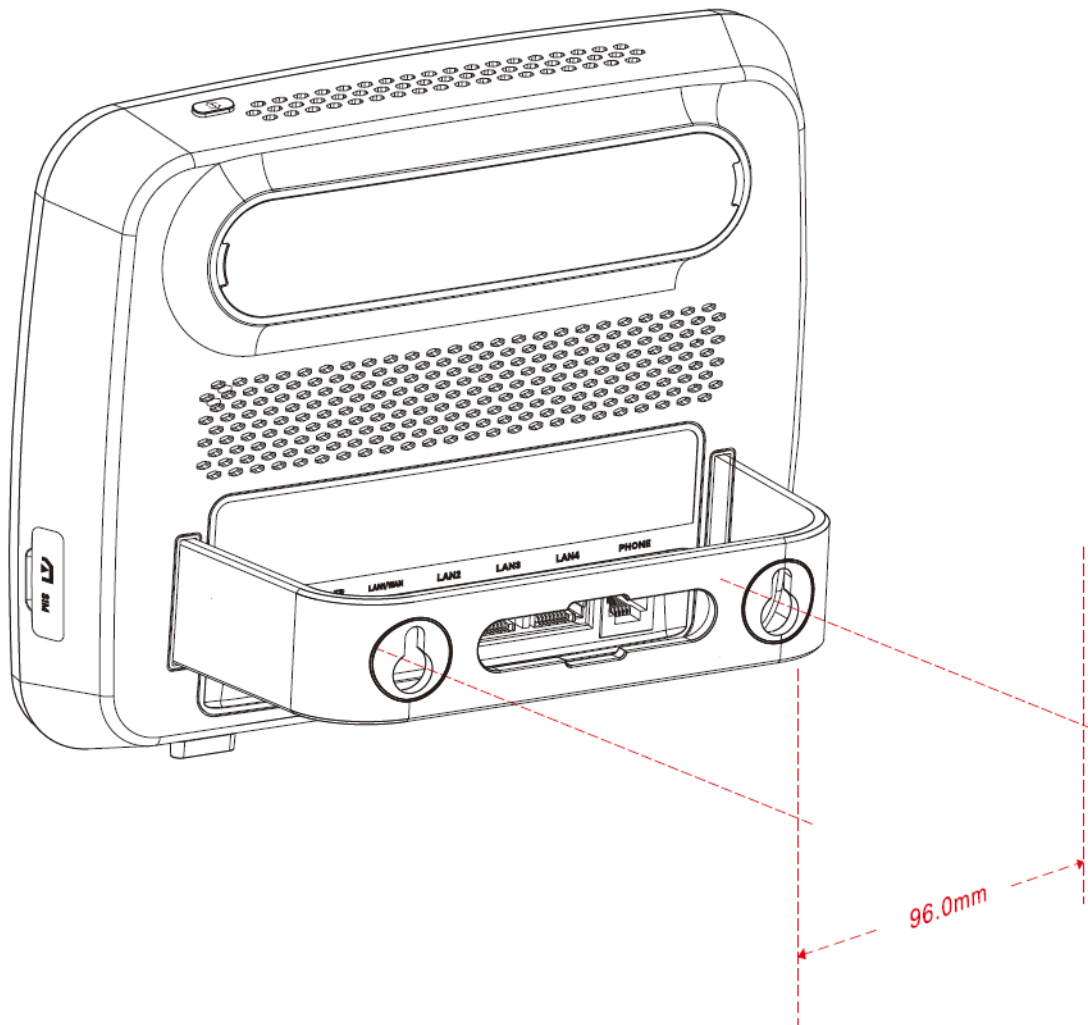
**Do not wall mount the LTE over a height of 2 m.**

- 3 If using screw anchors, drill two holes for the screw anchors into the wall. Push the anchors into the full depth of the holes, then insert the screws into the anchors. Do not insert the screws all the way in - leave a small gap of about 0.5 cm.

If not using screw anchors, use a screwdriver to insert the screws into the wall. Do not insert the screws all the way in - leave a gap of about 0.5 cm.

- 4 Make sure the screws are fastened well enough to hold the weight of the LTE with the connection cables.
- 5 Align the holes on the back of the LTE with the screws on the wall. Hang the LTE on the screws.

**Figure 4** Wall Mounting Example



# CHAPTER 2

# Web Configurator

## 2.1 Overview

This chapter describes how to access the LTE Web Configurator and provides an overview of its screens.

The Web Configurator is an HTML-based management interface that allows easy system setup and management via Internet browser. Use a browser that supports HTML5, such Internet Explorer 11, Mozilla Firefox, or Google Chrome. The recommended screen resolution is 1024 by 768 pixels.

In order to use the Web Configurator, you must:

- Web browser pop-up windows from your device.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

Refer to the Troubleshooting chapter ([Chapter 26 on page 168](#)) to see how to make sure these functions are allowed in Internet Explorer.

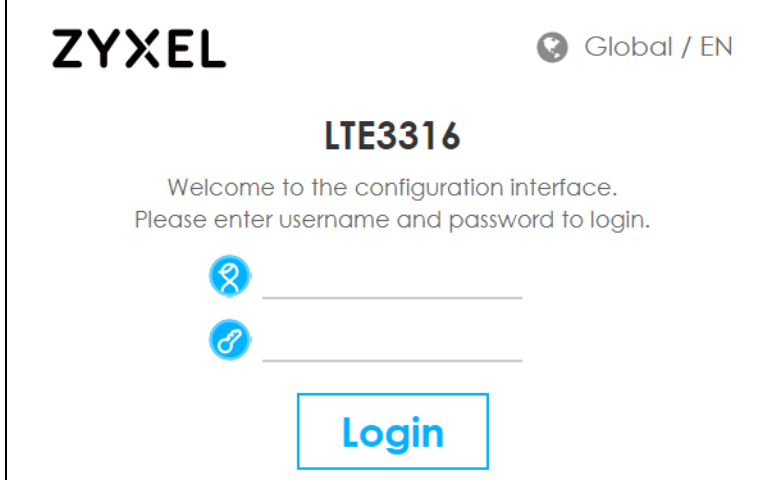
## 2.2 Login Accounts

There is one system account that you can use to log in to the LTE: "**admin**". The **admin** account allows you full access to all system configurations. The default admin user name is "admin" and password is "1234".

## 2.3 Accessing the Web Configurator

- 1 Make sure your LTE hardware is properly connected and prepare your computer or computer network to connect to the LTE (refer to the Quick Start Guide).
- 2 Launch your web browser.

- 3 Enter "http://192.168.1.1" as the website address. The **Login** screen appears.  
Your computer must be in the same subnet in order to access this website address.



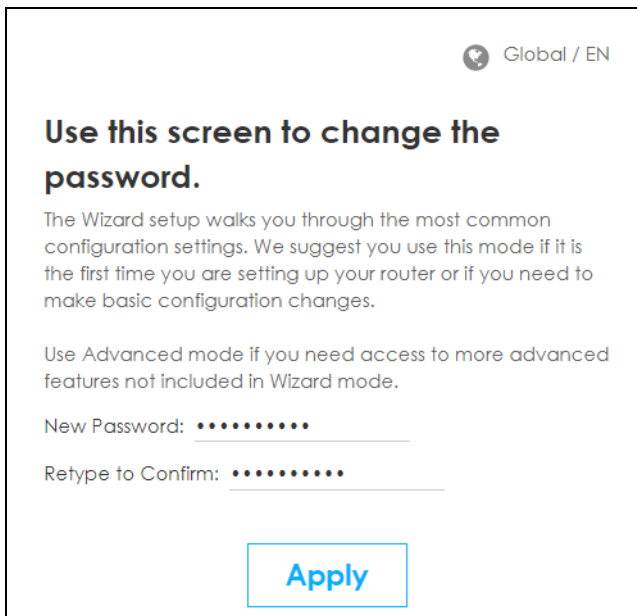
**ZYXEL** Global / EN

**LTE3316**

Welcome to the configuration interface.  
Please enter username and password to login.

**Login**

- 4 Enter the **User Name** (default: "admin") and **Password** (default: "1234"). See [Section 2.2 on page 20](#) for more information about login accounts. Click **Login**.
- 5 The following screen displays if you have not yet changed your password. Enter a new password, retype it to confirm and click **OK**.



Global / EN

**Use this screen to change the password.**

The Wizard setup walks you through the most common configuration settings. We suggest you use this mode if it is the first time you are setting up your router or if you need to make basic configuration changes.

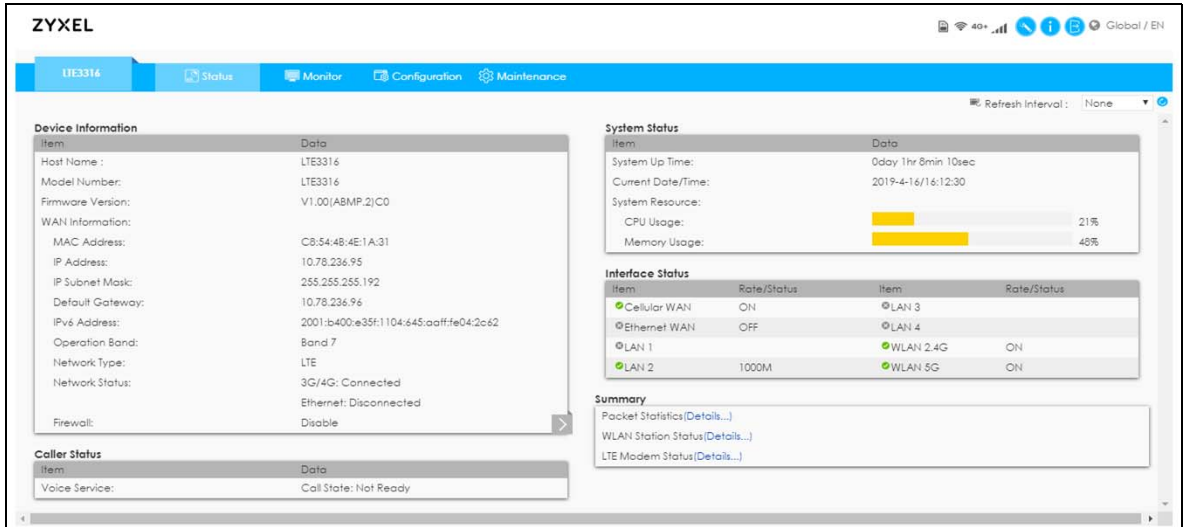
Use Advanced mode if you need access to more advanced features not included in Wizard mode.

New Password:

Retype to Confirm:

**Apply**

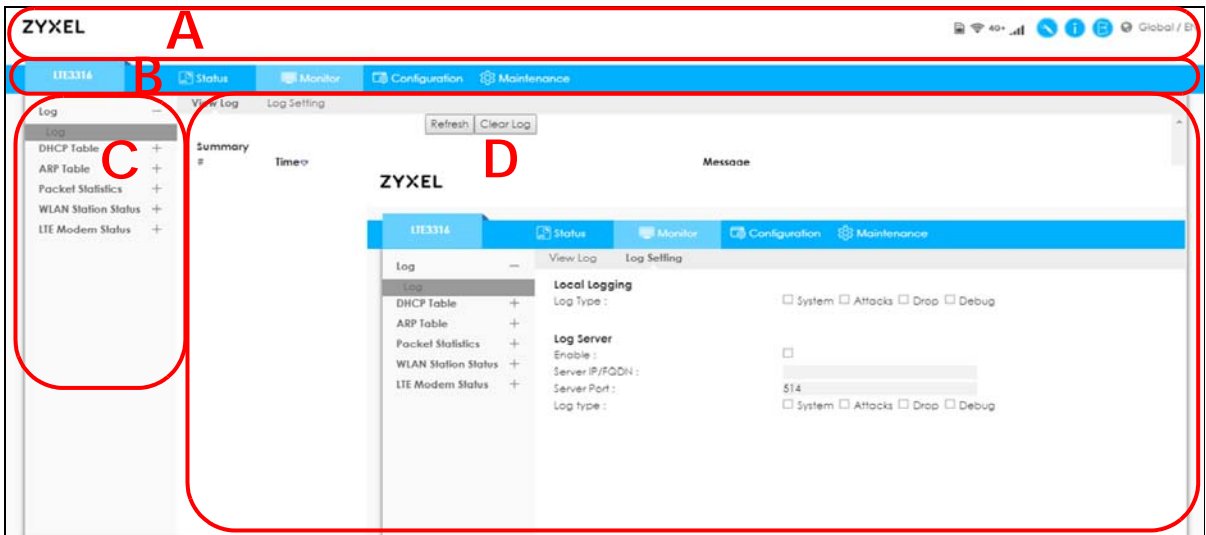
- 6 The **Home** screen appears.



## 2.4 Navigating the Web Configurator

The following summarizes how to navigate the Web Configurator from the **Home** screen.

**Figure 5** The Web Configurator's Main Screen



The Web Configurator's main screen is divided into these parts:

- **A** - Title Bar
- **B** - Navigation Panel: Main Menus
- **C** - Navigation Panel: Sub-Menus
- **D** - Main Window

## 2.4.1 Title Bar











The title bar provides some useful links that always appear over the screens below, regardless of how deep into the Web Configurator you navigate.

**Figure 6** Title Bar



The icons provide the following functions.

**Table 3** Title Bar: Web Configurator Icons

LABEL	DESCRIPTION
SIM 	This shows whether a SIM card is inserted in the LTE. The icon shows  if there is no SIM card inserted.
WiFi 	This shows whether the LTE's WiFi LAN network is enabled. The following icon  displays when the WiFi LAN network is disabled.
WAN Connection 	This displays the type of mobile data connection ( <b>4G+</b> , <b>4G</b> , <b>3G</b> ) the LTE has to the ISP.
Signal Strength 	This shows the current signal strength to the mobile network. The icon shows no bars if the mobile data connection is not up.
Setup Wizard 	Click this icon to open the Setup Wizard for the LTE.
Help 	Click this to open a screen where you can click a link to visit the Zyxel website to see detailed product information.
Logout 	Click this icon to log out of the Web Configurator.
Language  Global / EN	Choose your language from the drop-down list on the upper right corner of the title bar.

## 2.4.2 Navigation Panel

Use the menu items on the navigation panel to open screens to configure LTE features. The following sections introduce the LTE's navigation panel menus and their screens.

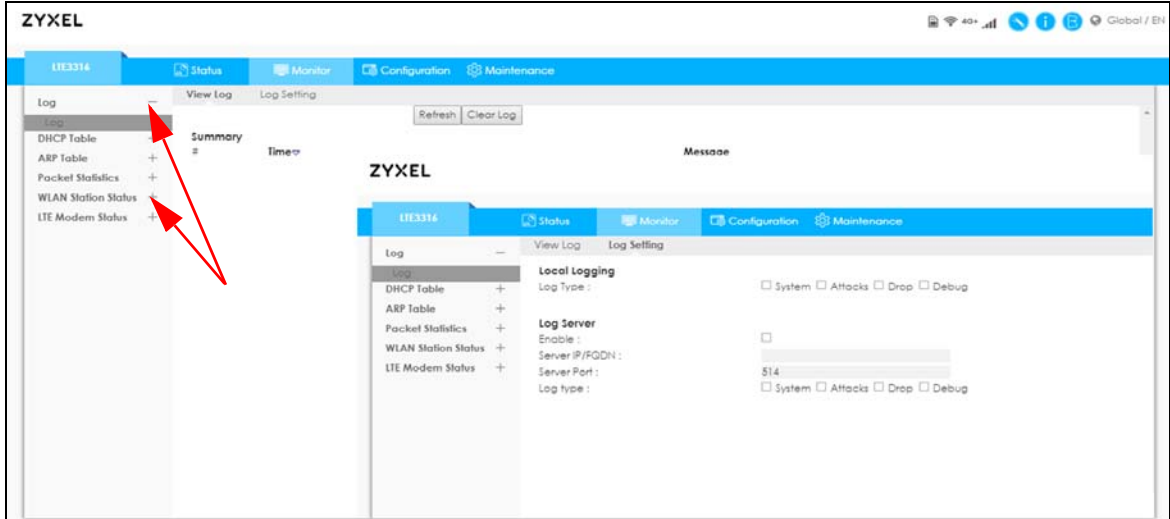
Figure 7 Navigation Panel



## 2.4.3 Dashboard

Use the menu items in the navigation panel on the right to open screens to configure the Zyxel Device's features.

Figure 8 Navigation Panel



The following table describes the navigation panel menus and sub-menus.

Table 4 Navigation Panel

MENU	SUB-MENU	DESCRIPTION
Status		This screen shows the LTE's general device, system and interface status information. Use this screen to access the summary statistics tables.
Monitor		
Log	View Log	Use this screen to see the logs for the categories that you selected in the Log Settings screen.
	Log Setting	Use this screen to configure to where and when the LTE is to send the logs and which logs and/or immediate alerts it is to send.
DHCP Table		Use this screen to view current DHCP client information.
ARP Table		Use this screen to view the ARP table. It displays the IP and MAC address of each DHCP connection
Packet Statistics		Use this screen to view port status and packet specific statistics.
WLAN Station Status		Use this screen to view the wireless stations that are currently associated to the LTE's 2.4G and 5G wireless LAN.
LTE Modem Status		Use this screen to view the detailed information about the LTE module, cellular interface, and SIM card. You can also view the LTE connection status.
Configuration		
Network		



Table 4 Navigation Panel (continued)

MENU	SUB-MENU	DESCRIPTION
WAN	WAN Management	This screen allows you to configure ISP parameters, WAN IP address assignment, and DNS servers.
	Network Scan	Use this screen to specify the type of the mobile network to which the LTE connected and how you want the LTE to connect to an available mobile network.
	IPv6	Use this screen to configure the LTE's IPv6 settings.
	PIN Management	Use this screen to enable PIN code authentication and enter the PIN code.
Wireless LAN	General	Use this screen to enable the wireless LAN and configure wireless LAN and wireless security settings.
	More AP	Use this screen to configure multiple BSSs on the LTE.
	MAC Filter	Use the MAC filter screen to allow or deny wireless stations based on their MAC addresses from connecting to the LTE.
	Advanced	This screen allows you to configure advanced wireless LAN settings.
	QoS	Use this screen to configure Wi-Fi Multimedia Quality of Service (WMM QoS). WMM QoS allows you to prioritize wireless traffic according to the delivery requirements of individual services.
	WPS	Use this screen to configure the WPS settings.
	WPS Station	Use this screen to add a wireless station using WPS.
	Scheduling	Use this screen to schedule the times the Wireless LAN is enabled.
	WDS	Use this screen to enable and configure the WDS settings.
LAN	IP	Use this screen to configure LAN IP address and subnet mask.
DHCP Server	General	Use this screen to enable the LTE's DHCP server.
	Advanced	Use this screen to assign IP addresses to specific individual computers based on their MAC addresses and to have DNS servers assigned by the DHCP server.
	Client List	Use this screen to view information related to your DHCP status.
NAT	General	Use this screen to enable NAT.
	Port Forwarding	Use this screen to configure servers behind the LTE and forward incoming service requests to the servers on your local network.
	Port Trigger	Use this screen to change your LTE's port triggering settings.
	ALG	Use this screen to enable or disable SIP (VoIP) ALG (Application Layer Gateway) in the LTE.
	DMZ	Use this screen to set the IP address of your network DMZ (if you have one) for the LTE.
Dynamic DNS	Dynamic DNS	Use this screen to set up dynamic DNS.
Routing	Static Route	Use this screen to configure IP static routes.
	Dynamic Routing	Use this screen to enable and configure RIP on the LTE.
Interface Group	Interface Group	Use this screen to create a new interface group.
Security		
Firewall	General	Use this screen to activate/deactivate the firewall.
	Services	This screen shows a summary of the firewall rules, and allows you to edit/add a firewall rule.
Content Filter	Content Filter	Use this screen to restrict web features and designate a trusted computer. You can also block certain web sites containing certain keywords in the URL.

Table 4 Navigation Panel (continued)

MENU	SUB-MENU	DESCRIPTION
IPv6 Firewall	Services	Use this screen to configure IPv6 firewall rules.
Application		
VPN	L2TP Server	Use this screen to configure the LTE L2TP server settings.
	L2TP Client	Use this screen to configure the L2TP VPN client settings.
	GRE	Use this screen to configure the GRE VPN client mode tunnel settings.
	VPN Passthrough	Use this screen to allow VPN traffic to pass through the LTE.
SMS	SMS	Use this screen to view the SIM card's SMS inbox and send short messages.
Voice Call	General	Use this screen to enable voice service in the LTE.
	Call Conf.	Use this screen to configure enable call forwarding and configure call forwarding rules in the LTE.
Management		
MGMT Interface	Local MGMT	Use this screen to specify from which zones you can access the LTE using HTTP, HTTPS, SSH or Telnet.
	Remote MGMT	Use this screen to enable specific traffic directions for network services.
Bandwidth MGMT	General	Use this screen to enable bandwidth management, set the upstream bandwidth and edit a bandwidth management rule.
UPnP	UPnP	Use this screen to enable UPnP on the LTE.
TR069	TR069	Use this screen to configure your LTE to be managed by an ACS.
Maintenance		
General	General	Use this screen to view and change administrative settings such as system and domain names.
Account	User Account	Use this screen to change the user name and password of your LTE.
Time	Time Setting	Use this screen to change your LTE's time and date.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your LTE.
Module Upgrade	Module Upgrade	Use this screen to upload firmware for the built-in LTE module.
Backup / Restore	Backup / Restore	Use this screen to backup and restore the configuration or reset the factory defaults to your LTE.
Reboot	System Reboot	This screen allows you to reboot the LTE without turning the power off.

# CHAPTER 3

## Setup Wizard

### 3.1 Overview

This chapter provides information on the Wizard setup screens in the Web Configurator.

The Web Configurator's Wizard helps you configure your device to access the Internet and change the wireless LAN settings. Refer to your ISP for your Internet account information. Leave a field blank if you don't have that information.

### 3.2 Accessing the Wizard

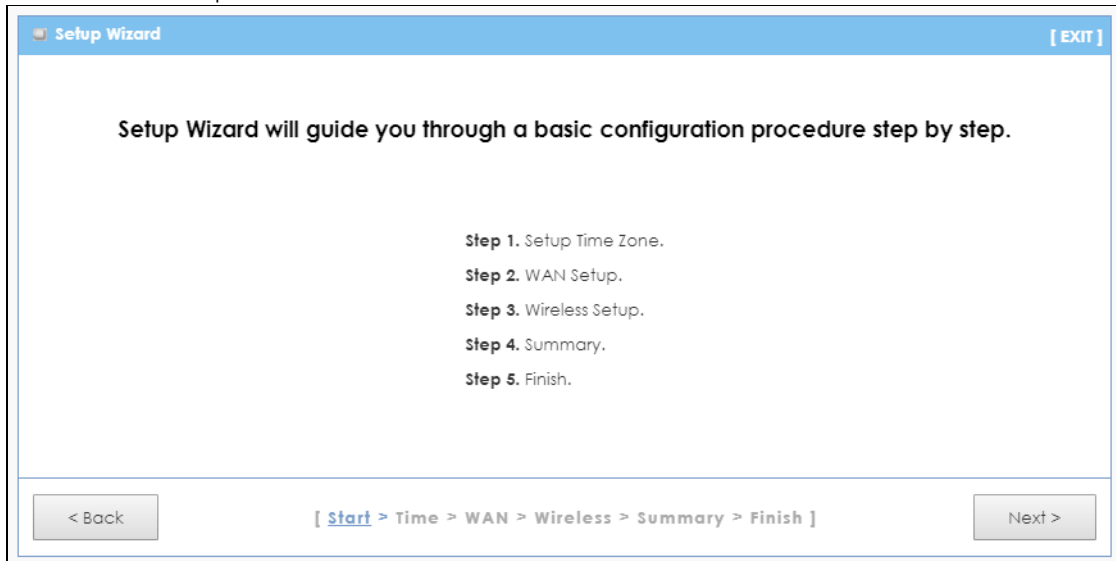
- 1 Launch your web browser and enter "http://192.168.1.1" as the website address. Type "**admin**" (default) as the user name, "**1234**" (default) as the password and click **Login**.
- 2 Click the Wizard icon in the right corner of the Web Configurator's title bar to open the Wizard screen.

**Figure 9** Wizard Icon

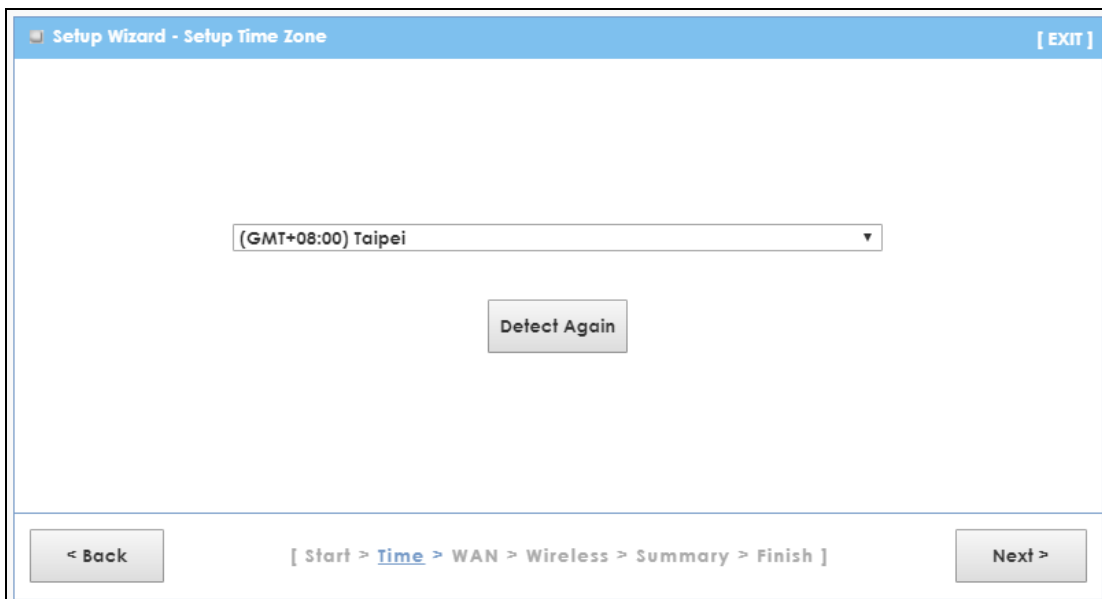


## 3.3 Wizard Setup

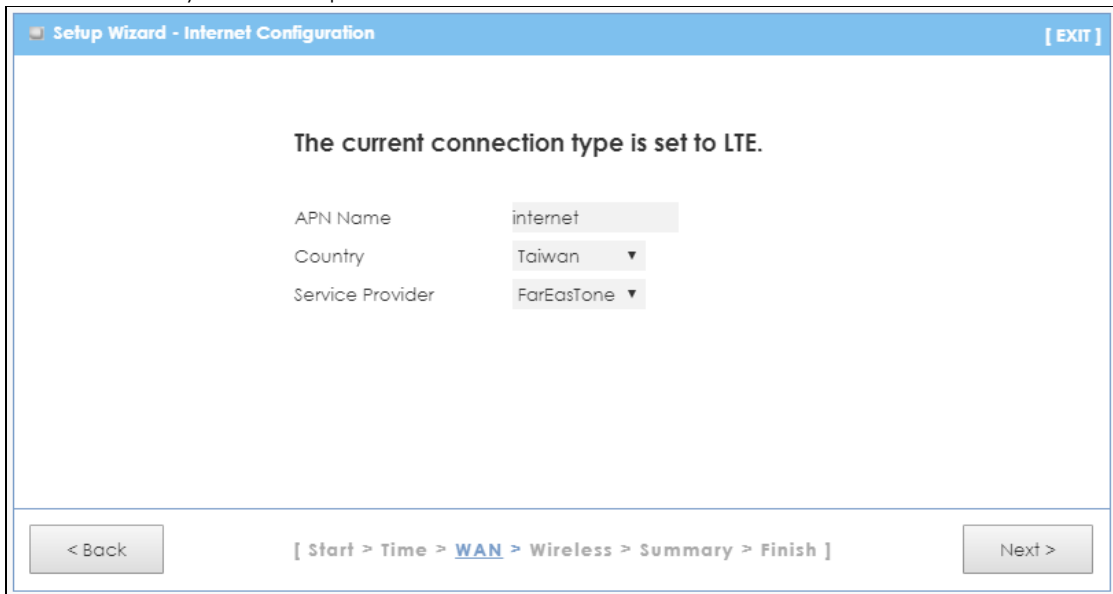
- 1 The first Wizard screen displays showing the main steps in the Wizard setup. Click **Next** to proceed with the time zone setup screen.



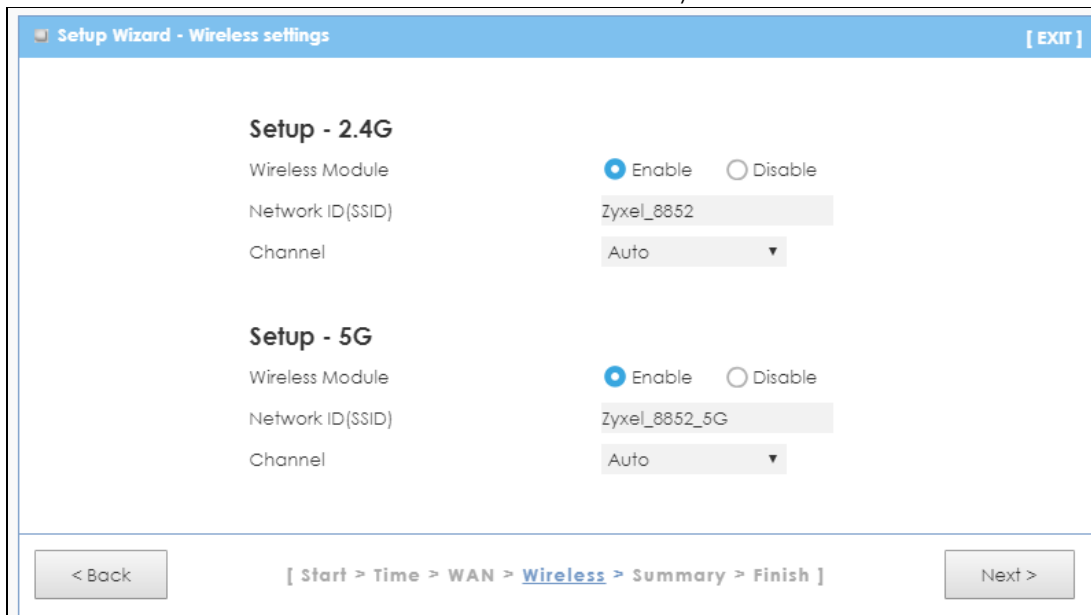
- 2 The LTE automatically detects your location and displays the correct time zone. If the result is not correct, click **Detect Again** or manually select the time zone of the LTE and click **Next**.



- 3 Enter your APN (Access Point Name) provided by your service provider. Select the country where the LTE is located and your service provider name. Click **Next**.



- 4 Use this screen to enable or disable the LTE's wireless LAN, and enter the wireless network name (SSID). Select a channel or use Auto to have the LTE automatically determine a channel to use. Click **Next**.



- 5 Select **WPA2-PSK** and enter a pre-shared key from 8 to 63 case-sensitive characters for data encryption. The wireless clients which want to associate with this wireless network must have the same wireless security settings. Otherwise, select **No Security** to allow any client to associate with this network without any data encryption or authentication. Click **Next**.

**Setup Wizard - Wireless settings** [EXIT]

**Setup - 2.4G**

Security Mode: WPA2-PSK

Pre-Shared Key: 123456789

**Setup - 5G**

Security Mode: WPA2-PSK

Pre-Shared Key: 123456789

< Back [ Start > Time > WAN > **Wireless** > Summary > Finish ] Next >

- 6 Use the read-only summary table to check whether what you have configured is correct. Click **Apply Settings** to save your settings. Otherwise, click **Back** to go back to the previous screens.

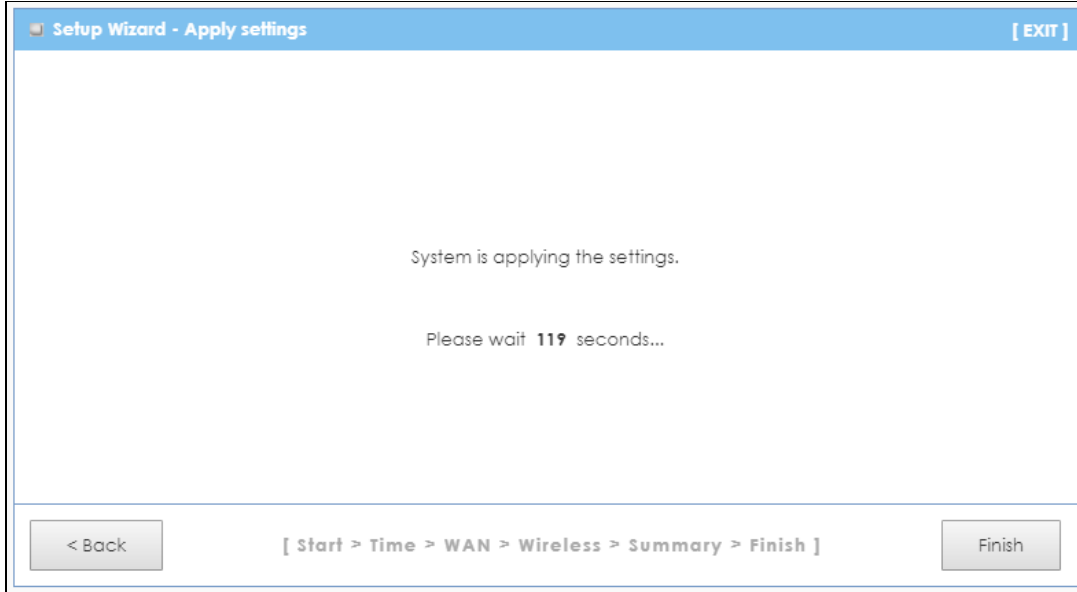
**Setup Wizard - Summary** [EXIT]

Please confirm the information below

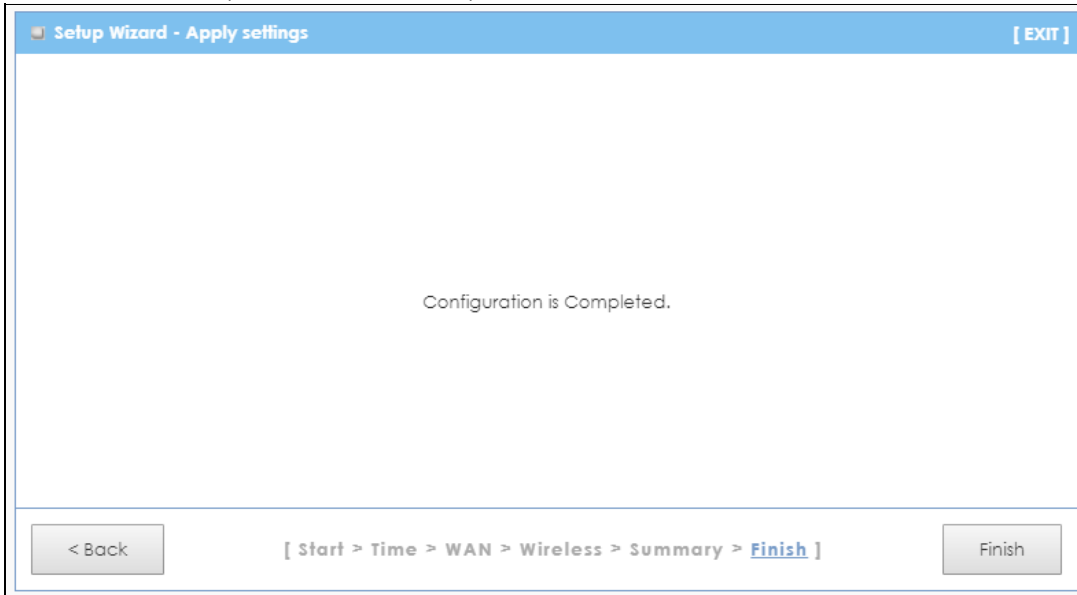
[ WAN Setting ]	
WAN Interface	WAN
WAN Type	3G/4G
APN	internet
[ Wireless Setting - 2.4G ]	
Wireless	Enable
SSID	Zyxel_8852
Channel	Auto
Security Mode	WPA2-PSK
Pre-Shared Key	123456789
[ Wireless Setting - 5G ]	
Wireless	Enable
SSID	Zyxel_8852_5G
Channel	Auto
Security Mode	WPA2-PSK
Pre-Shared Key	123456789

< Back [ Start > Time > WAN > Wireless > **Summary** > Finish ] Apply Settings

- 7 The system takes about 120 seconds to apply settings.



- 8 Click **Finish** to complete the wizard setup.



You are now ready to connect wirelessly to your LTE and access the Internet.

# CHAPTER 4

## Tutorials

### 4.1 Overview

This chapter provides tutorials for setting up your LTE.

- [Connecting to the LTE Using WPS](#)
- [Connect to LTE Wireless Network Without WPS](#)
- [Using Multiple SSIDs on the LTE](#)

### 4.2 Connecting to the LTE Using WPS

This section gives you an example of how to set up a wireless network using WPS. This example uses the LTE as the AP and a WPS-enabled Android 4.4.2 smartphone as the wireless client.

There are two WPS methods for creating a secure connection via the Web Configurator or utility. This tutorial shows you how to do both.

- **Push Button Configuration (PBC)** - create a secure wireless network simply by pressing a button. See [Section 4.2.1 on page 32](#). This is the easier method.
- **PIN Configuration** - create a secure wireless network simply by entering a wireless client's PIN (Personal Identification Number) in the LTE's interface. See [Section 4.2.2 on page 33](#). This is the more secure method, since one device can authenticate the other.

#### 4.2.1 Push Button Configuration (PBC)

- 1 Make sure that your LTE is turned on and that it's within range of your computer.
- 2 WPS is disabled by default on the LTE. log into LTE's Web Configurator and turn it on in the **Configuration > Network > Wireless LAN > WPS Station** screen. You can either press the WPS button on the LTE's panel or press the **Push Button** in the **Configuration > Network > Wireless LAN > WPS Station** screen.

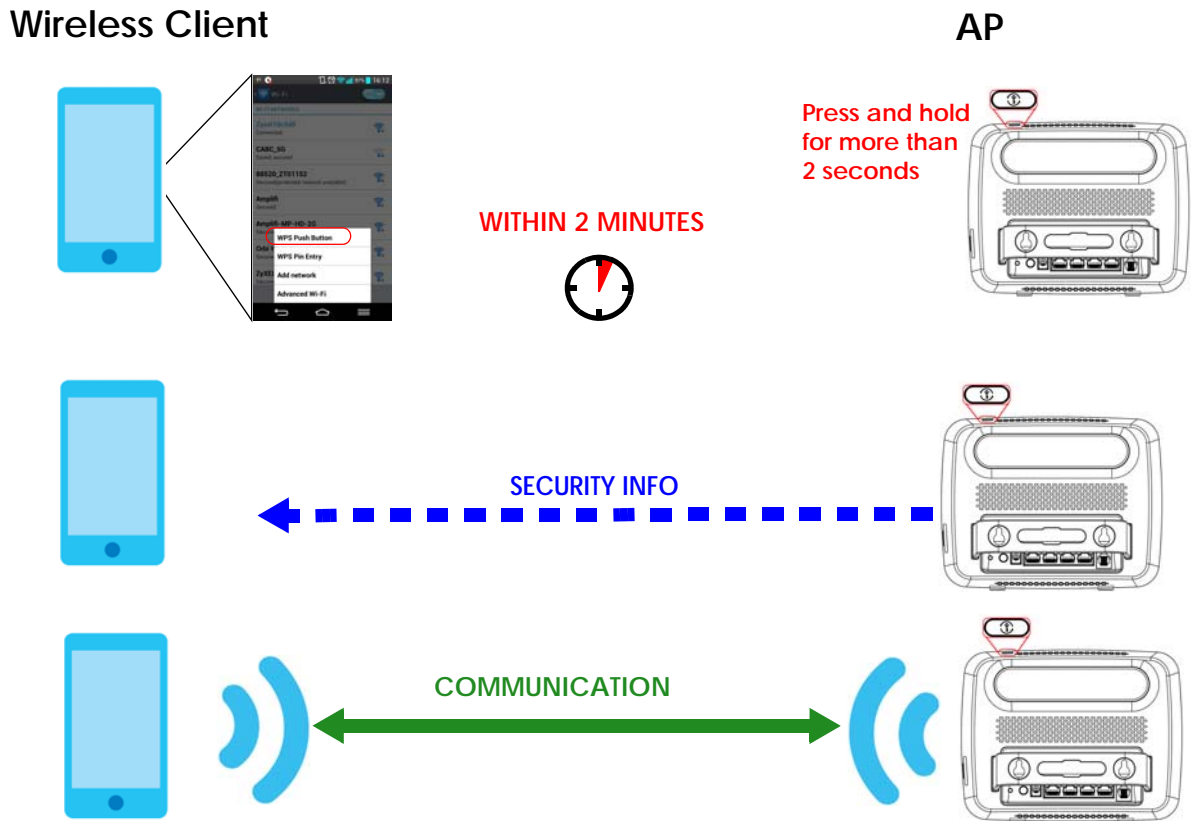
Note: It doesn't matter which button is pressed first. You must press the second button within two minutes of pressing the first one.

The LTE sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the LTE securely.

The following figure shows you an example of how to set up a wireless network and its security by pressing a button on both LTE and wireless client (the Android 4.4.2 phone in this example).



Figure 10 Example WPS Process: PBC Method



## 4.2.2 PIN Configuration

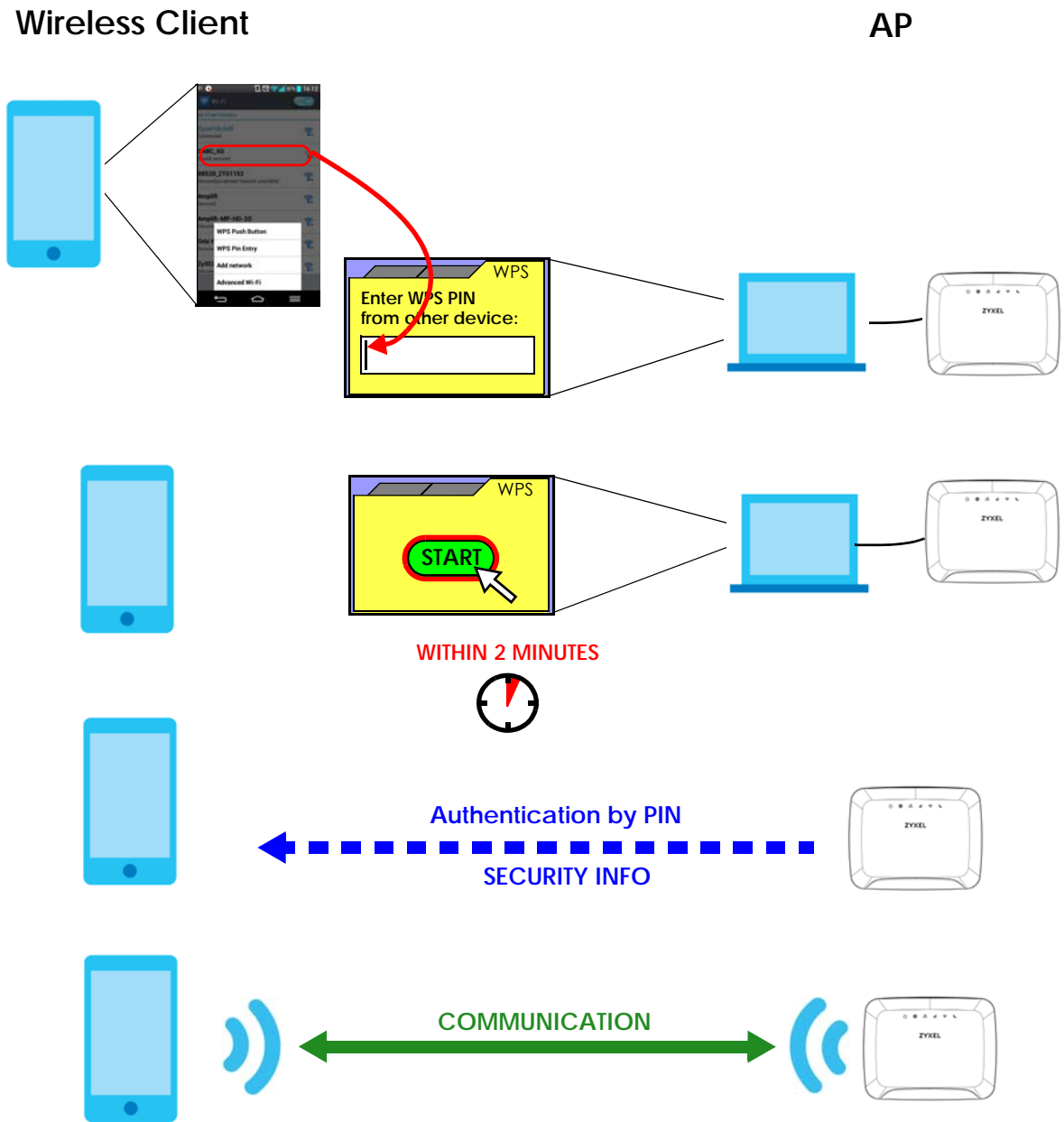
When you use the PIN configuration method, you need to check the client's PIN number and use the LTE's configuration interface.

- 1 Go to your phone settings and turn on WiFi. Open the WiFi networks list and tap WPS PIN Entry to get a PIN number.
- 2 Enter the client's PIN number to the **PIN** field in the **Configuration > Network > Wireless LAN > WPS Station** screen on the LTE.
- 3 Click the **Start** button (or button next to the PIN field) on the LTE's **WPS Station** screen within two minutes.

The LTE authenticates the wireless client and sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the LTE securely.

The following figure shows you how to set up a wireless network and its security on a LTE and a wireless client (android 4.4.2 smartphone) by using PIN method.

Figure 11 Example WPS Process: PIN Method



### 4.3 Connect to LTE Wireless Network Without WPS

This example shows you how to configure wireless security settings with the following parameters on your LTE and connect your computer to the LTE wireless network.

SSID	SSID_Example3
Channel	6
Security	WPA-PSK (Pre-Shared Key: 1234567890)

Follow the steps below to configure the wireless settings on your LTE.

The instructions require that your hardware is connected (see the Quick Start Guide) and you are logged into the Web Configurator through your LAN connection (see [Section 2.3 on page 20](#)).

- 1 Make sure the **WIFI** switch (at the back panel of the LTE) is set to **ON**.
- 2 Open the **Configuration > Network > Wireless LAN > General** screen in the AP's Web Configurator.
- 3 Confirm that the wireless LAN is enabled on the LTE.
- 4 Enter **SSID\_Example3** as the SSID and select **Channel-06** as the channel. Set security mode to **WPA2-PSK** and enter **1234567890** in the **Pre-Shared Key** field. Click **Apply**.

**General** More AP MAC Filter Advanced QoS WPS WPS Station Scheduling WDS

### Wireless Setup - 2.4G

Wireless LAN Status :  Enable  Disable

Name (SSID) : SSID\_Example3

Hide SSID

Channel Selection : 6  Auto Channel Selection

Operating Channel : Channel-1

Channel Width : Auto

802.11 Mode : 802.11b/g/n Mixed

### Security - 2.4G

Security Mode : WPA2-PSK

Encryption : TKIP / AES

Preshared Key : 1234567890  Show Password

Group Key Update Timer : 3600 seconds(Range: 60~86400)

- 5 Open the **Status** screen. Verify your wireless and wireless security settings under **Device Information** and check if the WLAN connection is up under **Interface Status**.

**ZYXEL** LTE3316 Status Monitor Configuration Maintenance Refresh Interval: None

#### Device Information

Item	Data
Host Name :	LTE3316
Model Number :	LTE3316
Firmware Version :	V1.00(ARMP 21C)
<b>WLAN 2.4G:</b>	
Mode :	Access Point Mode
MAC Address :	C8:54:4B:4E:1A:32
SSID :	Zyxel_1A32
Channel :	6
802.11 Mode :	802.11b/g/n Mixed
Security :	WPA2-PSK
<b>WLAN 5G:</b>	
Mode :	Access Point Mode
MAC Address :	C8:54:4B:4E:1A:33
SSID :	Zyxel_1A32_5G
Channel :	36
802.11 Mode :	802.11a/n/ac Mixed
Security :	WPA2-PSK

#### System Status

Item	Data
System Up Time :	0day 0hr 46min 16sec
Current Date/Time :	2019-4-16/18:22:13
System Resource:	
CPU Usage :	25%
Memory Usage :	47%

#### Interface Status

Item	Rate/Status	Item	Rate/Status
Cellular WAN	ON	LAN 3	
Ethernet WAN	OFF	LAN 4	
LAN 1		WLAN 2.4G	ON
LAN 2	1000M	WLAN 5G	ON

#### Summary

[Packet Statistics \(Details...\)](#)  
[WLAN Station Status \(Details...\)](#)  
[LTE Modem Status \(Details...\)](#)

Copyright © 2017 Zyxel Communications Corp. All Rights Reserved.

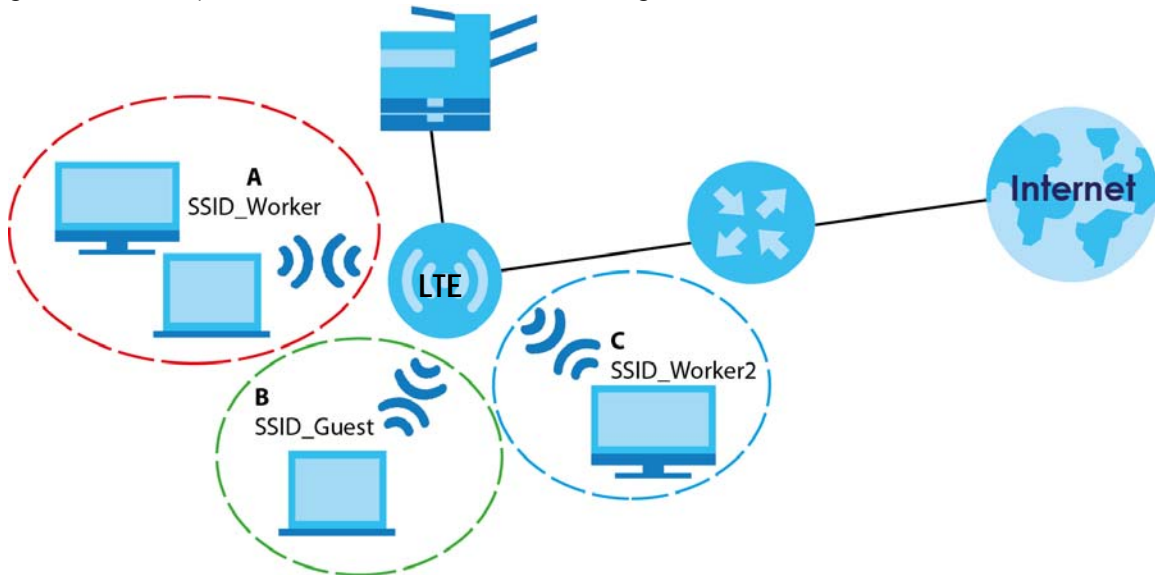
## 4.4 Using Multiple SSIDs on the LTE

You can configure more than one SSID on a LTE. See [Section 8.4 on page 75](#).

This allows you to configure multiple independent wireless networks on the LTE as if there were multiple APs (virtual APs). Each virtual AP has its own SSID, and wireless security type. That is, each SSID on the LTE represents a different access point/wireless network to wireless clients in the network.

Clients can associate only with the SSIDs for which they have the correct security settings. Clients using different SSIDs can access the Internet and the wired network behind the LTE (such as a printer).

For example, you may set up three wireless networks (**A**, **B** and **C**) in your office. **A** is for workers, **B** is for guests and **C** is specific to a VoIP device in the meeting room.



### 4.4.1 Configuring Security Settings of Multiple SSIDs

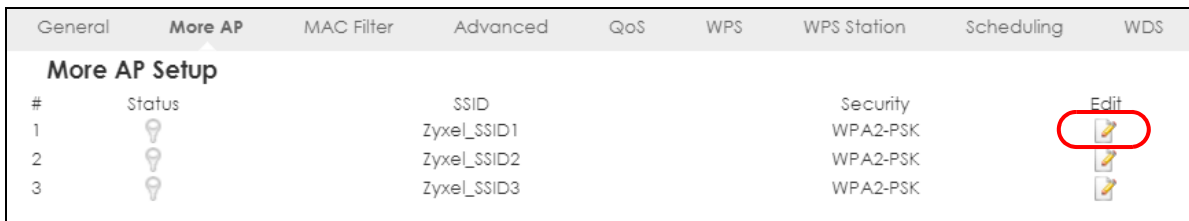
The LTE is in router mode by default.

This example shows you how to configure the SSIDs with the following parameters on your LTE.

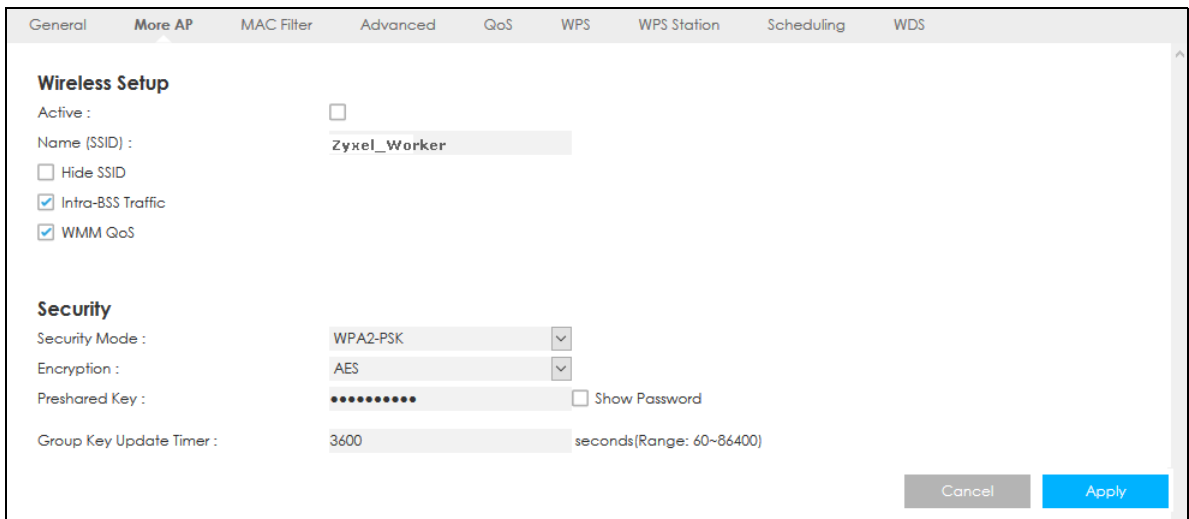
SSID	SECURITY TYPE	KEY
ZyxeL_Worker	WPA2-PSK WPA Compatible	DoNotStealMyWirelessNetwork
ZyxeL_VWorker2	WPA-PSK	12345678
ZyxeL_Guest	WPA-PSK	keyexample123

- 1 Connect your computer to the LAN port of the LTE using an Ethernet cable.
- 2 The default IP address of the LTE is "192.168.1.1". In this case, your computer must have an IP address in the range between "192.168.1.2" and "192.168.1.254".
- 3 Click **Start > Run** on your computer in Windows. Type "cmd" in the dialog box. Enter "ipconfig" to show your computer's IP address.

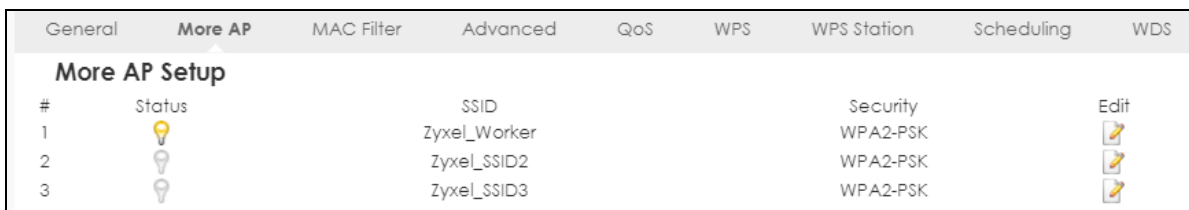
- 4 After you've set your computer's IP address, open a web browser such as Internet Explorer and enter "http://192.168.1.1" as the web address in your web browser.
- 5 Enter "admin" as the user name and "1234" (default) as the password and click **Login**.
- 6 Type a new password and retype it to confirm, then click **Apply**. Otherwise, click **Ignore**.
- 7 Go to **Configuration > Network > Wireless LAN > More AP**. Click the **Edit** icon of the first entry to configure wireless and security settings for **SSID\_Worker**.



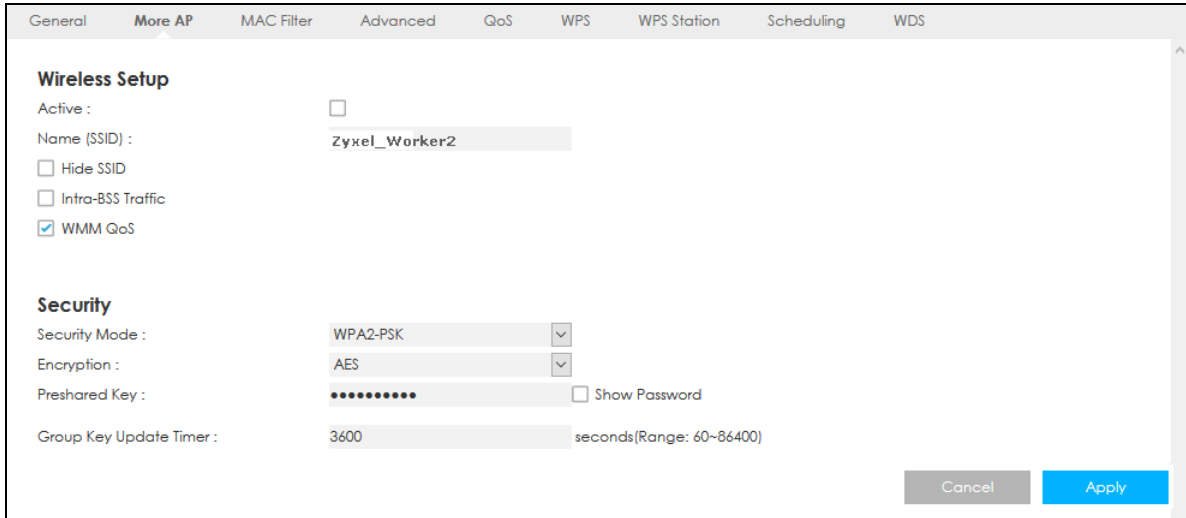
- 8 Configure the screen as follows. In this example, you enable **Intra-BSS Traffic** for **SSID\_Worker** to allow wireless clients in the same wireless network to communicate with each other. Click **Apply**.



- 9 Click the **Edit** icon of the second entry to configure wireless and security settings for **SSID\_Worker2**.



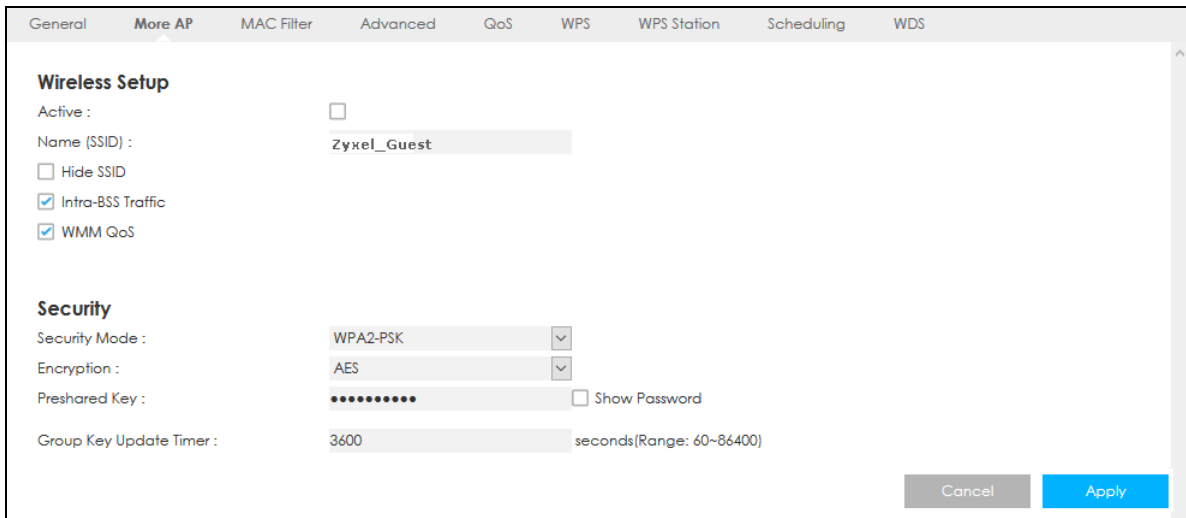
- 10 Configure the screen as follows. You do not enable **Intra-BSS Traffic** for **SSID\_Worker2**. Click **Apply**.



11 Click the **Edit** icon of the third entry to configure wireless and security settings for **SSID\_Guest**.



12 Configure the screen as follows. In this example, you enable **Intra-BSS Traffic** for **SSID\_Guest** to allow wireless clients in the same wireless network to communicate with each other. Click **Apply**.



---

# PART II

## Technical Reference

---

# CHAPTER 5

## Status

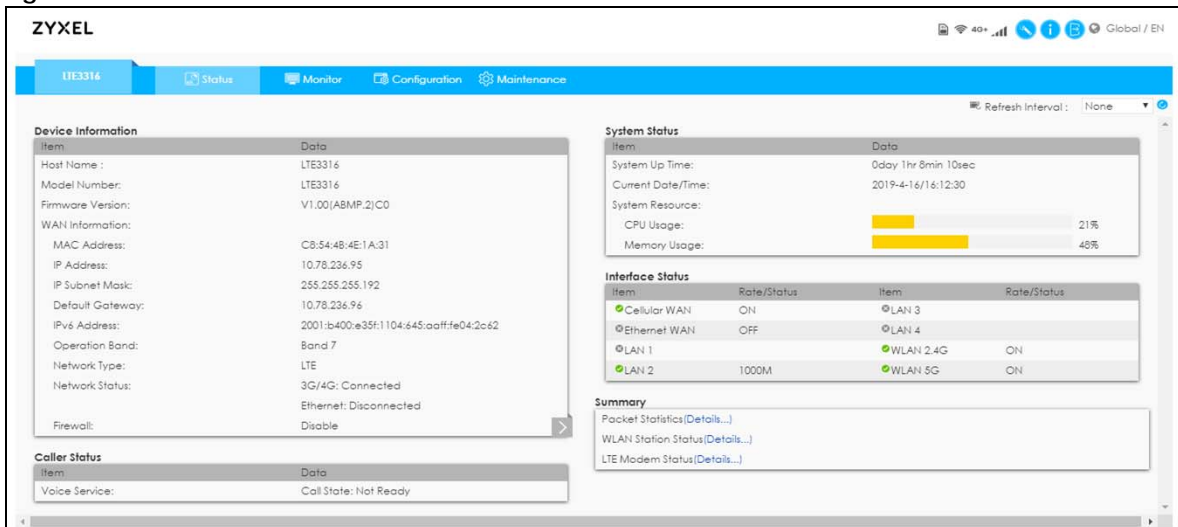
### 5.1 Overview

Use the **Status** screen to check status information about the LTE.

### 5.2 Status

This screen is the first thing you see when you log into the LTE. It also appears every time you click the **Status** icon in the navigation panel. The **Status** screen displays the LTE's connection mode, wireless LAN information and traffic statistics.

Figure 12 Status



The following table describes the labels in this screen.

Table 5 Status

LABEL	DESCRIPTION
Device Information	
Item	This column shows the type of data the LTE is recording.
Data	This column shows the actual data recorded by the LTE.
Host Name	This is the <b>System Name</b> you enter in the <b>Maintenance &gt; General</b> screen. It is for identification purposes.
Model Number	This is the model name of your device.
Firmware Version	This is the firmware version and the date created.
WAN Information	



Table 5 Status (continued)

LABEL	DESCRIPTION
MAC Address	This shows the WAN Ethernet adapter MAC address of your device.
IP Address	This shows the WAN port's IP address.
IP Subnet Mask	This shows the WAN port's subnet mask.
Default Gateway	This shows the WAN port's gateway IP address.
IPv6 Address	This shows the IPv6 address of the LTE on the WAN.
Operation Band	This shows the network type and the frequency band used by the mobile network to which the LTE is connecting.
Network Type	This shows the type of network to which the LTE is connected.
Network Status	This shows cellular WAN connection and Ethernet WAN connection status.
Firewall	This shows <b>Enable</b> when the firewall is activated, and <b>Disable</b> when it is deactivated.
LAN Information	
MAC Address	This shows the LAN Ethernet adapter MAC address of your device.
IP Address	This shows the LAN port's IP address.
IP Subnet Mask	This shows the LAN port's subnet mask.
DHCP	This shows the LAN port's DHCP role - Server or Disable.
IPv6 Address	This shows the IPv6 address of the LTE on the LAN.
WLAN Information	
WLAN Mode	This is the device mode to which the LTE's wireless LAN is set.
MAC Address	This shows the 2.4G wireless adapter MAC address of your device.
WLAN 2.4G	
SSID	This shows a descriptive name used to identify the LTE in the 2.4G wireless LAN.
Channel	This shows the channel number for the current operation channel.
802.11 Mode	This shows the wireless standards the LTE supports.
Security	This shows the level of wireless security the LTE is using.
WLAN 5G	
SSID	This shows a descriptive name used to identify the LTE in the 5G wireless LAN.
Channel	This shows the channel number for the current operation channel.
802.11 Mode	This shows the wireless standards the LTE supports.
Security	This shows the level of wireless security the LTE is using.
Caller Status	
Voice Service	This displays the service type of call made through the LTE.
System Status	
Call State	This shows the status of call/voice mode status.
System Up time	This is the total time the LTE has been on.
Current Date/Time	This field displays your LTE's present date and time.
System Resource	
CPU Usage	This displays what percentage of the LTE's processing ability is currently used. When this percentage is close to 100%, the LTE 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 (for example, using bandwidth management.)
Memory Usage	This shows what percentage of the heap memory the LTE is using.
Interface Status	

Table 5 Status (continued)


LABEL	DESCRIPTION
Item	This displays the LTE port types. The port types are: <b>Cellular WAN</b> , <b>Ethernet WAN</b> , <b>LAN 1-LAN 4</b> , <b>WLAN 2.4G</b> and <b>WLAN 5G</b> .
Rate/Status	<p>For the LAN and WAN ports, this field displays <b>Off</b> (line is down) or <b>On</b> (line is up or connected). For the LAN ports it displays the port speed or is left blank when the line is disconnected. For the WAN port, it always displays the maximum transmission rate.</p> <p>For the <b>WLAN 2.4G</b>, it displays <b>On</b> when the 2.4G WLAN is enabled or <b>Off</b> when the 2.4G WLAN is disabled. For the <b>WLAN 5G</b>, it displays <b>On</b> when the 5G WLAN is enabled or <b>Off</b> when the 2.4G WLAN is disabled. It displays the maximum transmission rate when the WLAN is enabled and is left blank when the WLAN is disabled.</p>
Summary	
Packet Statistics	Click <b>Details...</b> to go to the <b>Monitor &gt; Packet statistics</b> screen ( <a href="#">Section 6.6 on page 46</a> ). Use this screen to view port status and packet specific statistics.
WLAN Station Status	Click <b>Details...</b> to go to the <b>Monitor &gt; WLAN station status</b> screen ( <a href="#">Section 6.7 on page 47</a> ). Use this screen to view the wireless stations that are currently associated to the LTE's 2.4G wireless LAN.
LTE Modem Status	Click <b>Details...</b> to go to the <b>Monitor &gt; LTE modem status</b> screen ( <a href="#">Section 6.8 on page 48</a> ). Use this screen to view the detailed information about the LTE module, cellular interface, and SIM card. You can also view the LTE connection status.

# CHAPTER 6

## Monitor

### 6.1 Overview

This chapter discusses read-only information related to the device state of the LTE.

To access the **Monitor** screens, click  after login.

You can also click the links in the **Summary** table of the **Status** screen to view the packets sent/received as well as the status of wireless clients connected to the LTE.

### 6.2 What You Can Do

- Use the **Log** screen to see the logs for the activity on the LTE ([Section 6.3 on page 43](#)).
- Use the **DHCP Table** screen to view information related to your DHCP status ([Section 6.4 on page 45](#)).
- Use the **ARP Table** screen to view the mapping of IP and MAC addresses ([Section 6.5 on page 45](#)).
- Use the **Packet Statistics** screen to view port status, packet statistics, the system up time ([Section 6.6 on page 46](#)).
- Use the **WLAN station status** screen to view the wireless stations that are currently associated to the LTE ([Section 6.7 on page 47](#)).
- Use the **LTE modem status** screen to view the detailed information about the LTE module, cellular interface, and SIM card. You can also check the LTE connection status ([Section 6.8 on page 48](#)).

### 6.3 Log

The Web Configurator allows you to look at all of the LTE's logs in one location.

#### 6.3.1 View Log

Use the **View Log** screen to see the logged messages for the LTE. The log wraps around and deletes the old entries after it fills. Select what logs you want to see in the **Log Setting** screen. Click **Refresh** to renew the log screen. Click **Clear Log** to delete all the logs.

Figure 13 Monitor &gt; Log &gt; View Log

View Log		Log Setting
Refresh Clear Log		
<b>Summary</b>		
#	Time $\Delta$	Message
1	Jul 23 10:28:10	radvd_cli: radvd_cli is terminated
2	Jul 23 10:28:12	commander: start v6 wan type
3	Jul 23 10:28:13	radvd_cli: radvd_cli is terminated
4	Jul 23 10:28:16	commander: start v6 wan type
5	Jul 23 10:28:17	radvd_cli: radvd_cli is terminated
6	Jul 23 10:28:20	commander: start v6 wan type
7	Jul 23 10:28:21	radvd_cli: radvd_cli is terminated
8	Jul 23 10:28:23	commander: start v6 wan type
9	Jul 23 10:28:25	radvd_cli: radvd_cli is terminated
10	Jul 23 10:28:27	commander: start v6 wan type
11	Jul 23 10:28:28	radvd_cli: radvd_cli is terminated
12	Jul 23 10:28:31	commander: start v6 wan type
13	Jul 23 10:28:32	radvd_cli: radvd_cli is terminated
14	Jul 23 10:28:35	commander: start v6 wan type
15	Jul 23 10:28:36	radvd_cli: radvd_cli is terminated
16	Jul 23 10:28:38	commander: start v6 wan type
17	Jul 23 10:28:40	radvd_cli: radvd_cli is terminated
18	Jul 23 10:28:42	commander: start v6 wan type
19	Jul 23 10:28:43	radvd_cli: radvd_cli is terminated
20	Jul 23 10:28:46	commander: start v6 wan type
21	Jul 23 10:28:47	radvd_cli: radvd_cli is terminated
22	Jul 23 10:28:50	commander: start v6 wan type
23	Jul 23 10:28:51	radvd_cli: radvd_cli is terminated

You can configure which logs to display in the View Log screen. Go to the **Log Setting** screen and select the types of logs you wish to display. You can enable the log server, to send detailed events to this server. Enter its IP address or a Fully Qualified Domain Name (FQDN), and port. Then select the types of logs you wish to send to this server.

Click **Apply** to save your settings. Click **Cancel** to start the screen afresh.

Figure 14 Monitor &gt; Log &gt; Log Setting

View Log		Log Setting
<b>Local Logging</b>		
Log Type	<input type="checkbox"/> System <input type="checkbox"/> Attacks <input type="checkbox"/> Drop <input type="checkbox"/> Debug	
<b>Log Server</b>		
Enable :	<input type="checkbox"/>	
Server IP/FQDN :	<input type="text"/>	
Server Port :	<input type="text" value="514"/>	
Log type :	<input type="checkbox"/> System <input type="checkbox"/> Attacks <input type="checkbox"/> Drop <input type="checkbox"/> Debug	
		<input type="button" value="Cancel"/> <input type="button" value="Apply"/>

## 6.4 DHCP Table

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the LTE's LAN as a DHCP server or disable it. When configured as a server, the LTE provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on that network, or else the computer must be manually configured.

Click **Monitor** > **DHCP Table** to open this screen. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP client information (including MAC address, and IP address) of all network clients using the LTE's DHCP server.

**Figure 15** Monitor > DHCP Table

#	Status	Host Name	IP Address	MAC Address	Reserve
1			192.168.1.9	00:E0:4C:68:02:18	<input type="checkbox"/>

The following table describes the labels on this screen.

**Table 6** Monitor > DHCP Table

LABEL	DESCRIPTION
#	This is the index number of the entry.
Status	This field displays whether the connection to the host computer is up (a lit bulb) or down (a gray bulb).
Host Name	This field displays the computer host name.
IP Address	This field displays the IP address relative to the # field listed above.
MAC Address	This field shows the MAC address of the computer with the name in the Host Name field.  Every Ethernet device has a unique MAC (Media Access Control) address which uniquely identifies a device. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Reserve	Select this if you want to reserve the IP address for this specific MAC address.
Cancel	Click <b>Cancel</b> to reload the previous configuration for this screen.
Apply	Click <b>Apply</b> to save your changes back to the LTE.

## 6.5 ARP Table

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network. Use the ARP table to view IP-to-MAC address mappings.

Click **Monitor > ARP Table** to open the following screen.

**Figure 16** Monitor > ARP Table

ARP Table			
#	IP Address	MAC Address	State

[Refresh](#)

The following screen describes the labels on this screen.

**Table 7** Monitor > ARP Table

LABEL	DESCRIPTION
#	This is the index number of the entry.
IP Address	This is the learned IPv4 or IPv6 IP address of a device connected to a port.
MAC Address	This is the MAC address of the device with the listed IP address.
State	This column shows the current status of the connection.

## 6.6 Packet Statistics

Click **Monitor > Packet Statistics** or the **Packet Statistics (Details...)** hyperlink in the **Status** screen. Read only information here includes port status, packet specific statistics and the "system up time". The **Poll Interval(s)** field is configurable and is used for refreshing the screen.

**Figure 17** Monitor > Packet Statistics

Packet Statistics							
Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
Cellular WAN	Up	389	790	0	0	0	21:6:21
Ethernet WAN	Down	0	0	0	0	0	21:6:21
LAN	1000M	3600	4846	0	0	0	21:6:21
WLAN 2.4G	Up	11	45	0	0	0	21:6:21
WLAN 5G	Up	0	0	0	0	0	21:6:21

System Up Time :21:6:21

Poll Interval(s) :  [Set Interval](#) [Stop](#)

The following table describes the labels on this screen.

Table 8 Monitor > Packet Statistics

LABEL	DESCRIPTION
Port	This is the LTE's interface type.
Status	For the LAN ports, this displays the port speed and duplex setting or <b>Down</b> when the line is disconnected.  For the WAN port, it displays Up when the mobile data connection is up, Connecting when the LTE is trying to bring the mobile data connection up, and displays Down when the 3G/4G connection is down or not activated.  For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and Down when the WLAN is disabled.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Collisions	This is the number of collisions on this port.
Tx B/s	This displays the transmission speed in bytes per second on this port.
Rx B/x	This displays the reception speed in bytes per second on this port.
Up Time	This is the total time the LTE has been for each session.
System Up Time	This is the total time the LTE has been on.
Poll Interval(s)	Enter the time interval in seconds for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the <b>Poll Interval(s)</b> field.
Stop	Click <b>Stop</b> to stop refreshing statistics.

## 6.7 WLAN Station Status

Click **Monitor > WLAN station status** or the **WLAN Station Status (Details...)** hyperlink in the **Status** screen. View the wireless stations that are currently associated to the LTE's 2.4G and 5G wireless network in the Association List. Association means that a wireless client (for example, your network or computer with a wireless network card) has connected successfully to the AP (or wireless router) using the same SSID, channel and security settings.

Click **Monitor > WLAN Station Status** to open the following screen.

Figure 18 Monitor > WLAN Station Status



Association List		
<b>Association List - 2.4G</b>		
#	MAC Address	Association Time
<b>Association List - 5G</b>		
#	MAC Address	Association Time

The following table describes the labels on this screen.

Table 9 Monitor > WLAN Station Status

LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.
Association Time	This field displays the time a wireless station first associated with the LTE's WLAN.

## 6.8 LTE Modem Status

Click **Monitor > LTE Modem Status** to open the following screen.

Figure 19 Monitor > LTE Modem Status

LTE Modem Status									
<b>Modem Information</b>									
Module Name	IMEI/MEID	HW Version	FW Version						
EG06	355498090000001	E	EG06ELAR01A04M4G_BETA1228						
<b>SIM Status</b>									
PIN Code Status	PIN Code Remaining Times		PUK Code Remaining Times						
Ready	3		10						
<b>Service Information</b>									
Operator	Cell Broadcast	MCC	MNC	LAC	TAC	Cell ID	Service Type	Operation Band	RSSI
Far EasTone	N/A	466	1	N/A	59242	56410645	LTE	Band 28	-77
CS Register Status	PS Register Eclo Status	PS Attached Status	Roaming Status	IMSI	SMSC	MSISDN			
Registered	N/A Registered	Attached	Not Roaming	466011801891892	+886931000099	N/A			
RSRP	RSRQ	SINR	PLMN	MIMO	Support Band List				
-105	-11	14	46601	1T2R	WCDMA 2100/WCDMA 1800/WCDMA 850/WCDMA 900/LTE Band1 (2100MHz)/LTE Band3 (1800MHz)/LTE Band5 (850MHz)/Band7 (2600MHz)/Band8 (900MHz)/LTE Band20 (800MHz)/LTE Band28 (700MHz)/LTE Band32 (1500MHz)/LTE Band38 (2600MHz)/LTE Band40 (2300MHz)/LTE Band41 (2500MHz)				

The following table describes the labels on this screen.

Table 10 Monitor > LTE Modem Status

LABEL	DESCRIPTION
Modem Information	
Module Name	This displays the name of the built-in LTE module.



Table 10 Monitor &gt; LTE Modem Status (continued)

LABEL	DESCRIPTION
IMEI/MEID	This displays the International Mobile Equipment Number (IMEI) or Mobile Equipment Identifier (MEID), which is the serial number of the built-in LTE module. It is a unique 15-digit number used to identify a mobile device.
HW Version	This displays the hardware version of the built-in LTE module.
FW Version	This displays the firmware version of the built-in LTE module.
SIM Status	
PIN Code Status	This displays the status of PIN code authentication.
PIN Code Remaining Times	This displays how many times you can enter the PIN code.
PUK Code Remaining Times	This displays how many times you can enter the PUK code.
Service Information	
Operator	This displays the name of the service provider.
Cell Broadcast	This displays whether the one-to-many messaging service is available.
MCC	This displays the Mobile Country Code (MCC), which is used to identify the country of a mobile subscriber.
MNC	This displays the Mobile Network Code (MNC), which is used in combination with MCC to identify the public land mobile network (PLMN) of a mobile subscriber.
LAC	This displays the 2-octet Location Area Code (LAC), which is used to identify a location area within a PLMN.
TAC	This displays the Tracking Area Code (TAC), which is to identify a tracking area within a PLMN.
Cell ID	This displays the ID of a cell at the physical layer.
Service Type	This displays the type of the mobile network to which the LTE is connecting.
Operation Band	This displays the network type and the frequency band used by the mobile network to which the LTE is connecting.
RSSI	This displays the received signal strength indicator (RSSI), that is, the received signal strength in dBm.
CS Register Status	This displays the Circuit Switched (CS) network registration status.
Eclo	This displays the ratio (in dB) of the received energy per chip and the interference level.
PS Register Status	This displays the Packet Switched (PS) network registration status.
PS Attached Status	This displays the Packet switched Domain Attachment status.
Roaming Status	This displays whether the LTE is connected to another service provider's mobile network using roaming.
IMSI	This displays the International Mobile Subscriber Identity (IMSI) stored in the SIM (Subscriber Identity Module) card. The SIM card is installed in a mobile device and used for authenticating a customer to the carrier network. IMSI is a unique 15-digit number used to identify a user on a network.
SMSC	This displays the number for Short Message Service Center (SMSC), which stores, forwards and delivers SMS text message.
MSISDN	This displays the MSISDN (Mobile Subscriber ISDN) number, a phone number assigned to a mobile subscriber to call a mobile device.
RSRP	This displays the Reference Signal Receive Power (RSRP), which is the average received power of all Resource Elements (RE) that carry cell-specific Reference Signals (RS) within the specified bandwidth.
RSRQ	This displays the Reference Signal Received Quality (RSRQ), which is the ratio of RSRP to the E-UTRA carrier RSSI and indicates the quality of the received reference signal.

Table 10 Monitor &gt; LTE Modem Status (continued)

LABEL	DESCRIPTION
SINR	This displays the Signal to Interference plus Noise Ratio (SINR). A negative value means more noise than signal.
PLMN	This displays the Public Land Mobile Network (PLMN) code of the mobile network.
MIMO	This displays the MIMO (Multi-input Multi-output) technology supported by the LTE, such as 1T2R (1 Transmit and 2 Receive paths/antennas) or TM1-TM4 (Transmission Mode 4).
Support Band List	This displays the frequency bands that are supported by the LTE.

# CHAPTER 7

## WAN

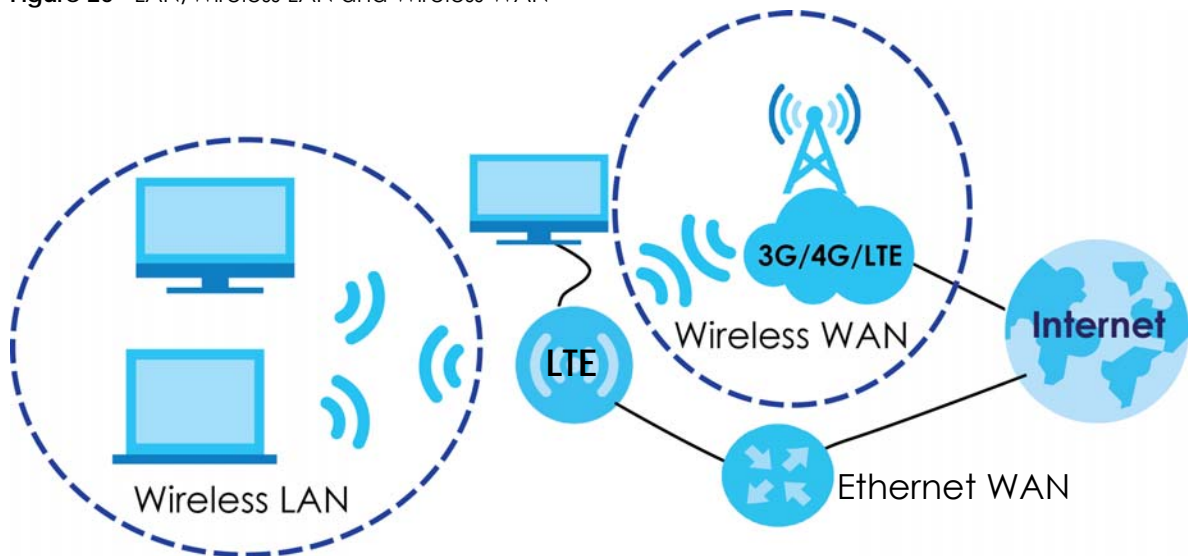
### 7.1 Overview

This chapter discusses the LTE's **WAN** screens. Use these screens to configure your LTE for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

3G and 4G standards for the sending and receiving of voice, video, and data in a mobile environment. You can insert a 4G SIM card and set the LTE to use this 3G/4G connection as your WAN.

**Figure 20** LAN/Wireless LAN and Wireless WAN



### 7.2 What You Can Do

- Use the **WAN Management** screen to configure 3G/4G WAN connection settings ([Section 7.4 on page 54](#)).
- Use the **Network Scan** screen to specify the type of the mobile network to which the LTE is connected and how you want the LTE to connect to an available mobile network ([Section 7.5 on page 60](#)).
- Use the **IPv6** screen to configure the LTE's IPv6 settings ([Section 7.6 on page 61](#)).
- Use the **PIN Management** screen to enable or disable PIN code authentication ([Section 7.7 on page 63](#)).

## 7.3 What You Need To Know

The information in this section can help you configure the screens for your WAN connection, as well as enable/disable some advanced features of your LTE.

### 3G

3G (Third Generation) is a digital, packet-switched wireless technology. Bandwidth usage is optimized as multiple users share the same channel and bandwidth is only allocated to users when they send data. It allows fast transfer of voice and non-voice data and provides broadband Internet access to mobile devices.

### 4G

4G is the fourth generation of the mobile telecommunications technology and a successor of 3G. Both the WiMAX and Long Term Evolution (LTE) standards are the 4G candidate systems. 4G only supports all-IP-based packet-switched telephony services and is required to offer gigabit speed access.

### DNS Server Address Assignment

Use Domain Name System (DNS) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of `www.zyxel.com` is `204.217.0.2`. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

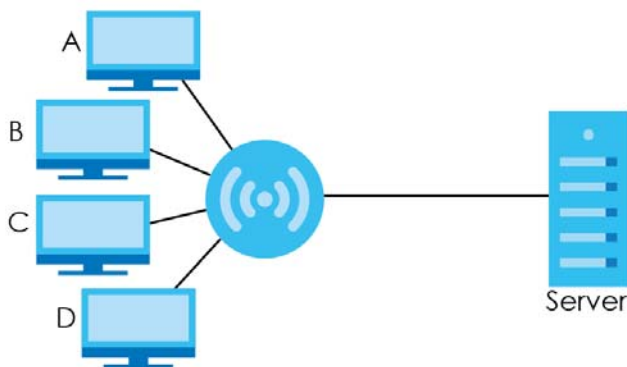
The LTE can get the DNS server addresses in the following ways.

- 1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
- 2 If your ISP dynamically assigns the DNS server IP addresses (along with the LTE's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

### Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

**Figure 21** Multicast Example



In the multicast example above, systems **A** and **D** comprise one multicast group. In multicasting, the server only needs to send one data stream and this is delivered to systems **A** and **D**.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group - it is not used to carry user data. The LTE supports both IGMP version 1 (**IGMP v1**), IGMP version 2 (**IGMP v2**) and IGMP version 3 (**IGMP v3**).

At start up, the LTE queries all directly connected networks to gather group membership. After that, the LTE periodically updates this information. IP multicasting can be enabled/disabled on the LTE WAN interface in the Web Configurator.

## IPv6 Introduction

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to  $3.4 \times 10^{38}$  IP addresses. The LTE can use IPv4/IPv6 dual stack to connect to IPv4 and IPv6 networks, and supports IPv6 stateless autoconfiguration (SLAAC).

## IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` Or `2001:db8:0:0:1a2f::15`.

## IPv6 Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as "/x" where x is a number. For example,

```
2001:db8:1a2b:15::1a2f:0/32
```

means that the first 32 bits (`2001:db8`) is the subnet prefix.



## IPv6 Subnet Masking

Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block's 16 bits are then represented by four hexadecimal characters. For example, `FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000`.

## 7.4 WAN Management

The summary table shows you the WAN connections configured on the LTE. Click **Configuration > Network > WAN > WAN Management** from the **Configuration** menu.

**Figure 22** Configuration > Network > WAN > WAN Management

WAN Management		Network Scan	IPv6	PIN Management	
<b>WAN Entries</b>					
Interface Name	Physical Interface	Operation Mode	WAN Type	Action	
WAN-1	3G/4G	Always on	3G/4G		
WAN-2	Ethernet	Disable	Dynamic IP		

The following table describes the labels in this screen.

**Table 11** Configuration > Network > WAN > WAN Management

LABEL	DESCRIPTION
Interface Name	This field displays the name of the WAN interface for this connection.
Physical Interface	This field displays the LTE's WAN physical connections.
IP Address	This field displays the IPv4 and IPv6 addresses of the WAN connection.
Operation Mode	This field indicates whether the IPv4 and IPv6 connectivity is available.
WAN Type	This field displays the type of the WAN connection.
Action	Click the Edit icon to configure the WAN connection settings.

### 7.4.1 WAN Management Edit 3G/4G

Use this screen to change your LTE's 3G/4G WAN connection settings. Click the Edit icon in the **Physical Interface: 3G/4G** row in the **Configuration > Network > WAN > WAN Management** screen.

Figure 23 WAN Management Edit 3G/4G

### Cellular WAN

Antenna Select :

Network Type :

Band Selection :

Band List :

3G

- Band1 (2100MHz)
- Band3 (1800MHz)
- Band5 (850MHz)
- Band8 (900MHz)

4G

- Band1 (2100MHz)
- Band3 (1800MHz)
- Band5 (850MHz)
- Band7 (2600MHz)
- Band8 (900MHz)
- Band20 (800MHz)
- Band28 (700MHz)
- Band32 (1500MHz)
- Band38 (2600MHz)
- Band40 (2300MHz)
- Band41 (2500MHz)

Roaming :  Enable

Dial-Up Profile :

Authentication :

IP Type :

IP Mode :

Primary DNS :  (Optional)

Secondary DNS :  (Optional)

MTU :

IGMP :  Enable

IGMP Proxy :  Enable

Bridge Mode :  Enable

Bridge Mode Fixed MAC :

### Network Monitoring

Network Monitoring :  Enable

Checking By :  DNS Query  ICMP Checking

Loading Check :  Enable

Check Interval :  (seconds)

Check Timeout :  (seconds)

Latency Threshold :  (ms)

Fail Threshold :  (Times)

Target1 :

Target2 :

The following table describes the labels in this screen.

Table 12 Management WAN Edit: 3G/4G

LABEL	DESCRIPTION
Cellular WAN	
Antenna Select	Select <b>Internal</b> for the LTE to use its internal antennas for WAN connection. If you attached external antennas (not included) to the LTE, select <b>External</b> . Select <b>Auto</b> for the LTE to automatically select the antennas for WAN connection.

Table 12 Management WAN Edit: 3G/4G (continued)

LABEL	DESCRIPTION
Network Type	Select the type of the network ( <b>4G</b> or <b>3G</b> ) to which you want the LTE to connect. Otherwise, select <b>Auto</b> to have the LTE connect to an available network using the default settings on the SIM card. If the currently registered mobile network is not available or the mobile network's signal strength is too low, the LTE switches to another available mobile network.
Band Selection	Select <b>Manual</b> to select the frequency bands the LTE uses to connect to the mobile network. Otherwise, select <b>Auto</b> to have the LTE connect to any available frequency band using the default settings
Band List	Select the frequency bands you want the LTE to use to connect to the mobile network.  You can only select the frequency bands from this list if you selected <b>Manual</b> in the <b>Band Selection</b> field.
Roaming	3G/4G roaming is to use your mobile device in an area which is not covered by your service provider. Enable roaming to ensure that your LTE is kept connected to the Internet when you are traveling outside the geographical coverage area of the network to which you are registered.
Dial-Up Profile	Select <b>Auto-Detection</b> to have the LTE use the inserted SIM card's default settings to connect to any available mobile network.  Select <b>Manual</b> and enter the information provided by your service provider to connect to the service provider's mobile network.
APN	Connections with different APNs (Access Point Names) may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charge method.  The corresponding APN automatically displays when you select a pre-defined service provider.  If you select <b>Manual</b> in the <b>Dial-Up Profile</b> field, manually enter the APN provided by your service provider. You can enter up to 32 ASCII printable characters. Spaces are allowed.
Dial Number	This is the phone number (dial string) used to dial up a connection to your service provider's base station. Your service provider should provide the phone number. For example, *99# is the dial string to establish a GPRS or 3G/4G connection in Taiwan.  The corresponding phone number automatically displays when you select a pre-defined service provider.  If you select <b>Others</b> in the <b>Service Provider</b> field, manually enter the phone number provided by your service provider.
Account	Type the user name (of up to 64 ASCII printable characters) given to you by your service provider.
Password	Type the password (of up to 64 ASCII printable characters) associated with the user name above.
Authentication	The LTE supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms  Select an authentication protocol ( <b>PAP</b> , or <b>CHAP</b> ) used by the service provider. Otherwise, select <b>Auto</b> to have the LTE accept either CHAP or PAP.
IP Type	Select <b>IPv4</b> if you want the LTE3202-M430 to run IPv4 only.  Select <b>IPv6</b> if you want the LTE3202-M430 to run IPv6 only.  Select <b>IPv4/IPv6</b> to allow the LTE3202-M430 to run IPv4 and IPv6 at the same time.
IP Mode	Select <b>Dynamic IP</b> if you have a dynamic IP address.  Select <b>Static IP</b> if you have a fixed IP address assigned by your service provider.
IP Address	Enter your WAN IP address in this field if you selected <b>Static IP</b> in the <b>IP Mode</b> field.
IP Subnet Mask	Enter the subnet mask in this field if you selected <b>Static IP</b> in the <b>IP Mode</b> field.



Table 12 Management WAN Edit: 3G/4G (continued)

LABEL	DESCRIPTION
IP Gateway	Enter the gateway IP address in this field if you selected <b>Static IP</b> in the <b>IP Mode</b> field.
Primary DNS	Enter the first DNS server address assigned by the service provider.
Secondary DNS	Enter the second DNS server address assigned by the service provider.
MTU	Enter the MTU (Maximum Transmission Unit) of each data packet, in bytes, that can move through the WAN connection.
IGMP	Select this to enable multicasting. This applies to traffic routed from the WAN to the LAN. Disable it to turn off this feature. This may cause incoming traffic to be dropped or sent to all connected network devices.
IGMP Proxy	Select this option to have the LTE act as an IGMP proxy on this connection. This allows the LTE to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Bridge Mode	Select this option to allow the computer connected to the first Ethernet LAN port to get an individual IP address from the ISP's DHCP server directly. In Bridge mode, the Multy Device broadcasts traffic to the local network from the Internet. Choose Bridge mode if you have an existing router in your network and you do not want to reconfigure routing settings.
Bridge Mode Fixed MAC	Specify the MAC address to which the WAN IP address is destined.
Network Monitoring	Select this option to have the LTE test the WAN connection.
Checking By	Select <b>DNS Query</b> to periodically send a DNS query to a DNS server. Select <b>ICMP Checking</b> to send a ping to either the default gateway or the addresses you specify in the <b>Target1</b> and <b>Target2</b> fields.
Loading Check	Select this option to check how many packets have been transmitted or received through the WAN connection within a time period specified in the <b>Check Interval</b> field.
Check Interval	Type a number of seconds (0 to 99999) to set the time interval between checks. Allow more time if your destination IP address handles lots of traffic.
Check Timeout	Type the number of seconds (0 to 99999) for your LTE to wait for a response to the ping or DNS query before considering the check to have failed. This setting must be less than the <b>Check Interval</b> . Use a higher value in this field if your network is busy or congested.
Latency Threshold	Type a number of milliseconds (0 to 99999) for the latency threshold.  If the specified latency threshold is exceeded, the LTE considers the check to have failed and makes a new connection after (Latency Threshold * Fail Threshold) seconds.
Fail Threshold	Type how many WAN connection checks can fail (0 to 99999) before the connection is considered "down" (not connected). The LTE still checks a "down" connection to detect if it reconnects.
Target1 / Target 2	Select <b>DNS1</b> to have the LTE send a DNS query to the first DNS server address assigned by the service provider.  Select <b>DNS2</b> to have the LTE send a DNS query to the second DNS server address assigned by the service provider.  Select <b>Gateway</b> to have the LTE ping the WAN interface's default gateway IP address.  Select <b>Other Host</b> and enter a domain name or IP address of a reliable nearby computer to have the LTE ping that address.

## 7.4.2 WAN Management Edit Ethernet

The LTE has 4 LAN Ethernet ports, you can configure **LAN 1** port to work as a WAN port if needed. This WAN port will work as a fail-over port, which means that if the 3G/4G WAN connection fails, the LTE will use the WAN Ethernet connection for backup.

Use this screen to enable the **LAN 1** port as a WAN port, and configure its settings. Click the Edit icon in the **Physical Interface: Ethernet** row in the **Configuration > Network > WAN > Management WAN** screen.

**Figure 24** WAN Management Edit Ethernet

The screenshot shows the 'WAN Management' configuration page for 'Ethernet WAN'. It includes sections for enabling the WAN port, selecting a WAN type (Dynamic IP), and configuring dynamic IP settings such as Host Name, ISP Registered MAC Address, MTU, and Network Monitoring (DNS Query, ICMP Checking, Loading Check, Check Interval, Check Timeout, Latency Threshold, Fail Threshold, Target1, Target2). Buttons for 'Cancel' and 'Apply' are visible at the bottom right.

The following table describes the labels in this screen.

**Table 13** WAN Management Edit Ethernet

LABEL	DESCRIPTION
Ethernet WAN	
Port 1 config as WAN port	Select this so the <b>LAN 1</b> Ethernet port works a WAN port.
WAN Type	Select the routing method used by your ISP from the drop-down list box. Select <b>Static IP</b> if you have a fixed IP address assigned by your ISP. Select <b>Dynamic IP</b> if you want to obtain an IP address from a DHCP server. Select <b>PPPoE</b> if your ISP requires you to use a PPPoE connection to the Internet. This method of connection typically requires you to enter a Username and Password (provided by your ISP) to gain access to the Internet. You need to ensure that any PPPoE client software on your computer is removed or disabled.
Dynamic IP WAN Type Configuration These fields appears when you select <b>Dynamic IP</b> in the <b>WAN Type</b> field.	
Host Name	Type a host name for the Ethernet WAN interface.
ISP Registered MAC Address	Click the <b>Clone</b> button and the LTE will enter the MAC address of the computer on the LAN automatically. Click the <b>Clear</b> button to remove the MAC address from this field.
Static IP WAN Type Configuration These fields appears when you select <b>Static IP</b> in the <b>WAN Type</b> field.	
WAN IP Address	Enter your WAN IP address in this field.
WAN Subnet Mask	Enter the subnet mask in this field.

Table 13 WAN Management Edit Ethernet (continued)

LABEL	DESCRIPTION
WAN Gateway	Enter the gateway IP address.
Primary DNS	Enter the first DNS server address assigned by the service provider.
Secondary DNS	Enter the second DNS server address assigned by the service provider.
PPoE WAN Type Configuration	
These fields appears when you select <b>PPPoE</b> in the <b>WAN Type</b> field.	
PPPoE Account	Type the user name or account given by your ISP.
PPPoE Password	Type the password associated to this account.
Primary DNS	Enter the first DNS server address assigned by the service provider.
Secondary DNS	Enter the second DNS server address assigned by the service provider.
Service Name	Type the PPPoE <b>Service Name</b> from your ISP provider. PPPoE uses a service name to identify and reach the PPPoE server.
Assigned IP Address	Enter the IP address assigned by your ISP.
MTU	Enter the MTU (Maximum Transmission Unit) of each data packet, in bytes, that can move through the WAN connection.
Network Monitoring	Select this option to have the LTE test the WAN connection by periodically sending <b>DNS Query</b> to a DNS server or sending a ping ( <b>ICMP Checking</b> ) to either the default gateway or the addresses you specify in the <b>Target1</b> and <b>Target2</b> fields.
Loading Check	Select this option to check how many packets have been transmitted or received through the WAN connection within a time period specified in the <b>Check Interval</b> field.
Check Interval	Type a number of seconds (0 to 99999) to set the time interval between checks. Allow more time if your destination IP address handles lots of traffic.
Check Timeout	Type the number of seconds (0 to 99999) for your LTE to wait for a response to the ping or DNS query before considering the check to have failed. This setting must be less than the <b>Check Interval</b> . Use a higher value in this field if your network is busy or congested.
Latency Threshold	Type a number of milliseconds (0 to 99999) for the latency threshold.  If the specified latency threshold is exceeded, the LTE considers the check to have failed and makes a new connection after (Latency Threshold * Fail Threshold) seconds.
Fail Threshold	Type how many WAN connection checks can fail (0 to 99999) before the connection is considered "down" (not connected). The LTE still checks a "down" connection to detect if it reconnects.
Target1 / Target 2	Select <b>DNS1</b> to have the LTE send a DNS query to the first DNS server address assigned by the service provider.  Select <b>DNS2</b> to have the LTE send a DNS query to the second DNS server address assigned by the service provider.  Select <b>Gateway</b> to have the LTE ping the WAN interface's default gateway IP address.  Select <b>Other Host</b> and enter a domain name or IP address of a reliable nearby computer to have the LTE ping that address.

## 7.5 Network Scan

Use this screen to set how you want the LTE to connect to an available mobile network. Click **Configuration > Network > WAN > Network Scan** from the **Configuration** menu.

**Figure 25** Configuration > Network > WAN > Network Scan

The screenshot shows the 'Network Scan' configuration screen. At the top, there are tabs for 'WAN Management', 'Network Scan', 'IPv6', and 'PIN Management'. The 'Network Scan' tab is active. Below the tabs, the 'Configuration' section includes:
 

- Physical Interface :** 3G/4G
- Network Type :** Auto (dropdown menu)
- Scan Approach :** Manual (dropdown menu)

 Below the configuration fields are two buttons: 'Scan' and 'Apply'. Underneath these is a table header for 'Network Provider List' with columns: 'Provider Name', 'Mobile System', 'Network Status', and 'Action'. At the bottom of the screen are three buttons: 'Cancel', 'Refresh', and 'Apply'.

The following table describes the labels in this screen.

**Table 14** Configuration > Network > WAN > Network Scan

LABEL	DESCRIPTION
Physical Interface	This shows the type of the interface used by the WAN connection.
Network Type	Select the type of the network ( <b>4G only</b> , <b>3G only</b> , or <b>Auto</b> ) to which you want the LTE to connect when there is a SIM card inserted.
Scan Approach	Select <b>Auto</b> to have the LTE connect to an available network using the default settings on the SIM card. If the currently registered mobile network is not available or the mobile network's signal strength is too low, the LTE switches to another available mobile network. Select <b>Manual</b> to search for and select the mobile networks to which you want the LTE to connect.
Network Provider List	This table is available only when you set <b>Scan Approach</b> to <b>Manual</b> . Click <b>Scan</b> to search for available mobile networks based on the network type you selected. Click <b>Apply</b> to save your changes in the <b>Action</b> field.
Provider Name	This shows the name of the service provider.
Mobile System	This shows the mobile telecommunications standard supported by the mobile network.
Network Status	This shows whether the mobile network is available.
Action	Click <b>Select</b> to have the LTE establish a connection to the selected mobile network.
Cancel	Click <b>Cancel</b> to reload the previous configuration for this screen.
Refresh	Click <b>Refresh</b> to update this screen.
Apply	Click <b>Apply</b> to save your changes back to the LTE.

## 7.6 IPv6

Use this screen to configure the LTE's IPv6 settings. Click **Configuration > Network > WAN > IPv6** from the **Configuration** menu.

**Figure 26** Configuration > Network > WAN > IPv6

The screenshot shows the 'IPv6 Setup' configuration screen. At the top, there are four tabs: 'WAN Management', 'Network Scan', 'IPv6' (selected), and 'PIN Management'. Below the tabs, the 'IPv6 Setup' section contains the following fields and options:

- IPv6 :** Radio buttons for  Enable and  Disable.
- IPv6 Connection :** A dropdown menu currently set to 'DHCPv6'.
- DNS Setting :** Radio buttons for  Obtain DNS Server address Automatically and  Use the following DNS address.
- Primary DNS Address :** An empty text input field.
- Secondary DNS Address :** An empty text input field.
- LAN IPv6 Address :** A text input field with a placeholder and a '/64' suffix.
- LAN IPv6 Link-Local Address :** A text input field with the value 'fe80::8e59:73ff:fe27:8852'.
- Auto configuration :** Radio buttons for  Enable and  Disable.
- Auto configuration Type :** A dropdown menu currently set to 'Stateless'.

At the bottom right of the screen, there are two buttons: 'Cancel' (grey) and 'Apply' (blue).

The following table describes the labels in this screen.

**Table 15** Configuration > Network > WAN > IPv6

LABEL	DESCRIPTION
IPv6	Select <b>Enable</b> to allow the LTE to run IPv6. Otherwise, select <b>Disable</b> .
IPv6 Connection	This displays <b>Static IPv6</b> if you have a fixed IPv6 address assigned by your ISP. This displays <b>DHCPv6</b> if you want to obtain an IPv6 address from a DHCPv6 server.
(These fields appear when the <b>IPv6 Connection</b> is set to <b>Static IPv6</b> .)	
IPv6 Address	Enter the IPv6 address on the WAN side in this field.
Subnet Prefix Length	Enter the address prefix length to specify how many most significant bits in an IPv6 address compose the network address.
Default Gateway	Enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your LTE's interfaces. The gateway helps forward packets to their destinations.
Primary DNS Address	Enter the first IPv6 DNS server address assigned by the ISP.
Secondary DNS Address	Enter the second IPv6 DNS server address assigned by the ISP.
(These fields appear when the <b>IPv6 Connection</b> is set to <b>DHCPv6</b> .)	
DNS Setting	Select <b>Obtain DNS Server address Automatically</b> to have the LTE get the IPv6 DNS server addresses from the ISP automatically. Select <b>Use the following DNS address</b> to have the LTE use the IPv6 DNS server addresses you configure manually.

Table 15 Configuration &gt; Network &gt; WAN &gt; IPv6 (continued)

LABEL	DESCRIPTION
Primary DNS Address	Enter the first IPv6 DNS server address assigned by the ISP.
Secondary DNS Address	Enter the second IPv6 DNS server address assigned by the ISP.
(These fields appear when the <b>IPv6 Connection</b> is set to <b>PPPoE</b> .)	
Address Mode	Select <b>Dynamic IP</b> if you have a dynamic IP address. Select <b>Static IP</b> if the ISP assigned a fixed IP address.
IP Address	Enter the static IP address provided by your ISP.
Username	Enter a user name (of up to 31 printable characters) for login using PPPoE connection.
Password	Enter the password associated with the user name above.
Service Name	Enter the name of your PPPoE service here.
Reconnect Mode	Select <b>Auto Reconnect (always-on)</b> if you do not want the connection to time out. Select <b>Connection-on-Demand</b> if you want to connect for a certain amount of time before the router automatically disconnects from the PPPoE server. If you select this you will need to enter the number of minutes in the <b>Maximum Idle Time</b> field. Select <b>Manually</b> if want to make the connection manually.
Maximum Idle Time	Specify the time in minutes that elapses before the LTE automatically disconnects from the PPPoE server.
(These fields appear when the <b>IPv6 Connection</b> is set to <b>6RD</b> .)	
Remote IPv4 Address	Enter the IPv4 address of the relay server,
IPv4 Mask Length	Enter the IPv4 subnet mask number (1 to 32).
Remote Prefix	Enter an IPv6 prefix for tunneling IPv6 traffic to the ISP's Border Relay router and connecting to the native IPv6 Internet.
Prefix Length	Enter the address prefix length to specify how many most significant bits in an IPv6 address compose the network address.
Primary DNS Address	Enter the first IPv6 DNS server address assigned by the ISP.
Secondary DNS Address	Enter the second IPv6 DNS server address assigned by the ISP.
LAN IPv6 Address	Enter the IPv6 address for the LTE LAN interface in this field.
LAN IPv6 Link-Local Address	This shows the IPv6 Link-local address in the LAN side. This is used by LTE when communicating with neighboring devices on the same link. It allows IPv6-capable devices to communicate with each other in the LAN side.i
Auto configuration	Click <b>Enable</b> if you want the devices on your local area network to obtain network address that are not managed by a DHCPv6 server. Otherwise, select <b>Disable</b> .
Auto configuration Type	Select <b>Stateless</b> if you want the LTE interface to automatically generate a link-local address via stateless auto configuration. Select <b>Stateful (DHCPv6)</b> when the devices connected to your LAN needs to have their TCP/IP configuration set to DHCPv6 or obtain an IPv6 address automatically.
IPv6 Address Range (Start)	If you select <b>Stateful (DHCPv6)</b> , specify the range of IPv6 addresses from which the DHCPv6 server assigns to the clients. Enter the smallest value of the last block of the IPv6 addresses which are to be allocated.
IPv6 Address Range (End)	If you select <b>Stateful (DHCPv6)</b> , specify the range of IPv6 addresses from which the DHCPv6 server assigns to the clients. Enter the largest value of the last block of the IPv6 addresses which are to be allocated.
IPv6 Address Lifetime	If you select <b>Stateful (DHCPv6)</b> , specify how long (in minutes) the IPv6 addresses remain valid.

## 7.7 PIN Management

Use this screen to enable PIN authentication and configure the PIN code. Click **Configuration > Network > WAN > PIN Management** from the Configuration menu.

**Figure 27** Configuration > Network > WAN > PIN Management

The following table describes the labels in this screen.

**Table 16** Configuration > Network > WAN > PIN Management

LABEL	DESCRIPTION
PIN Code Request function	Select <b>Enable</b> to turn on PIN code authentication. A PIN (Personal Identification Number) code is a key to a SIM card. Without the PIN code, you cannot use the SIM card. Select <b>Disable</b> to turn off PIN code authentication.
SIM PIN Code	If you select <b>Enable</b> , enter the 4-digit PIN code (0000 for example) provided by your ISP for the inserted SIM card.
Apply	Click <b>Apply</b> to save your changes back to the LTE.
Cancel	Click <b>Cancel</b> to reload the previous configuration for this screen.

# CHAPTER 8

## Wireless LAN

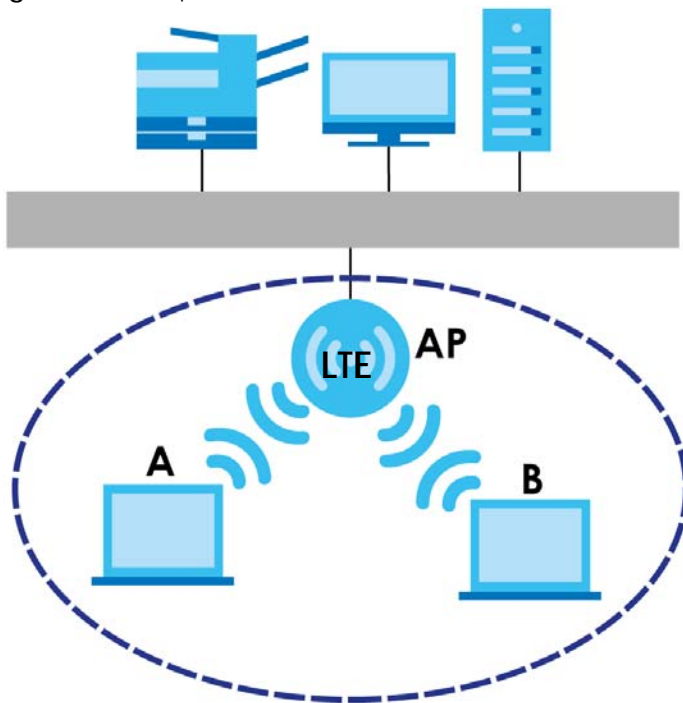
### 8.1 Overview

This chapter discusses how to configure the wireless network settings in your LTE.

See the appendices for more detailed information about wireless networks.

The following figure provides an example of a wireless network.

**Figure 28** Example of a Wireless Network



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

#### 8.1.1 What You Can Do

- Use the **General** screen to turn the wireless connection on or off, set up wireless security between the LTE and the wireless clients, and make other basic configuration changes ([Section 8.2 on page 67](#)).
- Use the **More AP** screen to set up multiple wireless networks on your LTE ([Section 8.4 on page 75](#)).
- Use the **MAC Filter** screen to allow or deny wireless stations based on their MAC addresses from connecting to the LTE ([Section 8.5 on page 77](#)).



- Use the **Advanced** screen to allow intra-BSS networking and set the RTS/CTS Threshold ([Section 8.6 on page 79](#)).
- Use the **QoS** screen to ensure Quality of Service (QoS) in your wireless network ([Section 8.7 on page 80](#)).
- Use the **WPS** screen to quickly set up a wireless network with strong security, without having to configure security settings manually ([Section 8.8 on page 81](#)).
- Use the **WPS Station** screen to add a wireless station using WPS ([Section 8.9 on page 82](#)).
- Use the **Scheduling** screen to set the times your wireless LAN is turned on and off ([Section 8.10 on page 83](#)).
- Use the **WDS** screen to configure the LTE's WDS settings ([Section 8.11 on page 84](#)).

## 8.1.2 What You Should Know

Every wireless network must follow these basic guidelines.

- Every wireless client in the same wireless network must use the same SSID.  
The SSID is the name of the wireless network. It stands for Service Set IDentity.
- If two wireless networks overlap, they should use different channels.  
Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every wireless client 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.

### Wireless Security Overview

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

#### SSID

Normally, the AP acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the AP 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 devices to get the SSID. In addition, unauthorized devices can still see the information that is sent in the wireless network.

#### MAC Address Filter

Every wireless client has a unique identification number, called a MAC address.<sup>1</sup> A MAC address is usually written using twelve hexadecimal characters<sup>2</sup>; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each wireless client, see the appropriate User's Guide or other documentation.

---

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, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

You can use the MAC address filter to tell the AP which wireless clients are allowed or not allowed to use the wireless network. If a wireless client is allowed to use the wireless network, it still has to have the correct settings (SSID, channel, and security). If a wireless client is not allowed to use the wireless network, it does not matter if it has the correct settings.

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

## User Authentication

You can make every user log in to the wireless network before they can use it. This is called user authentication. However, every wireless client in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, there are two typical places to store the user names and passwords for each user.

- In the AP: this feature is called a local user database or a local database.
- In a RADIUS server: this is a server used in businesses more than in homes.

If your AP does not provide a local user database and if you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized 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.


Local user databases also have an additional limitation that is explained in the next section.

## 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 user authentication. (See [page 66](#) for information about this.)

Table 17 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest	No Security	WPA
	WPA-PSK	
	WPA2-PSK	WPA2
Strongest		

For example, if the wireless network has a RADIUS server, you can choose **WPA/WPA2** or **WPA2**. If users do not log in to the wireless network, you can choose **None**, **WPA-PSK**, or **WPA-PSK/WPA2-PSK**.

Usually, you should set up the strongest encryption that every wireless client in the wireless network supports. For example, suppose the AP does not have a local user database, and you do not have a RADIUS server. Therefore, there is no user authentication. Suppose the wireless network has two wireless

clients. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.

Note: It is recommended that wireless networks use **WPA-PSK**, **WPA**, or stronger encryption. IEEE 802.1x and WEP encryption are better than none at all, but it is still possible for unauthorized devices to figure out the original information pretty quickly.

Note: It is not possible to use **WPA-PSK**, **WPA** or stronger encryption with a local user database. In this case, it is better to set up stronger encryption with no authentication than to set up weaker encryption with the local user database.

When you select **WPA2** or **WPA2-PSK** in your LTE, you can also select an option (**WPA/WPA-PSK Compatible**) to support WPA/WPA-PSK as well. In this case, if some wireless clients support WPA and some support WPA2, you should set up **WPA2-PSK** or **WPA2** (depending on the type of wireless network login) and select the **WPA/WPA-PSK Compatible** option in the LTE.

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

## WPS

WiFi Protected Setup (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. Depending on the devices in your network, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (Personal Identification Number) in the devices. Then, they connect and set up a secure network by themselves. See how to set up a secure wireless network using WPS in the [Section 4.2 on page 32](#).

## 8.2 General Wireless LAN Settings

Use this screen to configure the SSID and wireless security of the wireless LAN.

Note: If you are configuring the LTE from a computer connected to the wireless LAN and you change the LTE's SSID, channel 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's new settings.

Click **Configuration > Network > Wireless LAN** to open the **General** screen.

Figure 29 Configuration &gt; Network &gt; Wireless LAN &gt; General

General	More AP	MAC Filter	Advanced	QoS	WPS	WPS Station	Scheduling	WDS	
<b>Wireless Setup - 2.4G</b>									
Wireless LAN Status :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable								
Name (SSID) :	Zyxel_8852								
<input type="checkbox"/> Hide SSID									
Channel Selection :	1	<input checked="" type="checkbox"/> Auto Channel Selection							
Operating Channel :	Channel-1								
Channel Width :	Auto								
802.11 Mode :	802.11b/g/n Mixed								
<b>Security - 2.4G</b>									
Security Mode :	WPA-PSK / WPA2-PSK								
Encryption	AES								
Preshared Key	••••••••							<input type="checkbox"/> Show Password	
Group Key Update Timer	3600							seconds(Range: 60~86400)	
<b>Wireless Setup - 5G</b>									
Wireless LAN Status :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable								
Name (SSID) :	Zyxel_8852_5G								
<input type="checkbox"/> Hide SSID									
Channel Selection :	36	<input checked="" type="checkbox"/> Auto Channel Selection							
Operating Channel :	Channel-116								
Channel Width :	Auto								
802.11 Mode :	802.11 a/n/ac Mixed								
<b>Security - 5G</b>									
Security Mode :	WPA-PSK / WPA2-PSK								
Encryption	AES								
Preshared Key	••••••••							<input type="checkbox"/> Show Password	
Group Key Update Timer	3600							seconds(Range: 60~86400)	
<b>Note:</b> Open and WPA2-PSK can be configured when WPS enabled.									
						Cancel	Apply		

The following table describes the general wireless LAN labels in this screen.

Table 18 Configuration &gt; Network &gt; Wireless LAN &gt; General

LABEL	DESCRIPTION
Wireless Setup - 2.4G / Wireless Setup - 5G	
Wireless LAN Status	Select <b>Enable</b> to activate the 2.4G/5G wireless LAN. Select <b>Disable</b> to turn it off. You can also enable or disable the 2.4G/5G wireless LANs by using the WLAN/WPS button located on the side panel of the LTE.
Name (SSID)	The SSID (Service Set Identity) identifies the Service Set with which a wireless client is associated. Enter a descriptive name (up to 32 printable characters found on a typical English language keyboard) for the wireless LAN.

Table 18 Configuration &gt; Network &gt; Wireless LAN &gt; General (continued)

LABEL	DESCRIPTION
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.
Channel Selection	<p>Set the operating frequency/channel depending on your particular region.</p> <p>Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in.</p> <p>Refer to the Connection Wizard chapter for more information on channels. This option is only available if <b>Auto Channel Selection</b> is disabled.</p>
Auto Channel Selection	Select this check box for the LTE to automatically choose the channel with the least interference. De-select this check box if you wish to manually select the channel using the <b>Channel Selection</b> field.
Operating Channel	This displays the operating frequency/channel depending on your particular region.
Channel Width	<p>Select the wireless channel width used by LTE.</p> <p>A standard 20 MHz channel (<b>HT20</b>) offers transfer speeds of up to 144 Mbps (2.4G) or 217 Mbps (5G) whereas a 40 MHz channel (<b>HT40</b>) uses two standard channels and offers speeds of up to 300 Mbps (2.4G) or 450 Mbps (5G). An IEEE 802.11ac-specific 80 MHz channel (<b>HT80</b>) offers speeds of up to 1.3 Gbps.</p> <p>Because not all devices support 40 MHz and/or 80 MHz channels, select <b>Auto</b> to allow the LTE to adjust the channel bandwidth automatically.</p> <p><b>HT40</b> (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. A <b>HT80</b> channel consists of two adjacent 40 MHz channels. The wireless clients must also support <b>HT40</b> or <b>HT80</b>. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal.</p> <p>Select <b>HT20</b> if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding.</p>
802.11 Mode	<p>In Wireless Setup for 2.4G network you can select from the following:</p> <ul style="list-style-type: none"> <li>• <b>802.11b Only:</b> allows either IEEE 802.11b compliant WLAN devices to associate with the LTE. In this mode, all wireless devices can only transmit at the data rates supported by IEEE 802.11b.</li> <li>• <b>802.11g Only:</b> allows IEEE 802.11g compliant WLAN devices to associate with the Device. IEEE 802.11b compliant WLAN devices can associate with the LTE only when they use the short preamble type.</li> <li>• <b>802.11n Only:</b> allows IEEE 802.11n compliant WLAN devices to associate with the LTE. This can increase transmission rates, although IEEE 802.11b or IEEE 802.11g clients will not be able to connect to the LTE.</li> <li>• <b>802.11b/g Mixed:</b> allows either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the LTE. The LTE adjusts the transmission rate automatically according to the wireless standard supported by the wireless devices.</li> <li>• <b>802.11g/n Mixed:</b> allows either IEEE 802.11g or IEEE 802.11n compliant WLAN devices to associate with the LTE. The transmission rate of your LTE might be reduced.</li> <li>• <b>802.11b/g/n Mixed:</b> allows IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the LTE. The transmission rate of your LTE might be reduced.</li> </ul> <p>In Wireless Setup for 5G network you can select from the following:</p> <ul style="list-style-type: none"> <li>• <b>802.11a Only:</b> allows only IEEE 802.11a compliant WLAN devices to associate with the LTE.</li> <li>• <b>802.11n Only:</b> allows IEEE 802.11n compliant WLAN devices to associate with the LTE. This can increase transmission rates, although IEEE 802.11a clients will not be able to connect to the LTE.</li> <li>• <b>802.11a/n Mixed:</b> allows both IEEE802.11n and IEEE802.11a compliant WLAN devices to associate with the LTE. The transmission rate of your LTE might be reduced.</li> <li>• <b>802.11a/n/ac Mixed:</b> allows both IEEE802.11a, IEEE802.11n and IEEE802.11ac compliant WLAN devices to associate with the LTE. The transmission rate of your LTE might be reduced.</li> </ul>
Security - 2.4G / Security - 5G	

Table 18 Configuration &gt; Network &gt; Wireless LAN &gt; General (continued)

LABEL	DESCRIPTION
Security Mode	<p>Select <b>WPA2-PSK</b>, <b>WPA2</b>, <b>WPA/WPA2</b>, <b>WPA-PSK/WPA2-PSK</b> to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as this device. After you select to use a security, additional options appears in this screen. See <a href="#">Section 8.3 on page 70</a> for detailed information on different security modes. Or you can select <b>Open</b> to allow any client to associate this network without authentication.</p> <p>Note: If the WPS function is enabled (default), only <b>Open</b> and <b>WPA2-PSK</b> are available in this field.</p>
Apply	Click <b>Apply</b> to save your changes back to the LTE.
Cancel	Click <b>Cancel</b> to reload the previous configuration for this screen.

See the rest of this chapter for information on the other labels in this screen.

## 8.3 Wireless Security

The screen varies depending on what you select in the **Security Mode** field.

### 8.3.1 No Security

Select **Open** to allow wireless clients to communicate with the access points without any data encryption.

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

Figure 30 Configuration &gt; Network &gt; Wireless LAN &gt; General: No Security

The screenshot displays the configuration page for the Wireless LAN, divided into sections for 2.4G and 5G. The 2.4G section includes settings for Wireless LAN Status (Enabled), Name (SSID) (Zyxel\_8852), Hide SSID (unchecked), Channel Selection (1), Auto Channel Selection (checked), Operating Channel (Channel-1), Channel Width (Auto), and 802.11 Mode (802.11b/g/n Mixed). The Security - 2.4G section shows Security Mode set to Open and Encryption set to None. The 5G section includes settings for Wireless LAN Status (Enabled), Name (SSID) (Zyxel\_8852\_5G), Hide SSID (unchecked), Channel Selection (36), Auto Channel Selection (checked), Operating Channel (Channel-116), Channel Width (Auto), and 802.11 Mode (802.11 a/n/ac Mixed). The Security - 5G section shows Security Mode set to Open and Encryption set to None. A note at the bottom states: "Note: Open and WPA2-PSK can be configured when WPS enabled." Buttons for Cancel and Apply are located at the bottom right.

Section	Property	Value
Wireless Setup - 2.4G	Wireless LAN Status	Enable
	Name (SSID)	Zyxel_8852
	Hide SSID	<input type="checkbox"/>
	Channel Selection	1
	Auto Channel Selection	<input checked="" type="checkbox"/>
	Operating Channel	Channel-1
	Channel Width	Auto
	802.11 Mode	802.11b/g/n Mixed
Security - 2.4G	Security Mode	Open
	Encryption	None
Wireless Setup - 5G	Wireless LAN Status	Enable
	Name (SSID)	Zyxel_8852_5G
	Hide SSID	<input type="checkbox"/>
	Channel Selection	36
	Auto Channel Selection	<input checked="" type="checkbox"/>
	Operating Channel	Channel-116
	Channel Width	Auto
	802.11 Mode	802.11 a/n/ac Mixed
Security - 5G	Security Mode	Open
	Encryption	None

Note: Open and WPA2-PSK can be configured when WPS enabled.

Buttons: Cancel, Apply

### 8.3.2 WPA2-PSK

Select WPA2-PSK from the Security Mode list.

Figure 31 Network &gt; Wireless LAN &gt; General: WPA2-PSK

**General** More AP MAC Filter Advanced QoS WPS WPS Station Scheduling WDS

**Wireless Setup - 2.4G**

Wireless LAN Status :  Enable  Disable

Name (SSID) : Zyxel\_8852

Hide SSID

Channel Selection : 1  Auto Channel Selection

Operating Channel : Channel-1

Channel Width : Auto

802.11 Mode : 802.11b/g/n Mixed

**Security - 2.4G**

Security Mode : WPA2-PSK

Encryption : AES

Pre-shared Key : .....  Show Password

Group Key Update Timer : 3600 seconds(Range: 60-86400)

**Wireless Setup - 5G**

Wireless LAN Status :  Enable  Disable

Name (SSID) : Zyxel\_8852\_5G

Hide SSID

Channel Selection : 36  Auto Channel Selection

Operating Channel : Channel-116

Channel Width : Auto

802.11 Mode : 802.11 a/n/ac Mixed

**Security - 5G**

Security Mode : WPA2-PSK

Encryption : AES

Pre-shared Key : .....  Show Password

Group Key Update Timer : 3600 seconds(Range: 60-86400)

**Note:** Open and WPA2-PSK can be configured when WPS enabled.

Cancel Apply

The following table describes the labels in this screen.

Table 19 Network &gt; Wireless LAN &gt; General: WPA2-PSK

LABEL	DESCRIPTION
Security Mode	Select <b>WPA2-PSK</b> to enable data encryption.
Encryption	Select the encryption type of data encryption. Select <b>AES</b> if your wireless clients can all use <b>AES</b> . Select <b>TKIP / AES</b> to allow the wireless clients to use either <b>TKIP</b> or <b>AES</b> .
Pre-Shared Key	<b>WPA2-PSK</b> uses a simple common password for authentication. Type a pre-shared key from 8 to 63 case-sensitive keyboard characters.
Group Key Update Timer	The <b>Group Key Update Timer</b> is the rate at which the AP sends a new group key out to all clients. The default is <b>3600</b> seconds (60 minutes).



Table 19 Network &gt; Wireless LAN &gt; General: WPA2-PSK (continued)

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your changes back to the LTE.
Cancel	Click <b>Cancel</b> to reload the previous configuration for this screen.

### 8.3.3 WPA/WPA2

Select **WPA** or **WPA2** from the **Security Mode** list.

Note: WPA or WPA2 is not available if you enable WPS before you configure WPA or WPA2 in the **Wireless LAN > General** screen.

Figure 32 Configuration &gt; Network &gt; Wireless LAN &gt; General: WPA / WPA2

The screenshot shows the configuration page for Wireless LAN. It has tabs for General, More AP, MAC Filter, Advanced, QoS, WPS, WPS Station, Scheduling, and WDS. The 'General' tab is active.

**Wireless Setup - 2.4G**

- Wireless LAN Status:  Enable  Disable
- Name (SSID): Zyxel\_8852
- Hide SSID
- Channel Selection: 1  Auto Channel Selection
- Operating Channel: Channel-1
- Channel Width: Auto
- 802.11 Mode: 802.11b/g/n Mixed

**Security - 2.4G** (highlighted in red)

- Security Mode: WPA / WPA2
- RADIUS Server
- RADIUS Server IP: 0.0.0.0
- RADIUS Server Port: 1812
- RADIUS Shared Key:   Show Password
- Encryption: AES
- Group Key Update Timer: 3600 seconds (Range: 60~86400)

**Wireless Setup - 5G**

- Wireless LAN Status:  Enable  Disable
- Name (SSID): Zyxel\_8852\_5G
- Hide SSID
- Channel Selection: 36  Auto Channel Selection
- Operating Channel: Channel-116
- Channel Width: Auto
- 802.11 Mode: 802.11 a/n/ac Mixed

**Security - 5G** (highlighted in red)

- Security Mode: WPA / WPA2
- RADIUS Server
- RADIUS Server IP: 0.0.0.0
- RADIUS Server Port: 1812
- RADIUS Shared Key:   Show Password
- Encryption: AES
- Group Key Update Timer: 3600 seconds (Range: 60~86400)

**Note:** Open and WPA2-PSK can be configured when WPS enabled.

Buttons: Cancel, Apply

The following table describes the labels in this screen.

Table 20 Configuration &gt; Network &gt; Wireless LAN &gt; General: WPA / WPA2

LABEL	DESCRIPTION
Security Mode	Select <b>WPA</b> or <b>WPA2</b> to enable data encryption.
RADIUS Server	
RADIUS Server IP	Enter the IP address of the RADIUS server to be used for authentication.
RADIUS Server Port	Enter the port number of the RADIUS server to be used for authentication.
RADIUS Shared Key	Enter the shared secret password of the RADIUS server to be used for authentication.

Table 20 Configuration &gt; Network &gt; Wireless LAN &gt; General: WPA / WPA2 (continued)

LABEL	DESCRIPTION
Encryption	Select the encryption type of data encryption. Select <b>AES</b> if your wireless clients can all use <b>AES</b> . Select <b>TKIP / AES</b> to allow the wireless clients to use either <b>TKIP</b> or <b>AES</b> .
Group Key Update Time	The WPA Group Key Update Timer is the rate at which the AP (if using WPA-PSK key management) or RADIUS server (if using WPA key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the WPA Group Key Update Timer is also supported in WPA-PSK mode. The default setting is 3600 seconds (60 minutes).
Apply	Click <b>Apply</b> to save your changes back to the LTE.
Cancel	Click <b>Cancel</b> to reload the previous configuration for this screen.

## 8.4 More AP

This screen allows you to enable and configure multiple wireless networks and guest wireless network settings on the LTE.

You can configure up to four SSIDs to enable multiple BSSs (Basic Service Sets) on the LTE. This allows you to use one access point to provide several BSSs simultaneously. You can then assign varying security types to different SSIDs. Wireless clients can use different SSIDs to associate with the same access point.

Click **Configuration > Network > Wireless LAN > More AP**. The following screen displays.

Figure 33 Configuration &gt; Network &gt; Wireless LAN &gt; More AP

General	More AP	MAC Filter	Advanced	QoS	WPS	WPS Station	Scheduling	WDS
<b>More AP Setup - 2.4G</b>								
#	Status	SSID	Security	Edit				
1		ZyxeL_SSID1	WPA2-PSK					
2		ZyxeL_SSID2	WPA2-PSK					
3		ZyxeL_SSID3	WPA2-PSK					
<b>More AP Setup - 5G</b>								
#	Status	SSID	Security	Edit				
1		ZyxeL_SSID1_5G	WPA2-PSK					
2		ZyxeL_SSID2_5G	WPA2-PSK					
3		ZyxeL_SSID3_5G	WPA2-PSK					

The following table describes the labels in this screen.

Table 21 Configuration &gt; Network &gt; Wireless LAN &gt; More AP

LABEL	DESCRIPTION
#	This is the index number of each SSID profile.
Status	This shows whether the SSID profile is active (a yellow bulb) or not (a gray bulb).

Table 21 Configuration &gt; Network &gt; Wireless LAN &gt; More AP (continued)

LABEL	DESCRIPTION
SSID	An SSID profile is the set of parameters relating to one of the LTE'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.
Edit	Click the <b>Edit</b> icon to configure the SSID profile.

## 8.4.1 More AP Edit

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 34 Configuration &gt; Network &gt; Wireless LAN &gt; More AP: Edit

The following table describes the labels in this screen.

Table 22 Configuration &gt; Network &gt; Wireless LAN &gt; More AP: Edit

LABEL	DESCRIPTION
Active	Select this to activate the SSID profile.
Name (SSID)	The SSID (Service Set IDentity) identifies the Service Set with which a wireless client is associated. Enter a descriptive name (up to 32 printable characters found on a typical English language keyboard) 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.

Table 22 Configuration &gt; Network &gt; Wireless LAN &gt; More AP: Edit (continued)

LABEL	DESCRIPTION
Intra-BSS Traffic	<p>A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).</p> <p>Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless clients can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless clients can still access the wired network but cannot communicate with each other.</p>
WMM QoS	<p>Check this to have the LTE automatically give a service a priority level according to the ToS value in the IP header of packets it sends.</p> <p>WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly.</p>
Security Mode	<p>Select <b>WPA2-PSK</b>, <b>WPA/WPA2</b> to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as this device. After you select to use a security, additional options appears in this screen. See <a href="#">Section 8.3 on page 70</a> for detailed information on different security modes. Or you can select <b>Open</b> to allow any client to associate this network without authentication.</p> <p>Note: If the WPS function is enabled (default), only <b>Open</b> and <b>WPA2-PSK</b> are available in this field.</p>
Encryption	<p>Select the encryption type of data encryption.</p> <p>Select <b>AES</b> if your wireless clients can all use <b>AES</b>.</p> <p>Select <b>TKIP / AES</b> to allow the wireless clients to use either <b>TKIP</b> or <b>AES</b>.</p>
Pre-Shared Key	Type a password the wireless stations need to enter to connect to the wireless network.
Group Key Update Timer	The WPA Group Key Update Timer is the rate at which the AP (if using WPA-PSK key management) or RADIUS server (if using WPA key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the WPA Group Key Update Timer is also supported in WPA-PSK mode. The default setting is 3600 seconds (60 minutes).
Cancel	Click <b>Cancel</b> to reload the previous configuration for this screen.
Apply	Click <b>Apply</b> to save your changes back to the LTE.

## 8.5 MAC Filter

The MAC filter screen allows you to configure the LTE to give exclusive access to devices (**Allow**) or exclude devices from accessing the LTE (**Deny**). 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.

To change your LTE's MAC filter settings, click **Configuration > Network > Wireless LAN > MAC Filter**. The screen appears as shown.

**Figure 35** Configuration > Network > Wireless LAN > MAC Filter

General More AP **MAC Filter** Advanced QoS WPS WPS Station Scheduling WDS

MAC Address Filter :  Enable  Disable

Filter Action :  Allow  Deny

**MAC Filter Summary**

Set	MAC Address	Set	MAC Address
1		17	
2		18	
3		19	
4		20	
5		21	
6		22	
7		23	
8		24	
9		25	
10		26	
11		27	
12		28	
13		29	
14		30	
15		31	
16		32	

Cancel Apply

The following table describes the labels in this menu.

**Table 23** Configuration > Network > Wireless LAN > MAC Filter

LABEL	DESCRIPTION
MAC Address Filter	Select to turn on ( <b>Enable</b> ) or off ( <b>Disable</b> ) MAC address filtering.
Filter Action	Define the filter action for the list of MAC addresses in the <b>MAC Filter Summary</b> table. Select <b>Allow</b> to permit access to the LTE, MAC addresses not listed will be denied access to the LTE. Select <b>Deny</b> to block access to the LTE, MAC addresses not listed will be allowed to access the LTE.
MAC Filter Summary	
Set	This is the index number of the MAC address.
MAC Address	Enter the MAC address of the wireless station that are allowed or denied access to the LTE.
Apply	Click <b>Apply</b> to save your changes back to the LTE.
Cancel	Click <b>Cancel</b> to reload the previous configuration for this screen.

## 8.6 Wireless LAN Advanced Settings

Use this screen to allow wireless advanced features, such as the output power, RTS/CTS Threshold settings.

Click **Configuration > Network > Wireless LAN > Advanced**. The screen appears as shown.

**Figure 36** Configuration > Network > Wireless LAN > Advanced

The screenshot shows the 'Advanced' tab of the Wireless LAN configuration. It is split into two frequency bands: 2.4G and 5G. For each band, the following settings are visible:

- RTS/CTS Threshold:** Input field with value 2347 and range (1~2347).
- Fragmentation Threshold:** Input field with value 2346 and range (256 ~ 2346).
- Intra-BSS Traffic:** Radio buttons for 'Enable' (selected) and 'Disable'.
- Green AP:** Radio buttons for 'Enable' and 'Disable' (selected).
- Tx Power:** Dropdown menu set to 100%.
- Beacon Interval:** Input field with value 100 and range (msec, 100~1000).

At the bottom right, there are 'Cancel' and 'Apply' buttons.

The following table describes the labels in this screen.

**Table 24** Configuration > Network > Wireless LAN > Advanced

LABEL	DESCRIPTION
Wireless Advanced Setup - 2.4G / Wireless Advanced Setup - 5G	
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/ CTS (Clear To Send) handshake.  This field is not configurable and the LTE automatically changes to use the maximum value if you select 802.11n, 802.11gn or 802.11bgn in the <b>Wireless LAN &gt; General</b> screen.
Fragmentation Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent.  This field is not configurable and the LTE automatically changes to use the maximum value if you select <b>802.11n, 802.11gn or 802.11bgn</b> in the <b>Wireless LAN &gt; General</b> screen.
Intra-BSS Traffic	A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).  Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless clients can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless clients can still access the wired network but cannot communicate with each other.

Table 24 Configuration &gt; Network &gt; Wireless LAN &gt; Advanced (continued)

LABEL	DESCRIPTION
Green AP	Select <b>Enable</b> to reduce the power consumption by adjusting the output power. The LTE reduces the output power of the transmitter from about 260mA to 188mA when there is no IEEE 802.11 wireless clients associated with the LTE wireless network.
Tx Power	Set the output power of the LTE in this field. If there is a high density of APs in an area, decrease the output power of the LTE to reduce interference with other APs. Select one of the following <b>100%, 90%, 75%, 50%, 25%</b> or <b>10%</b> .
Beacon Interval	When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low-power mode before waking up to handle the beacon. A high value helps save current consumption of the access point.
Apply	Click <b>Apply</b> to save your changes back to the LTE.
Cancel	Click <b>Cancel</b> to reload the previous configuration for this screen.

## 8.7 Quality of Service (QoS)

The QoS screen allows you to automatically give a service (such as VoIP and video) a priority level.

Click **Configuration > Network > Wireless LAN > QoS**. The following screen appears.

Figure 37 Configuration &gt; Network &gt; Wireless LAN &gt; QoS

The screenshot shows the QoS configuration screen with the following content:

- General | More AP | MAC Filter | Advanced | **QoS** | WPS | WPS Station | Scheduling | WDS
- WMM QoS(2.4G) :  Enable  Disable
- WMM QoS(5G) :  Enable  Disable
- Buttons: Cancel, Apply

The following table describes the labels in this screen.

Table 25 Configuration &gt; Network &gt; Wireless LAN &gt; QoS

LABEL	DESCRIPTION
WMM QoS (2.4G)	Select <b>Enable</b> to have the LTE automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly.  This field is not configurable and the LTE automatically enables WMM QoS if you select <b>802.11n, 802.11g/n Mixed, or 802.11b/g/n Mixed</b> in the <b>Wireless LAN &gt; General</b> screen.
WMM QoS (5G)	Select <b>Enable</b> to have the LTE automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly.  This field is not configurable and the LTE automatically enables WMM QoS if you select <b>802.11n, 802.11a/n Mixed, or 802.11a/n/ac Mixed</b> in the <b>Wireless LAN &gt; General</b> screen.
Apply	Click <b>Apply</b> to save your changes to the LTE.
Cancel	Click <b>Cancel</b> to reload the previous configuration for this screen.



## 8.8 WPS

Use this screen to enable/disable WPS, view or generate a new PIN number and check current WPS status. To open this screen, click **Configuration > Network > Wireless LAN > WPS**.

Note: With WPS, wireless clients can only connect to the wireless network using the first SSID on the LTE.

**Figure 38** Configuration > Network > Wireless LAN > WPS

The screenshot shows the WPS configuration interface with the following sections:

- WPS Setup - 2.4G:**
  - WPS:  Enable  Disable
  - PIN Code:  Enable  Disable
  - PIN Number: 25908022
  - Generate button
- WPS Status - 2.4G:**
  - Status: CONFIGURED (Release Configuration button)
  - 802.11 Mode: 802.11b/g/n Mixed
  - SSID: ZyxeL\_8852
  - Security: WPA2-PSK
- WPS Setup - 5G:**
  - WPS:  Enable  Disable
  - PIN Code:  Enable  Disable
  - PIN Number: 25908039
  - Generate button
- WPS Status - 5G:**
  - Status: CONFIGURED (Release Configuration button)
  - 802.11 Mode: 802.11a/n/ac Mixed
  - SSID: ZyxeL\_8852\_5G
  - Security: WPA2-PSK

**Note:** The WPS enabled, the UPnP service will be turned on automatically.

Buttons: Cancel, Apply

The following table describes the labels in this screen.

**Table 26** Configuration > Network > Wireless LAN > WPS

LABEL	DESCRIPTION
WPS Setup 2.4G / 5G	
WPS	Select <b>Enable</b> to turn on the WPS feature. Otherwise, select <b>Disable</b> .
PIN Code	Select <b>Enable</b> so the LTE can connect by WPS using the PIN Configuration Method. Select <b>Disable</b> so it can only connect by WPS using the Push Button Method.

Table 26 Configuration &gt; Network &gt; Wireless LAN &gt; WPS (continued)

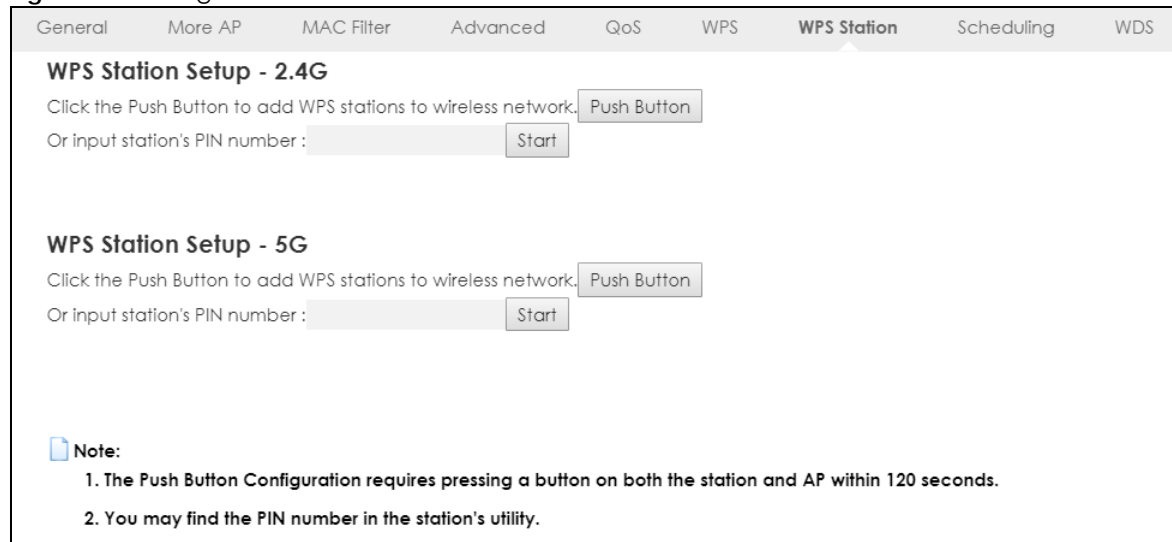
LABEL	DESCRIPTION
PIN Number	This is the WPS PIN (Personal Identification Number) of the LTE. Enter this PIN in the configuration utility of the device you want to connect to the LTE using WPS.  The PIN is not necessary when you use WPS push-button method.  Click <b>Generate</b> to generate a new PIN number.
WPS Status - 2.4G / WPS Status - 5G	
Status	This displays <b>Configured</b> when the LTE has configured wireless security settings.
802.11 Mode	This is the 802.11 mode used. Only compliant WLAN devices can associate with the LTE.
SSID	This is the name of the wireless network (the LTE's first SSID).
Security	This is the type of wireless security employed by the network.
Release Configuration	Click this button to remove all configured wireless and wireless security settings for WPS connections on the LTE.
Cancel	Click <b>Cancel</b> to reload the previous configuration for this screen.
Apply	Click <b>Apply</b> to save your changes back to the LTE.

## 8.9 WPS Station

Use this screen when you want to add a wireless station using WPS. To open this screen, click **Configuration > Network > Wireless LAN > WPS Station** tab.

Note: After you click **Push Button** on this screen, you have to press a similar button in the wireless station utility within 2 minutes. To add the second wireless station, you have to press these buttons on both device and the wireless station again after the first 2 minutes.

Figure 39 Configuration &gt; Network &gt; Wireless LAN &gt; WPS Station



The following table describes the labels in this screen.

Table 27 Configuration > Network > Wireless LAN > WPS Station

LABEL	DESCRIPTION
WPS Station Setup - 2.4G / WPS Station Setup - 5G	
Push Button	Use this button when you use the PBC (Push Button Configuration) method to configure wireless station's wireless settings.  Click this to start WPS-aware wireless station scanning and the wireless security information synchronization.
Or input station's PIN number	Use this button when you use the PIN Configuration method to configure wireless station's wireless settings.  Type the same PIN number generated in the wireless station's utility. Then click <b>Start</b> to associate to each other and perform the wireless security information synchronization.

## 8.10 Scheduling

Use this screen to set the times your wireless LAN is turned on and off. Wireless LAN scheduling is disabled by default. The wireless LAN can be scheduled to turn on or off on certain days and at certain times. To open this screen, click **Configuration > Network > Wireless LAN > Scheduling** tab.

Figure 40 Configuration > Network > Wireless LAN > Scheduling

General More AP MAC Filter Advanced QoS WPS WPS Station **Scheduling** WDS

Wireless LAN Scheduling :  Enable  Disable

Policy :  On  Off

Scheduling

Day

Day	For the following times (24-Hour Format)												
<input type="checkbox"/> EveryDay	00	▼	(hour)	00	▼	(min)	~	00	▼	(hour)	00	▼	(min)
<input type="checkbox"/> Mon	00	▼	(hour)	00	▼	(min)	~	00	▼	(hour)	00	▼	(min)
<input type="checkbox"/> Tue	00	▼	(hour)	00	▼	(min)	~	00	▼	(hour)	00	▼	(min)
<input type="checkbox"/> Wed	00	▼	(hour)	00	▼	(min)	~	00	▼	(hour)	00	▼	(min)
<input type="checkbox"/> Thu	00	▼	(hour)	00	▼	(min)	~	00	▼	(hour)	00	▼	(min)
<input type="checkbox"/> Fri	00	▼	(hour)	00	▼	(min)	~	00	▼	(hour)	00	▼	(min)
<input type="checkbox"/> Sat	00	▼	(hour)	00	▼	(min)	~	00	▼	(hour)	00	▼	(min)
<input type="checkbox"/> Sun	00	▼	(hour)	00	▼	(min)	~	00	▼	(hour)	00	▼	(min)

**Note:**  
Specify the same begin time and end time means the whole day schedule.

Cancel Apply

The following table describes the labels in this screen.

Table 28 Configuration > Network > Wireless LAN > Scheduling

LABEL	DESCRIPTION
Wireless LAN Scheduling	Select <b>Enable</b> to activate the wireless LAN scheduling feature. Select <b>Disable</b> to turn it off.
Policy	Select <b>On</b> or <b>Off</b> to specify whether the wireless LAN is turned on or off. This field works in conjunction with the <b>Day</b> and <b>For the following times</b> fields.

Table 28 Configuration &gt; Network &gt; Wireless LAN &gt; Scheduling (continued)

LABEL	DESCRIPTION
Scheduling	
Day	Select <b>Everyday</b> or the specific days to turn the wireless LAN on or off. If you select <b>Everyday</b> you cannot select any specific days. This field works in conjunction with the <b>For the following times</b> field.
For the following times (24-Hour Format)	Select a begin time using the first set of <b>hour</b> and minute ( <b>min</b> ) drop down boxes and select an end time using the second set of <b>hour</b> and minute ( <b>min</b> ) drop down boxes. If you have chosen <b>On</b> earlier for the WLAN Status the wireless LAN will turn on between the two times you enter in these fields. If you have chosen <b>Off</b> earlier for the WLAN Status the wireless LAN will turn off between the two times you enter in these fields.
Cancel	Click <b>Cancel</b> to reload the previous configuration for this screen.
Apply	Click <b>Apply</b> to save your changes back to the LTE.

## 8.11 WDS

A Wireless Distribution System (WDS) is a wireless connection between two or more APs. Use this screen to configure the LTE's WDS settings. To open this screen, click **Configuration > Network > Wireless LAN > WDS** tab.

Figure 41 Configuration &gt; Network &gt; Wireless LAN &gt; WDS

The following table describes the labels in this screen.

Table 29 Configuration &gt; Network &gt; Wireless LAN &gt; WDS

LABEL	DESCRIPTION
WDS Setup - 2.4G / WDS Setup - 5G	
Basic Setting	Select <b>Disable</b> to turn off the WDS function on the LTE. Select <b>AP+Bridge</b> to have the LTE function as a bridge and access point simultaneously. Select <b>Bridge Only</b> to have the LTE act as a wireless bridge only.
Local MAC Address	This shows the MAC address of the LTE.
Remote MAC Address	Type the MAC address of the peer device in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.

Table 29 Configuration > Network > Wireless LAN > WDS (continued)

LABEL	DESCRIPTION
Cancel	Click <b>Cancel</b> to reload the previous configuration for this screen.
Apply	Click <b>Apply</b> to save your changes back to the LTE.

# CHAPTER 9

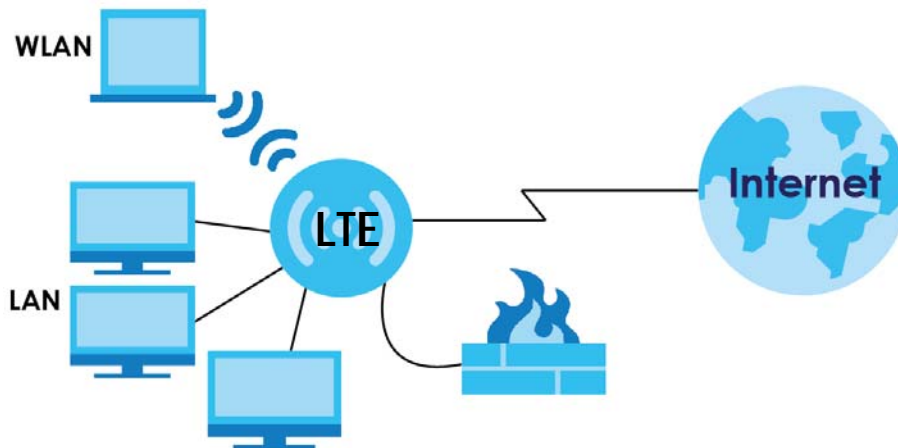
# LAN

## 9.1 Overview

This chapter describes how to configure LAN settings.

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building.

Figure 42 LAN Example



The LAN screens can help you configure a manage IP address, and partition your physical network into logical networks.

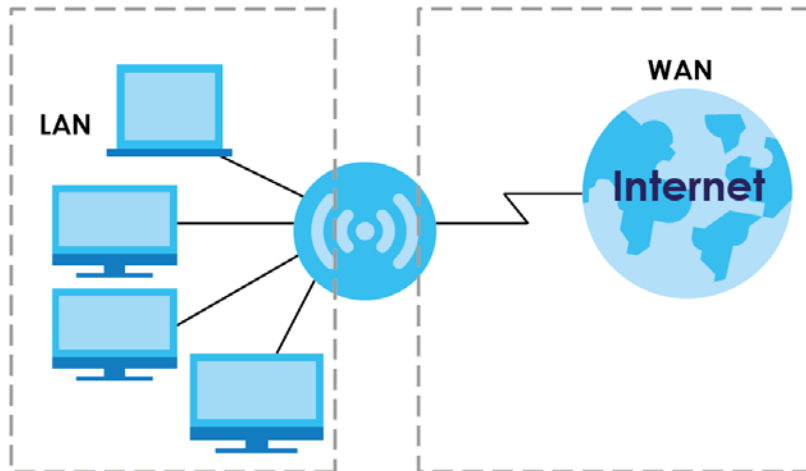
## 9.2 What You Can Do

Use the **IP** screen to change the IP address for your LTE ([Section 9.4 on page 87](#)).

## 9.3 What You Need To Know

The actual physical connection determines whether the LTE ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 43 LAN and WAN IP Addresses



The LAN parameters of the LTE are preset in the factory with the following values:

- IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits).
- DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), read the embedded Web Configurator help regarding what fields need to be configured.

## 9.4 LAN IP

Use this screen to change the IP address for your LTE. Click **Configuration > Network > LAN > IP**.

Figure 44 Configuration &gt; Network &gt; LAN &gt; IP

The following table describes the labels in this screen.

Table 30 Configuration &gt; Network &gt; LAN &gt; IP

LABEL	DESCRIPTION
IP Address	Type the IP address of your LTE in dotted decimal notation.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your LTE will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the LTE.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Apply	Click <b>Apply</b> to save your changes back to the LTE.

# CHAPTER 10

## DHCP Server

### 10.1 Overview

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the LTE's LAN as a DHCP server or disable it. When configured as a server, the LTE provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

#### 10.1.1 What You Can Do

- Use the **General** screen to enable the DHCP server ([Section 10.2 on page 88](#)).
- Use the **Advanced** screen to assign IP addresses on the LAN to specific individual computers based on their MAC addresses ([Section 10.3 on page 90](#)).
- Use the **Client List** screen to view the current DHCP client information ([Section 10.4 on page 92](#)).

#### 10.1.2 What You Need To Know

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

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

##### IP Pool Setup

The LTE is pre-configured with a pool of 32 IP addresses starting from 192.168.1.33 to 192.168.1.64. This configuration leaves 31 IP addresses (excluding the LTE itself) in the lower range (192.168.1.2 to 192.168.1.32) for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

### 10.2 DHCP Server General Settings

The LTE has built-in DHCP server capability that assigns IP addresses to systems that support DHCP client capability. Use this screen to enable the DHCP server. Click **Configuration > Network > DHCP Server**. The following screen displays.



Figure 45 Configuration &gt; Network &gt; DHCP Server &gt; General

**General**    Advanced    Client List

**DHCP 1 Server:**

DHCP Server :  Enable     Disable

IP Pool Starting Address : 192.168.1.33

Pool Size : 32

DHCP Relay

DHCP Server IP : \_\_\_\_\_

Lease Time : 86400 \_\_\_\_\_ seconds

**VLAN DHCP 2 Server:**

DHCP Server :  Enable     Disable

DHCP Server IP Address : 192.168.2.1

IP Pool Starting Address : 192.168.2.33

Pool Size : 32

First DNS Server: DNS Relay ▼ \_\_\_\_\_

Second DNS Server: DNS Relay ▼ \_\_\_\_\_

**VLAN DHCP 3 Server:**

DHCP Server :  Enable     Disable

DHCP Server IP Address : 192.168.3.1

IP Pool Starting Address : 192.168.3.33

Pool Size : 32

First DNS Server: DNS Relay ▼ \_\_\_\_\_

Second DNS Server: DNS Relay ▼ \_\_\_\_\_

**VLAN DHCP 4 Server:**

DHCP Server :  Enable     Disable

DHCP Server IP Address : 192.168.4.1

IP Pool Starting Address : 192.168.4.33

Pool Size : 32

First DNS Server: DNS Relay ▼ \_\_\_\_\_

Second DNS Server: DNS Relay ▼ \_\_\_\_\_

Cancel    Apply

The following table describes the labels in this screen.

Table 31 Configuration &gt; Network &gt; DHCP Server &gt; General

LABEL	DESCRIPTION
DHCP Server	Select <b>Enable</b> to activate DHCP for LAN.  DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. Enable the DHCP server unless your ISP instructs you to do otherwise. Select <b>Disable</b> to stop the LTE acting as a DHCP server. When configured as a server, the LTE provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computers must be manually configured. When set as a server, fill in the following four fields.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool for LAN.
Pool Size	This field specifies the size, or count of the IP address pool for LAN.

Table 31 Configuration &gt; Network &gt; DHCP Server &gt; General (continued)

LABEL	DESCRIPTION
DHCP Relay	Select this option to have the LTE forward DHCP requests to the DHCP server.
DHCP Server IP	This field is configurable only when you select <b>DHCP Relay</b> . Enter the IP address of the actual remote DHCP server in this field.
Lease Time	This is the period of time DHCP-assigned addresses is used. DHCP automatically assigns IP addresses to clients when they log in. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses, for a period of time, which means that past addresses are "recycled" and made available for future reassignment to other systems.
VLAN DHCP x Server This section is configurable only when you create a corresponding VLAN group in the <b>Interface Group</b> screen.	
DHCP Server	Select <b>Enable</b> to activate DHCP for the VLAN group.
DHCP Server IP Address	Enter the LAN IP address you want to assign to your LTE in this VLAN group.
IP Pool Starting Address	Specify the first of the contiguous addresses in the IP address pool for LAN.
Pool Size	Specify the size, or count of the IP address pool for LAN.
First DNS Server Second DNS Server	Specify the IP addresses up to two DNS servers for the DHCP clients to use.  Select <b>Obtained From ISP</b> if your ISP dynamically assigns DNS server information (and the LTE's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.  Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right.  Select <b>DNS Relay</b> to have the LTE act as a DNS proxy. The LTE's LAN IP address displays in the field to the right (read-only). The LTE tells the DHCP clients on the LAN that the LTE itself is the DNS server. When a computer on the LAN sends a DNS query to the LTE, the LTE forwards the query to the LTE's system DNS server (configured in the <b>WAN</b> screen) and relays the response back to the computer.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Apply	Click <b>Apply</b> to save your changes back to the LTE.

## 10.3 Advanced DHCP Server Setting

This screen allows you to assign IP addresses on the LAN to specific individual computers based on their MAC addresses. You can also use this screen to configure the DNS server information that the LTE sends to the DHCP clients.

To change your LTE's static DHCP settings, click **Configuration > Network > DHCP Server > Advanced**. The following screen displays.

**Figure 46** Configuration > Network > DHCP Server > Advanced

The following table describes the labels in this screen.

**Table 32** Configuration > Network > DHCP Server > Advanced

LABEL	DESCRIPTION
Static DHCP Table	
#	This is the index number of the static IP table entry (row).
MAC Address	Type the MAC address (with colons) of a computer on your LAN.
IP Address	Type the LAN IP address of a computer on your LAN.
DNS Server	
DNS Servers Assigned by DHCP Server	The LTE passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. The LTE only passes this information to the LAN DHCP clients when you enable <b>DHCP Server</b> in the <b>General</b> screen. When you disable <b>DHCP Server</b> , DHCP service is disabled and you must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured.
First DNS Server Second DNS Server	Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right.  Select <b>DNS Relay</b> to have the LTE act as a DNS proxy. The LTE's LAN IP address displays in the field to the right (read-only). The LTE tells the DHCP clients on the LAN that the LTE itself is the DNS server. When a computer on the LAN sends a DNS query to the LTE, the LTE forwards the query to the LTE's system DNS server (configured in the <b>WAN</b> screen) and relays the response back to the computer.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Apply	Click <b>Apply</b> to save your changes back to the LTE.

## 10.4 DHCP Client List

The DHCP table shows current DHCP client information (including IP address, Host Name and MAC address) of network clients using the LTE's DHCP servers.

Configure this screen to always assign an IP address to a MAC address (and host name). Click **Configuration > Network > DHCP Server > Client List**.

Note: You can also view a read-only client list by clicking **Monitor > DHCP Server**.

**Figure 47** Configuration > Network > DHCP Server > Client List

#	Status	Host Name	IP Address	MAC Address	Reserve
1			192.168.1.9	00:E0:4C:68:02:18	<input type="checkbox"/>

The following table describes the labels in this screen.

**Table 33** Configuration > Network > DHCP Server > Client List

LABEL	DESCRIPTION
#	This is the index number of the host computer.
Status	This field displays whether the connection to the host computer is up (a yellow bulb) or down (a gray bulb).
Host Name	This field displays the computer host name.
IP Address	This field displays the IP address relative to the # field listed above.
MAC Address	This field shows the MAC address of the computer with the name in the <b>Host Name</b> field. Every Ethernet device has a unique MAC (Media Access Control) address which uniquely identifies a device. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Reserve	Select this if you want to reserve the IP address for this specific MAC address.
Cancel	Click <b>Cancel</b> to reload the previous configuration for this screen.
Apply	Click <b>Apply</b> to save your changes back to the LTE.

# CHAPTER 11

## NAT

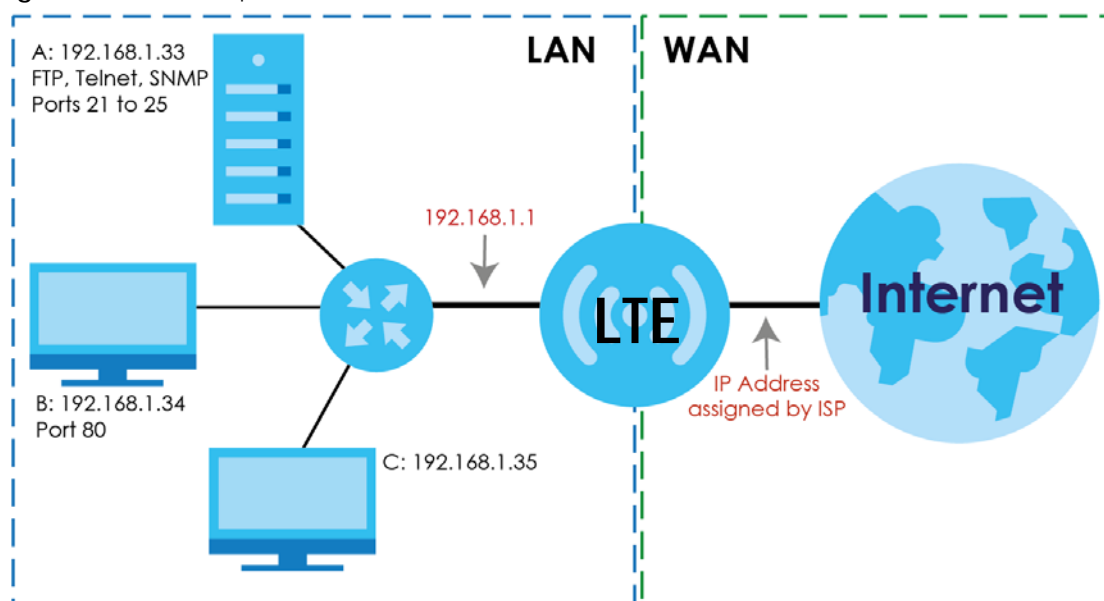
### 11.1 Overview

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 is changed to a different IP address known within another network.

The figure below is a simple illustration of a NAT network. 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 192.168.1.35 to a third (**C** in the example).

You assign the LAN IP addresses to the devices (**A** to **D**) connected to your LTE. The ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet. All traffic coming from **A** to **D** going out to the Internet use the IP address of the LTE, which is 192.168.1.1.

Figure 48 NAT Example



Note: You must create a firewall rule in addition to setting up NAT, to allow traffic from the WAN to be forwarded through the LTE.

#### 11.1.1 What You Can Do

- Use the **General** screen to enable NAT ([Section 11.2 on page 94](#)).
- Use the **Port Forwarding** screen to set a default server and change your LTE's port forwarding settings to forward incoming service requests to the servers on your local network ([Section 11.3 on page 94](#)).
- Use the **Port Trigger** screen to change your LTE's trigger port settings ([Section 11.4 on page 98](#)).

- Use the **ALG** screen to enable or disable SIP (VoIP) ALG (Application Layer Gateway) in the LTE (Section 11.5 on page 99).

## 11.2 General Settings

Use this screen to enable NAT and set a default server. Click **Configuration > Network > NAT** to open the **General** screen.

**Figure 49** Configuration > Network > NAT > General

General	Port Forwarding	Port Trigger	ALG	DMZ
Network Address Translation(NAT) :				
			<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
NAT Loopback :				
			<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
			Cancel	Apply

The following table describes the labels in this screen.

**Table 34** Configuration > Network > NAT > General

LABEL	DESCRIPTION
Network Address Translation (NAT)	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Select <b>Enable</b> to activate NAT. Select <b>Disable</b> to turn it off.
NAT Loopback	NAT loopback allows local users to use a domain name to access a server on the local network. A packet sent to the public (WAN) IP address is always forwarded to the default gateway (the LTE). With NAT loopback enabled, the LTE uses the WAN interface's IP address as the packet's source address and treats the packet as if it came from the WAN interface. The packet then can be forwarded to the local server according to the port forwarding rule. Select <b>Enable</b> to activate NAT loopback. Select <b>Disable</b> to turn it off.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Apply	Click <b>Apply</b> to save your changes back to the LTE.

## 11.3 Port Forwarding

Use this screen to forward incoming service requests to the servers on your local network and set a default server. 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.

In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

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.

Port forwarding allows you to define the local servers to which the incoming services will be forwarded. To change your LTE's port forwarding settings, click **Configuration > Network > NAT > Port Forwarding**. The screen appears as shown.

Note: If you do not assign a **Default Server**, the LTE discards all packets received for ports that are not specified in this screen or remote management.

Refer to [Appendix B on page 178](#) for port numbers commonly used for particular services.

**Figure 50** Configuration > Network > NAT > Port Forwarding

The screenshot shows the 'Port Forwarding' configuration page. The 'Service Name' is set to 'User-defined', 'Service Protocol' is 'TCP\_UDP', and 'WAN Interface' is 'Default'. There are input fields for 'Port Range' and 'Translation Port Range', and a 'Server IP Address' field. An 'Add' button is located below the 'Server IP Address' field. At the bottom, there is a table with the following columns: #, Status, Name, Protocol, WAN Interface, Port, Translation Port, Server IP Address, and Modify. The 'Cancel' and 'Apply' buttons are at the bottom right.

#	Status	Name	Protocol	WAN Interface	Port	Translation Port	Server IP Address	Modify

The following table describes the labels in this screen.

Table 35 Configuration > Network > NAT > Port Forwarding

LABEL	DESCRIPTION
Service Name	Select a pre-defined service from the drop-down list box. The pre-defined service port numbers and protocol will be displayed in the port forwarding summary table.  Otherwise, select <b>User define</b> to manually enter the service name and port numbers and select the IP protocol.
Service Protocol	Select the transport layer protocol supported by this virtual server. Choices are <b>TCP</b> , <b>UDP</b> , or <b>TCP_UDP</b> .  If you have chosen a pre-defined service in the <b>Service Name</b> field, the protocol will be configured automatically.
WAN Interface	Select the WAN interface on which the matched packets are received.
Port Range	Specify the first and last external port numbers that identify the service.  If you have chosen a pre-defined service in the <b>Service Name</b> field, the port numbers will be configured automatically.
Translation Port Range	Specify the first and last internal port numbers that identify the service.  If you have chosen a pre-defined service in the <b>Service Name</b> field, the port numbers will be configured automatically.
Server IP Address	Enter the inside IP address of the virtual server here and click <b>Add</b> to add it in the port forwarding summary table.
#	This is the number of an individual port forwarding server entry.
Status	This icon is turned on when the rule is enabled.
Name	This field displays a name to identify this rule.
Protocol	This is the transport layer protocol used for the service.
WAN Interface	This field displays the WAN interface on which the matched packets are received.
Port	This field displays the port numbers.
Translation Port	This field displays the internal port numbers that identifies the service.
Server IP Address	This field displays the inside IP address of the server.
Modify	Click the <b>Edit</b> icon to open the edit screen where you can modify an existing rule.  Click the <b>Delete</b> icon to remove a rule.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Apply	Click <b>Apply</b> to save your changes back to the LTE.

### 11.3.1 Edit Port Forwarding

This screen lets you edit a port forwarding rule. Click a rule's **Edit** icon in the **Port Forwarding** screen to open the following screen.



**Figure 51** Configuration > Network > NAT > Port Forwarding Edit

Port Forwarding :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Service Name :	User-defined <input type="text"/> User define ▼
Service Protocol :	TCP_UDP ▼
WAN Interface :	Default ▼
Port Range :	40 <input type="text"/> -50 <input type="text"/>
Translation Port Range :	20 <input type="text"/> -30 <input type="text"/>
Server IP Address :	192.168.1.100 <input type="text"/>
<input type="button" value="Back"/> <input type="button" value="Cancel"/> <input type="button" value="Apply"/>	

The following table describes the labels in this screen.

**Table 36** Configuration > Network > NAT > Port Forwarding Edit

LABEL	DESCRIPTION
Port Forwarding	Select <b>Enable</b> to turn on this rule and the requested service can be forwarded to the host with a specified internal IP address.  Select <b>Disable</b> to disallow forwarding of these ports to an inside server without having to delete the entry.
Service Name	Select <b>User define</b> and type a name (of up to 31 printable characters) to identify this rule in the first field next to <b>Service Name</b> . Otherwise, select a predefined service in the second field next to <b>Service Name</b> . The predefined service name and port numbers will display in the <b>Service Name</b> and <b>Port Range</b> fields.
Service Protocol	Select the transport layer protocol supported by this virtual server. Choices are <b>TCP</b> , <b>UDP</b> , or <b>TCP_UDP</b> .  If you have chosen a pre-defined service in the <b>Service Name</b> field, the protocol will be configured automatically.
WAN Interface	Select the WAN interface on which the matched packets are received.
Port Range	Type a port numbers to define the service to be forwarded to the specified server.  To specify a range of ports, enter the first number and the last number of the range.
Translation Port Range	Enter a port number to which you want the incoming ports translated.  For a range of ports, enter the first number and the last number of the range.
Server IP Address	Type the IP address of the server on your LAN that receives packets from the ports specified in the <b>Port Range</b> field.
Back	Click <b>Back</b> to return to the previous screen.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Apply	Click <b>Apply</b> to save your changes back to the LTE.

## 11.4 Port Trigger

To change your LTE's trigger port settings, click **Configuration > Network > NAT > Port Trigger**. The screen appears as shown.

Note: Only one LAN computer can use a trigger port (range) at a time.

**Figure 52** Configuration > Network > NAT > Port Trigger

#	Name	WAN Interface	Incoming Port		Trigger Port
			Start Port	End Port	
1		Defc ▼			
2		Defc ▼			
3		Defc ▼			
4		Defc ▼			
5		Defc ▼			
6		Defc ▼			
7		Defc ▼			
8		Defc ▼			
9		Defc ▼			
10		Defc ▼			
11		Defc ▼			
12		Defc ▼			

The following table describes the labels in this screen.

**Table 37** Configuration > Network > NAT > Port Trigger

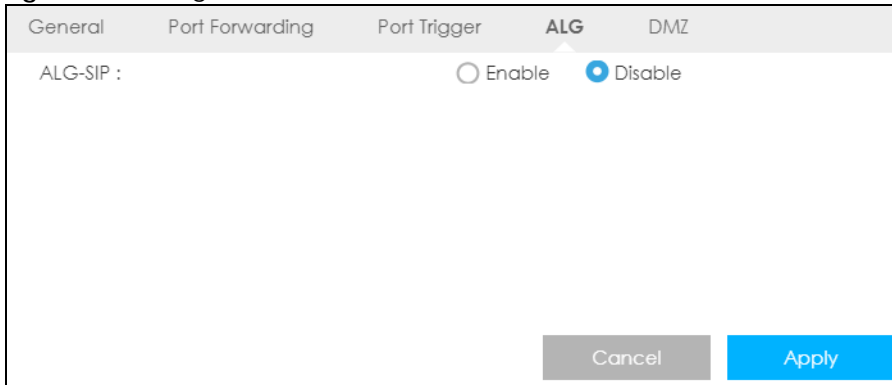
LABEL	DESCRIPTION
#	This is the rule index number (read-only).
Name	Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces.
WAN Interface	Select the WAN interface through which the matched packets are transmitted.
Incoming Port	Incoming Port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The LTE forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Trigger Port	The trigger port is a port that causes (or triggers) the LTE to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Apply	Click <b>Apply</b> to save your changes back to the LTE.

## 11.5 ALG

Some NAT routers may include a SIP Application Layer Gateway (ALG). A SIP ALG allows SIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream. When the LTE registers with the SIP register server, the SIP ALG translates the LTE'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 your LTE is behind a SIP ALG.

To enable and disable the SIP ALG in the LTE, click **Configuration > Network > NAT > ALG**. The screen appears as shown.

**Figure 53** Configuration > Network > NAT > ALG



The following table describes the labels in this screen.

**Table 38** Configuration > Network > NAT > ALG

LABEL	DESCRIPTION
ALG-SIP	Select <b>Enable</b> to make sure SIP (VoIP) works correctly with port-forwarding and address-mapping rules. Otherwise, select <b>Disable</b> to turn off the SIP ALG.
Apply	Click <b>Apply</b> to save your changes back to the LTE.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 11.6 Technical Reference

The following section contains additional technical information about the LTE features described in this chapter.

### 11.6.1 NAT Port Forwarding: Services and Port Numbers

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

Use the **Port Forwarding** screen to forward incoming service requests to the servers 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.

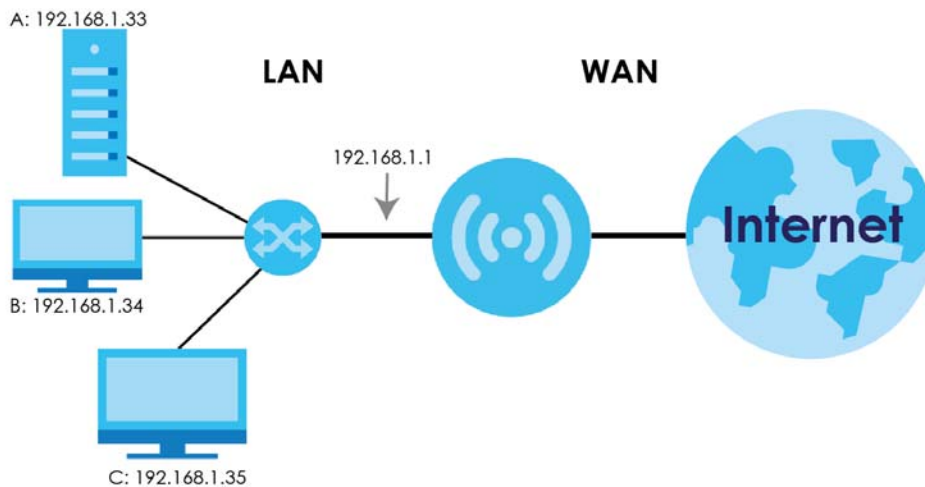
In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

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.

## 11.6.2 NAT 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 192.168.1.35 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 54** Multiple Servers Behind NAT Example



## 11.6.3 Trigger Port Forwarding

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

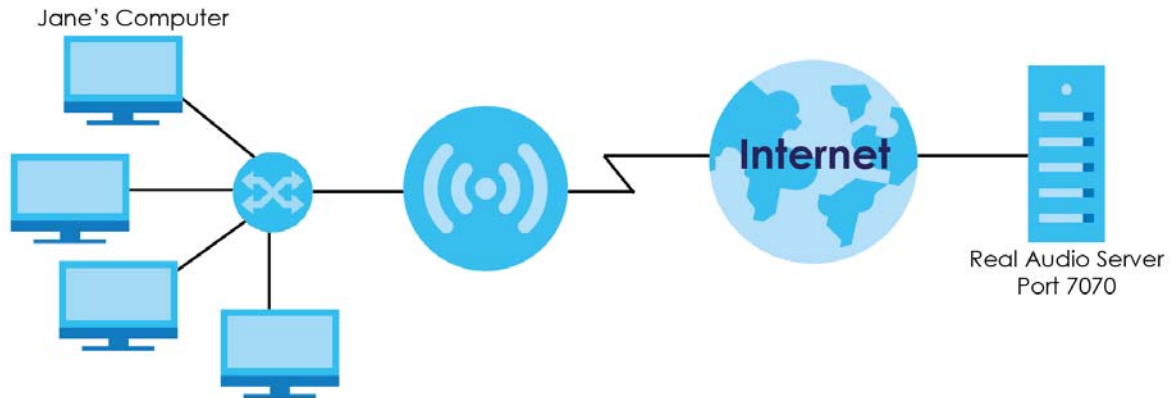
Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The LTE records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the LTE's WAN port receives a response with a specific port number and protocol ("incoming" port), the LTE forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you

do not need to configure a new IP address each time you want a different LAN computer to use the application.

## 11.6.4 Trigger Port Forwarding Example

The following is an example of trigger port forwarding.

**Figure 55** Trigger Port Forwarding Process: Example



- 1 Jane requests a file from the Real Audio server (port 7070).
- 2 Port 7070 is a "trigger" port and causes the LTE to record Jane's computer IP address. The LTE associates Jane's computer IP address with the "incoming" port range of 6970-7170.
- 3 The Real Audio server responds using a port number ranging between 6970-7170.
- 4 The LTE forwards the traffic to Jane's computer IP address.
- 5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The LTE times out in three minutes with UDP (User Datagram Protocol), or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

## 11.6.5 Two Points To Remember About Trigger Ports

- 1 Trigger events only happen on data that is coming from inside the LTE and going to the outside.
- 2 If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can't trigger it.

# CHAPTER 12

## DDNS

### 12.1 Overview

Dynamic Domain Name Service (DDNS) services let you use a fixed domain name with a dynamic IP address. Users can always use the same domain name instead of a different dynamic IP address that changes each time to connect to the LTE or a server in your network.

Note: The LTE must have a public global IP address and you should have your registered DDNS account information on hand.

### 12.2 General Settings

To change your LTE's DDNS, click **Network > DDNS**. The screen appears as shown.

Figure 56 Dynamic DNS

The screenshot shows the 'Dynamic DNS' configuration interface. It features two main sections: 'IPv4 Dynamic DNS Setup' and 'IPv6 Dynamic DNS Setup'. Each section includes a 'Dynamic DNS' toggle (currently set to 'Disable'), a 'Service Provider' dropdown menu (set to 'DynDNS.org' for IPv4 and 'freedns.afrai' for IPv6), and input fields for 'Host Name', 'Username', and 'Password' (for IPv4) or 'Token' (for IPv6). At the bottom right, there are 'Cancel' and 'Apply' buttons.

The following table describes the labels in this screen.

Table 39 Dynamic DNS

LABEL	DESCRIPTION
IPv4 Dynamic DNS Setup	
Dynamic DNS	Select <b>Enable</b> to use dynamic DNS. Select <b>Disable</b> to turn this feature off.
Service Provider	Select the name of your Dynamic DNS service provider.

Table 39 Dynamic DNS (continued)

LABEL	DESCRIPTION
Host Name	The host name is the domain name that the DDNS service will map to your dynamic global IP address. Type the host name fully qualified, for example, "yourhost.mydomain.net". You can specify up to two host names in the field separated by a comma (",").
Username	Enter your user name.
Password	Enter the password assigned to you.
IPv6 Dynamic DNS Setup	
Dynamic DNS	Select <b>Enable</b> to use dynamic DNS. Select <b>Disable</b> to turn this feature off.
Service Provider	Select the name of your Dynamic DNS service provider.
Host Name	The host name is the domain name that the DDNS service will map to your dynamic global IP address. Type the host name fully qualified, for example, "yourhost.mydomain.net". You can specify up to two host names in the field separated by a comma (",").
Token	This is the token authentication provided by the hosting provider (for example, FreeDDNS). When the host name is registered, the hosting server provides the token identifier.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Apply	Click <b>Apply</b> to save your changes back to the LTE.

# CHAPTER 13

## Routing

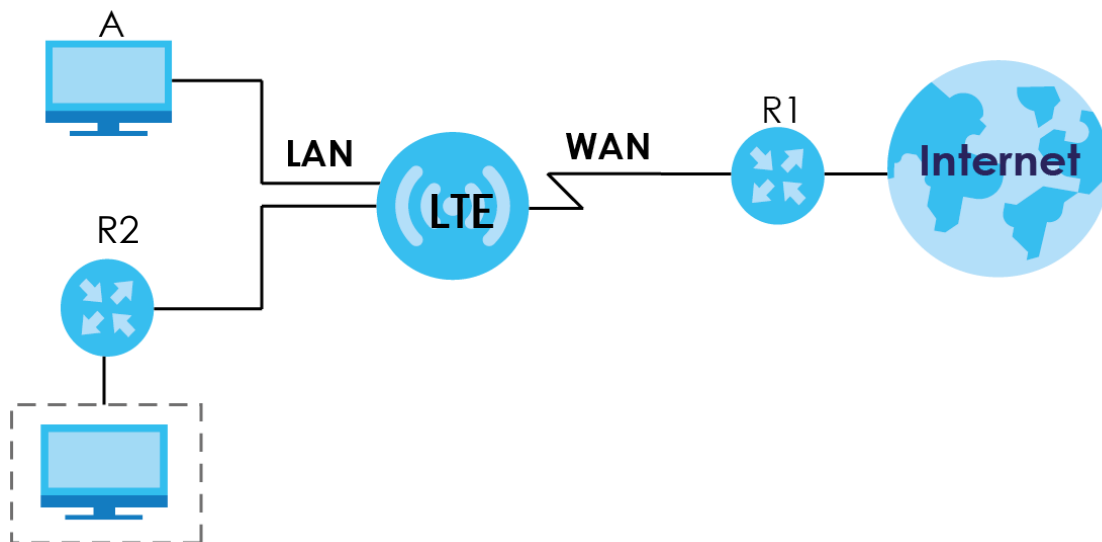
### 13.1 Overview

This chapter shows you how to configure static routes for your LTE.

The LTE usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the LTE 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's LAN interface. The LTE routes most traffic from **A** to the Internet through the LTE's default gateway (**R1**). You create a static route to communicate with a separate network behind a router **R2** connected to the LAN.

**Figure 57** Example of Static Routing Topology



### 13.2 Static Route

Click **Network > Routing > Static Route** to open the **Static Route** screen.



**Figure 58** Network > Routing > Static Route

The following table describes the labels in this screen.

**Table 40** Network > Routing > Static Route

LABEL	DESCRIPTION
Add Static Route	Click this to create a new rule.
#	This is the number of an individual static route.
Status	This field indicates whether the rule is active (yellow bulb) or not (gray bulb).
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Subnet Mask	This parameter specifies the IP network subnet mask of the final destination.
Gateway	This is the 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.
Modify	Click the <b>Edit</b> icon to open a screen where you can modify an existing rule. Click the <b>Delete</b> icon to remove a rule from the LTE.

## 13.2.1 Add/Edit Static Route

Click the **Add Static Route** button or a rule's **Edit** icon in the **Static Route** screen. Use this screen to configure the required information for a static route.

**Figure 59** Network > Routing > Static Route: Add/Edit

The following table describes the labels in this screen.

Table 41 Network > Routing > Static Route: Add/Edit

LABEL	DESCRIPTION
Static Route	Select to enable or disable this rule.
Destination IP Address	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.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your LTE's interfaces. The gateway helps forward packets to their destinations.
Back	Click <b>Back</b> to return to the previous screen without saving.
Cancel	Click <b>Cancel</b> to set every field in this screen to its last-saved value.
Apply	Click <b>Apply</b> to save your changes back to the LTE.

## 13.3 Dynamic Routing

Use this screen to enable and configure RIP on the LTE. Click **Network > Routing > Dynamic Routing** to open the **Dynamic Routing** screen.

Figure 60 Network > Routing > Dynamic Routing

The following table describes the labels in this screen.

Table 42 Network > Routing > Dynamic Routing

LABEL	DESCRIPTION
Dynamic Routing	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The RIP version controls the format and the broadcasting method of the RIP packets that the LTE sends (it recognizes both formats when receiving). RIP version 1 is universally supported but RIP version 2 carries more information. RIP version 1 is probably adequate for most networks, unless you have an unusual network topology.  Select the RIP version from <b>RIPv1</b> and <b>RIPv2</b> . Otherwise, select <b>Disable</b> to turn it off.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Apply	Click <b>Apply</b> to save your changes back to the LTE.

# CHAPTER 14

## Interface Group

### 14.1 Overview

By default, the four LAN interfaces on the LTE are in the same group and can communicate with each other. Creating a new interface will create a new LAN bridge interface (subnet) (for example, 192.168.2.0/24) that acts as a dependent LAN network, and is a different subnet from default LAN subnet (192.168.1.0/24).

### 14.2 Interface Group

You can manually add a LAN/WLAN interface to a new group.

Use the **DHCP** screen to configure the private IP addresses the DHCP server on the LTE assigns to the clients in the default and/or user-defined groups. See [Chapter 10 on page 88](#) for more information.

Use the **Interface Group** screen to create a new interface group, which is a new LAN bridge interface (subnet). Click **Network > Interface Group** to open the following screen.

**Figure 61** Network > Interface Group

Name	LAN Interface	VID	Actions
LAN	LAN-2, LAN-3 VAP-1, VAP-2, VAP-3, VAP-4 VAP-1, VAP-2, VAP-3, VAP-4	Native VLAN Tag 1	

The following table describes the fields in this screen.

**Table 43** Network > Interface Group

LABEL	DESCRIPTION
Add	Click this button to create a new interface group.
Name	This shows the descriptive name of the group.
LAN Interface	This shows the interface group.
VID	This shows the VLAN ID number (from 0 to 4094) of the interface group.
Actions	Click the <b>Delete</b> icon to remove the user-defined group.

## 14.2.1 Add Interface Group

Click the **Add** button in the **Interface Group** screen to open the following screen. Use this screen to create a new interface group.

Note: An interface can belong to only one group at a time.

**Figure 62** Network > Interface Group > Add

The screenshot shows the 'Interface Group' configuration screen. The fields are as follows:

- Name:** VLAN - 1
- VLAN TAG:** Disable
- VLAN ID:** 3 (3-4096)
- Port Members:**
  - Port:  LAN-2  LAN-3  LAN-4
  - 2.4G:  VAP-1  VAP-2  VAP-3  VAP-4
  - 5G:  VAP-1  VAP-2  VAP-3  VAP-4

Buttons: Cancel, Apply

The following table describes the fields in this screen.

**Table 44** Network > Interface Group > Add

LABEL	DESCRIPTION
Name	Enter a name to identify this group. You can enter up to 30 characters. You can use letters, numbers, hyphens (-) and underscores (_). Spaces are not allowed.
VLAN TAG	Click <b>Enable</b> to set the port to tag all LAN traffic with the VLAN ID.
VLAN ID	Select a VLAN ID (3-4094) to identify this group.
Port Members	Select the LAN interfaces (Ethernet LAN or wireless LAN) in the group.
Cancel	Click <b>Cancel</b> to exit this screen without saving.
Apply	Click <b>Apply</b> to save your changes back to the LTE.

# CHAPTER 15

## Firewall

### 15.1 Overview

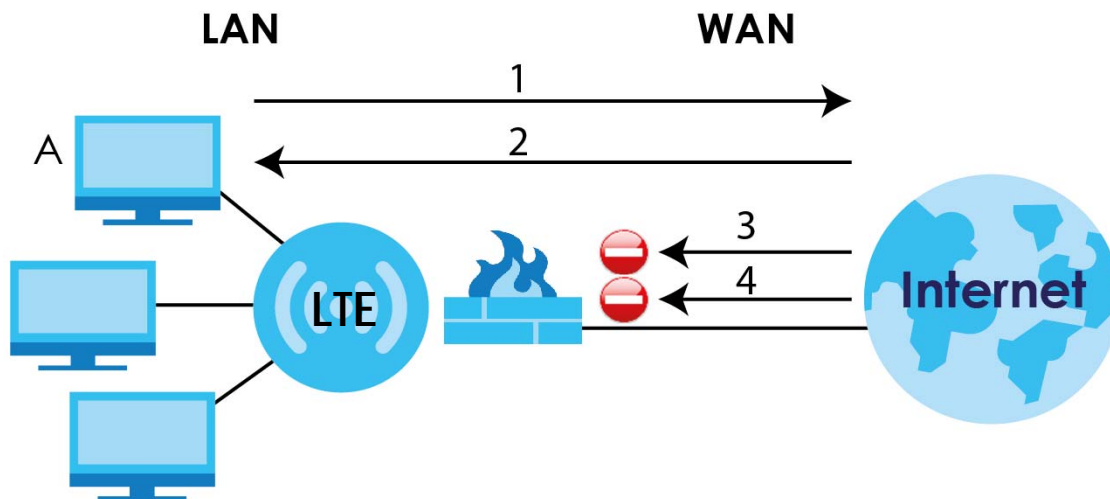
Use these screens to enable and configure the firewall that protects your LTE and your LAN from unwanted or malicious traffic.

Enable the firewall to protect your LAN computers from attacks by hackers on the Internet and control access between the LAN and WAN. By default the firewall:

- allows traffic that originates from your LAN computers to go to all of the networks.
- blocks traffic that originates on the other networks from going to the LAN.

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 63 Default Firewall Action



#### 15.1.1 What You Can Do

- Use the **General** screen to enable or disable the LTE's firewall ([Section 15.2 on page 110](#)).
- Use the **Services** screen enable service blocking, enter/delete/modify the services you want to block and the date/time you want to block them ([Section 15.3 on page 111](#)).

#### 15.1.2 What You Need To Know

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

## About the LTE Firewall

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

It is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (click the **General** tab under **Firewall** and then click the **Enable Firewall** check box). The LTE's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The LTE 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 is installed between the LAN and a broadband modem connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The LTE has one Ethernet WAN port and four Ethernet LAN ports, which are used to physically separate the network into two areas. The WAN (Wide Area Network) port attaches to the broadband (cable or DSL) modem to the Internet.

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 email, 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.

## Guidelines For Enhancing Security With Your Firewall

- 1 Change the default password via Web Configurator.
- 2 Think about access control before you connect to the network in any way, including attaching a modem to the port.
- 3 Limit who can access your router.
- 4 Don't enable any local service (such as NTP) 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.
- 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.
- 6 Protect against IP spoofing by making sure the firewall is active.
- 7 Keep the firewall in a secured (locked) room.

## 15.2 General Settings

Use this screen to enable or disable the LTE's firewall, and set up firewall logs. Click **Configuration > Security > Firewall** to open the **General** screen.

**Figure 64** Configuration > Security > Firewall > General

The following table describes the labels in this screen.

**Table 45** Configuration > Security > Firewall > General

LABEL	DESCRIPTION
Enable Firewall	Select this check box to activate the firewall. The LTE performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Cancel	Click <b>Cancel</b> to start configuring this screen again.
Apply	Click <b>Apply</b> to save the settings.

## 15.3 Firewall Services

If an outside user attempts to probe an unsupported port on your LTE, an ICMP response packet is automatically returned. This allows the outside user to know the LTE exists. Use this screen to prevent the ICMP response packet from being sent. This keeps outsiders from discovering your LTE when unsupported ports are probed.

You can also use this screen to enable service blocking, enter/delete/modify the services you want to block and the date/time you want to block them.

Click **Configuration > Security > Firewall > Services**. The screen appears as shown next.

Figure 65 Configuration &gt; Security &gt; Firewall &gt; Services

#	Service Name	MAC Address	Dest IP	Source IP	Protocol	DestPort Range	SourcePort Range	Action	Delete
1	Rule 1	AA98:CC11:2233	1.1.1.1	2.2.2.2	TCP	40-50	30-39	Drop	

The following table describes the labels in this screen.

Table 46 Configuration &gt; Security &gt; Firewall &gt; Services

LABEL	DESCRIPTION
ICMP	Internet Control Message Protocol 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.
Respond to Ping on	The LTE will not respond to any incoming Ping requests when <b>Disable</b> is selected. Select <b>LAN</b> to reply to incoming LAN Ping requests. Select <b>WAN</b> to reply to incoming WAN Ping requests. Otherwise select <b>LAN&amp;WAN</b> to reply to all incoming LAN and WAN Ping requests.
Apply	Click <b>Apply</b> to save the settings.
WAN Stealth Mode	
Enable WAN Stealth Mode	Select this check box to silently discard the matched packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender.
Apply	Click <b>Apply</b> to save the settings.
Enable Firewall Rule	
Enable Firewall Rule	Select this check box to activate the firewall rules that you define (see <b>Add Firewall Rule</b> below).
Apply	Click <b>Apply</b> to save the settings.
Black List/ White List	
Black List / White List	Select <b>Allow those match the following rules</b> to allow communication only if traffic matches the firewall rules.  Select <b>Deny those match the following rules</b> to deny communication only if traffic matches the firewall rules.
Apply	Click <b>Apply</b> to save your settings.
Add Firewall Rule	
Service Name	Enter a name that identifies or describes the firewall rule.
MAC Address	Enter the MAC address of the computer for which the firewall rule applies.



Table 46 Configuration &gt; Security &gt; Firewall &gt; Services (continued)

LABEL	DESCRIPTION
Dest IP Address	Enter the IP address of the computer to which traffic for the application or service is entering. The LTE applies the firewall rule to traffic initiating from this computer.
Source IP Address	Enter the IP address of the computer that initializes traffic for the application or service. The LTE applies the firewall rule to traffic initiating from this computer.
Protocol	Select the protocol ( <b>TCP</b> , <b>UDP</b> or <b>ICMP</b> ) used to transport the packets for which you want to apply the firewall rule.
Dest Port Range	Enter the port number/range of the destination that define the traffic type, for example TCP port 80 defines web traffic.
Source Port Range	Enter the port number/range of the source that define the traffic type, for example TCP port 80 defines web traffic.
Add Rule	Click <b>Add</b> to save the firewall rule.
Firewall Rule	
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.
Service Name	This is a name that identifies or describes the firewall rule.
MAC address	This is the MAC address of the computer for which the firewall rule applies.
Dest IP	This is the IP address of the computer to which traffic for the application or service is entering.
Source IP	This is the IP address of the computer from which traffic for the application or service is initialized.
Protocol	This is the protocol ( <b>TCP</b> , <b>UDP</b> or <b>ICMP</b> ) used to transport the packets for which you want to apply the firewall rule.
Dest Port Range	This is the port number/range of the destination that define the traffic type, for example TCP port 80 defines web traffic.
Source Port Range	This is the port number/range of the source that define the traffic type, for example TCP port 80 defines web traffic.
Action	<b>DROP</b> - Traffic matching the conditions of the firewall rule are stopped.
Delete	Click <b>Delete</b> to remove the firewall rule.
Cancel	Click <b>Cancel</b> to start configuring this screen again.

See [Appendix B on page 178](#) for commonly used services and port numbers.

# CHAPTER 16

# Content Filtering

## 16.1 Overview

This chapter shows you how to configure content filtering. Content filtering is the ability to block certain web features and specific URLs.

### Keyword Blocking URL Checking

The LTE checks the URL's domain name (or IP address) and file path separately when performing keyword blocking.

The URL's domain name or IP address is the characters that come before the first slash in the URL. For example, with the URL [www.zyxel.com.tw/news/pressroom.php](http://www.zyxel.com.tw/news/pressroom.php), the domain name is [www.zyxel.com.tw](http://www.zyxel.com.tw).

The file path is the characters that come after the first slash in the URL. For example, with the URL [www.zyxel.com.tw/news/pressroom.php](http://www.zyxel.com.tw/news/pressroom.php), the file path is [news/pressroom.php](http://www.zyxel.com.tw/news/pressroom.php).

Since the LTE checks the URL's domain name (or IP address) and file path separately, it will not find items that go across the two. For example, with the URL [www.zyxel.com.tw/news/pressroom.php](http://www.zyxel.com.tw/news/pressroom.php), the LTE would find "tw" in the domain name ([www.zyxel.com.tw](http://www.zyxel.com.tw)). It would also find "news" in the file path ([news/pressroom.php](http://www.zyxel.com.tw/news/pressroom.php)) but it would not find "tw/news".

## 16.2 Content Filter

Use this screen to restrict web features, and designate a trusted computer. You can also use this screen to configure URL filtering settings to block the users on your network from accessing certain web sites. Click **Configuration > Security > Content Filter** to open the **Content Filter** screen.

Figure 66 Configuration &gt; Security &gt; Content Filter

**Content Filter**

**Trusted IP Setup**  
A trusted computer has full access to all blocked resources.  
Trusted Computer IP Address:

**Restrict Web Features**  
 ActiveX     Java     Cookies     Web Proxy

**Keyword Blocking**  
 Enable URL Keyword Blocking  
Keyword:    
Keyword List

The following table describes the labels in this screen.

Table 47 Configuration &gt; Security &gt; Content Filter

LABEL	DESCRIPTION
Trusted IP Setup	To enable this feature, enter an IP address of any one of the computers in your network that you want to have as a trusted computer. This allows the trusted computer to have full access to all features that are configured to be blocked by content filtering.  Leave this field blank to have no trusted computers.
Restrict Web Features	Select the box(es) to restrict a feature. When you download a page containing a restricted feature, that part of the web page will appear blank or grayed out.
ActiveX	A tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.
Java	A programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.
Cookies	Used by Web servers to track usage and provide service based on ID.
Web Proxy	A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
Enable URL Keyword Blocking	The LTE can block Web sites with URLs that contain certain keywords in the domain name or IP address. For example, if the keyword "bad" was enabled, all sites containing this keyword in the domain name or IP address will be blocked, e.g., URL <a href="http://www.website.com/bad.html">http://www.website.com/bad.html</a> would be blocked. Select this check box to enable this feature.
Keyword	Type a keyword in this field. You may use any character (up to 64 characters). Wildcards are not allowed. You can also enter a numerical IP address.

Table 47 Configuration &gt; Security &gt; Content Filter (continued)

LABEL	DESCRIPTION
Keyword List	This list displays the keywords already added.
Add	Click <b>Add</b> after you have typed a keyword. Repeat this procedure to add other keywords. Up to 64 keywords are allowed. When you try to access a web page containing a keyword, you will get a message telling you that the content filter is blocking this request.
Delete	Highlight a keyword in the lower box and click <b>Delete</b> to remove it. The keyword disappears from the text box after you click <b>Apply</b> .
Clear All	Click this button to remove all of the listed keywords.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.
Apply	Click <b>Apply</b> to save your changes.

# CHAPTER 17

## IPv6 Firewall

### 17.1 Overview

This chapter shows you how to enable and create IPv6 firewall rules to block unwanted IPv6 traffic.

### 17.2 IPv6 Firewall

Click **Configuration > Security > IPv6 Firewall**. The **Service** screen appears as shown.

**Figure 67** Configuration > Security > IPv6 Firewall

Services

**Enable Firewall Rule**

Enable Firewall Rule

**Black List / White List**

Black List / White List

**Add Firewall Rule**

Service Name :

MAC Address :

Dest IP Address :

Source IP Address :

Protocol : TCP

Dest Port Range :  -

Source Port Range :  -

**Firewall Rule**

#	Service Name	MAC Address	Dest IP	Source IP	Protocol	DestPort Range	SourcePort Range	Action	Delete
---	--------------	-------------	---------	-----------	----------	----------------	------------------	--------	--------

The following table describes the labels in this screen.

**Table 48** Configuration > Security > IPv6 Firewall

LABEL	DESCRIPTION
Enable Firewall Rule	
Enable Firewall Rule	Select this check box to activate the firewall rules that you define (see <b>Add Firewall Rule</b> below).
Apply	Click <b>Apply</b> to save the settings.

Table 48 Configuration &gt; Security &gt; IPv6 Firewall (continued)

LABEL	DESCRIPTION
Black List/ White List	
Black List / White List	Select <b>Allow those match the following rules</b> to allow communication only if traffic matches the firewall rules.  Select <b>Deny those match the following rules</b> to deny communication only if traffic matches the firewall rules.
Apply	Click <b>Apply</b> to save your settings.
Add Firewall Rule	
Service Name	Enter a name that identifies or describes the firewall rule.
MAC Address	Enter the MAC address of the computer for which the firewall rule applies.
Dest IP Address	Enter the IPv6 address of the computer to which traffic for the application or service is entering.  The LTE applies the firewall rule to traffic destined for this computer.
Source IP Address	Enter the IPv6 address of the computer that initializes traffic for the application or service.  The LTE applies the firewall rule to traffic initiating from this computer.
Protocol	Select the protocol ( <b>TCP, UDP or ICMP</b> ) used to transport the packets for which you want to apply the firewall rule.
Dest Port Range	Enter the port number/range of the destination that defines the traffic type, for example TCP port 80 defines web traffic.
Source Port Range	Enter the port number/range of the source that defines the traffic type, for example TCP port 80 defines web traffic.
Add Rule	Click <b>Add Rule</b> to save the firewall rule.
Firewall Rule	
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.
ServiceName	This is a name that identifies or describes the firewall rule.
MACaddress	This is the MAC address of the computer for which the firewall rule applies.
DestIP	This is the IP address of the computer to which traffic for the application or service is entering.
Source IP	This is the IP address of the computer to which traffic for the application or service is initialized.
Protocol	This is the protocol ( <b>TCP, UDP or ICMP</b> ) used to transport the packets for which you want to apply the firewall rule.
DestPortRange	This is the port number/range of the destination that defines the traffic type, for example TCP port 80 defines web traffic.
SourcePortRange	This is the port number/range of the source that defines the traffic type, for example TCP port 80 defines web traffic.
Action	<b>DROP</b> - Traffic matching the conditions of the firewall rule is stopped.
Delete	Click <b>Delete</b> to remove the firewall rule.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.

# CHAPTER 18

## VPN

### 18.1 Overview

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing. It is used to transport traffic over the Internet or any insecure network that uses TCP/IP for communication.

#### 18.1.1 What You Can Do in this Chapter

- Use the **L2TP Server** screen to configure the LTE's L2TP VPN settings ([Section 18.3 on page 120](#)).
- Use the **L2TP Client** screen to view connection details for L2TP clients ([Section 18.4 on page 121](#)).
- Use the **GRE** screen to enable Generic Routing Encapsulation (GRE) tunnels ([Section 18.5 on page 124](#)).
- Use the **VPN Passthrough** screen to allow VPN traffic to pass through the LTE ([Section 18.6 on page 127](#)).

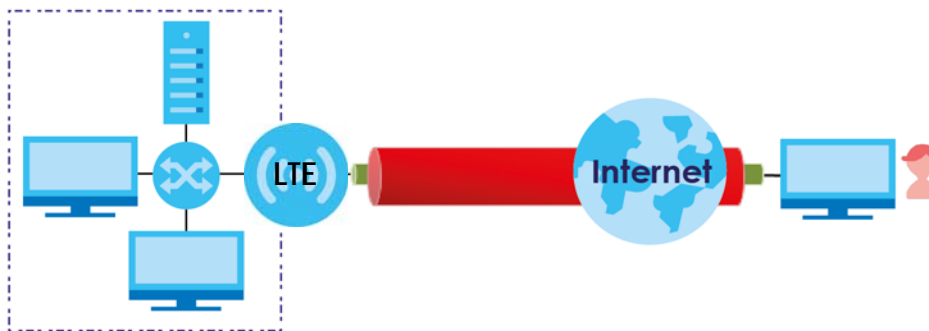
### 18.2 What You Need to Know

#### L2TP VPN

The Layer 2 Tunneling Protocol (L2TP) works at layer 2 (the data link layer) to tunnel network traffic between two peers over another network (like the Internet).

L2TP VPN lets remote users use the L2TP client software included with their computers' operating systems to securely connect to the network behind the LTE.

**Figure 68** L2TP VPN Overview



## 18.3 L2TP Server

Click **Configuration > Application > VPN > L2TP VPN** to open the following screen. Use this screen to configure the LTE L2TP VPN settings.

**Figure 69** Configuration > Application > VPN > L2TP VPN

**L2TP Server** | L2TP Client | GRE | VPN Passthrough

**Configuration**

Enable

Service Port 1701

Server Virtual IP 192.168.10.1

IP Pool Starting Address 10

IP Pool Ending Address 41

Authentication  PAP  CHAP  MS-CHAP  MS-CHAP v2

MPPE Encryption  Enable 40 bits

**Tunnel List** Refresh

User Name	Remote IP	Remote Virtual IP	Remote Call ID	Actions
No connection from remote				

**VPN Account List** Add Delete

ID	Enable	User Name	Password	Actions
1	<input checked="" type="checkbox"/>	User1	1234	Edit <input type="checkbox"/> Select

Cancel Apply

The following table describes the labels in this screen.

**Table 49** Configuration > Application > VPN > L2TP VPN

LABEL	DESCRIPTION
Configuration	
Enable	Select this to configure the LTE L2TP VPN functions as a server.
Service Port	This is the default L2TP VPN service port on the LTE. If you change this, you must let clients know what the new L2TP VPN service port is.
Server Virtual IP	Select the IP address used to establish the VPN tunnel connection.
IP Pool Starting Address	Enter the pool's starting IP address that the LTE uses to assign to the L2TP VPN clients.  Note: These addresses use a 24-bit netmask and should not conflict with any WAN, LAN, or WLAN subnet even if they are not in use.
IP Pool Ending Address	Enter the pool's ending IP address that the LTE uses to assign to the L2TP VPN clients.



Table 49 Configuration &gt; Application &gt; VPN &gt; L2TP VPN (continued)

LABEL	DESCRIPTION
Authentication	Select <b>PAP</b> , <b>CHAP</b> , <b>MS-CHAP</b> , and/or <b>MS-CHAP v2</b> as your authentication method.  <b>PAP</b> (Password Authentication Protocol) - The L2TP server will crosscheck the username and password sent by the client with the database for authentication purposes.  <b>CHAP</b> (Challenge Handshake Authentication Protocol) - When it's enabled, MSCHAP and MS-CHAP-v2 are both supported.  You can't enable <b>PAP</b> and <b>CHAP</b> when <b>MPPE Encryption</b> is enabled.
MPPE Encryption	Click the check box to use MPPE, Microsoft Point to Point Encryption. Select whether you will have <b>40-bit</b> , <b>56-bit</b> or <b>128-bit</b> session key used to initialize the encryption.
Tunnel List This displays the LTE's current L2TP VPN tunnels.	
Refresh	Click <b>Refresh</b> to update the LTE
User Name	This is the user name establishing an L2TP VPN tunnel.
Remote IP	This is the client's public IP for this VPN connection.
Remote Virtual IP	This displays the IP address assigned by the L2TP server to the connected client.
Remote Call ID	This displays the call identification the L2TP Server uses to identify its clients.
Actions	Use this to end a connected client's L2TP tunnel.
VPN Account List This displays a list of the L2TP user accounts allowed to establish VPN tunnels.	
Add	Click <b>Add</b> to create a new L2TP user account.
Delete	Click <b>Delete</b> to remove a L2TP user account.
ID	This field displays the index number of the L2TP user account.
Enable	Select this to enable this L2TP user account, once it is enabled that client can establish a VPN tunnel.
User Name	Enter the user name for PPP authentication. It must be consistent with the configuration made on LNS (L2TP Network Server). Otherwise the L2TP VPN connection will not be established.
Password	Enter the password for PPP authentication. It must be consistent with the configuration made on LNS (L2TP Network Server). Otherwise the L2TP VPN connection will not be established.
Action	Click <b>Modify</b> to change modify an existing L2TP user account, select the check box and click <b>Delete</b> to remove it.
Cancel	Click <b>Cancel</b> to exit this screen without saving.
Apply	Click <b>Apply</b> to save your changes back to the LTE.

## 18.4 L2TP Client

Use the L2TP Client Status screen to view details about L2TP clients. Click **Configuration > Application > VPN > L2TP Client** to open the following screen.

**Figure 70** Configuration > Application> VPN > L2TP Client

The following table describes the labels in this screen.

**Table 50** Configuration > Application > VPN > L2TP Client

LABEL	DESCRIPTION
L2TP Client Configuration	
L2TP Client	Select <b>Enable</b> to configure the L2TP settings for this client.
Tunnel List	
ID	This field is a sequential value, and it is not associated with a specific L2TP VPN session.
Name	This field displays the remote user's user name.
Enable	Select this to enable/disable this L2TP VPN connection.
Status	This displays the status of the L2TP client VPN connection. <ul style="list-style-type: none"> <li>• <b>Connected</b> - The L2TP client VPN connection is up.</li> <li>• <b>Disconnected</b> - The L2TP client VPN connection is down.</li> <li>• <b>Connecting</b> - The LTE is trying to establish an L2TP client VPN connection.</li> </ul>
Server	Enter the WAN IP address of the LTE.
Virtual IP	This field displays the IP address that the LTE assigned for the remote user's computer to use within the L2TP VPN tunnel.
Remote Subnet	This field displays the network IP address of the network behind the client.
Actions	Click the <b>Edit</b> button to modify an L2TP client 's configurations. Select it and click <b>Delete</b> to remove it.
Cancel	Click <b>Cancel</b> to exit this screen without saving.
Apply	Click <b>Apply</b> to save your changes back to the LTE.

### 18.4.1 Add L2TP Client

To add an L2TP client, make sure you enabled **L2TP Client Configuration**, then click **Add** in the **Tunnel List** for the following screen to display.

Figure 71 L2TP Client: Add

The following table describes the labels in this screen.

Table 51 L2TP Client: Add

LABEL	DESCRIPTION
Name	Specify a name for the L2TP VPN client.
Enable	Select this to enable the L2TP VPN client connection.
Server IP/FQDN	Enter the public IP address or FQDN of the L2TP Server.
Server Port	Enter the remote L2TP Network Server (LNS) port for this L2TP Tunnel. The port number should be between 1~65535.
User Name	Enter the user name for this L2TP tunnel to be authenticated when it connects to the L2TP server. The user name be between 1~32 ASCII characters.
Password	Enter the password for this L2TP tunnel to be authenticated when it connects to the L2TP server.
Authentication	Select <b>PAP</b> , <b>CHAP</b> , <b>MS-CHAP</b> , and/or <b>MS-CHAP v2</b> as your authentication method.  <b>PAP</b> (Password Authentication Protocol) - The L2TP server will crosscheck the username and password sent by the client with the database for authentication purposes.  <b>CHAP</b> (Challenge Handshake Authentication Protocol) - When it's enabled, MSCHAP and MS-CHAP-v2 are both supported.  You can't enable <b>PAP</b> and <b>CHAP</b> when <b>MPPE Encryption</b> is enabled.
MPPE Encryption	Click the check box to use MPPE, Microsoft Point to Point Encryption. Select whether you will have <b>40-bit</b> , <b>56-bit</b> or <b>128-bit</b> session key used to initialize the encryption.

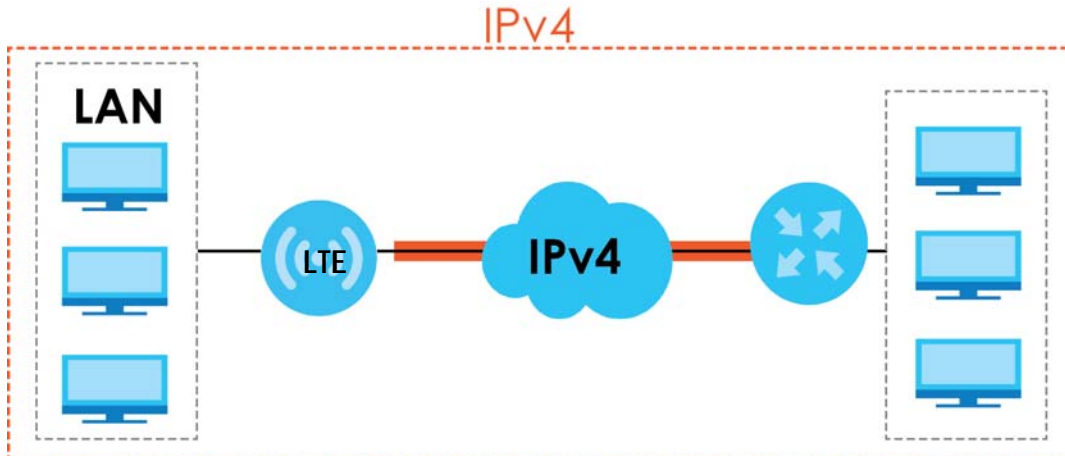
Table 51 L2TP Client: Add (continued)

LABEL	DESCRIPTION
Remote Subnet	<p>Specify the remote subnet for this L2TP tunnel to reach L2TP server. The <b>Remote Subnet</b> format must be IP address/netmask (e.g. 10.0.0.2/24).</p> <p>The <b>Remote Subnet</b> is used for the L2TP VPN server's Intranet. At the L2TP client's side, the packets whose destination is in the dedicated subnet will be transferred via the L2TP VPN tunnel. Other packets will be transferred based on current routing policy of the security gateway at L2TP client peer.</p> <p>If you entered 0.0.0.0/0 in the <b>Remote Subnet</b> field, the L2TP server will be treated as a default gateway setting for the L2TP client. This means all packets, including the Internet accessing of L2TP Client, will go through the established L2TP VPN tunnel.</p>
Tunneling Password (Option)	Enter the password for this L2TP VPN tunnel to be authenticated by the L2TP Server.
LCP Echo Type	<p>Specify the Link Control Protocol (LCP) Echo Type for this tunnel. This means the LTE checks the PPP connection to a remote client using LCP requests.</p> <p>In the <b>Interval</b> field define how often the LCP requests are prompted. If there is no reply to an LCP request then the remote client is checked in shorter intervals. Define how many times the LTE tries to reach the remote site in the <b>Max. Failure Time</b>.</p> <ul style="list-style-type: none"> <li>• Select <b>Auto</b> for the LTE to automatically set the <b>Interval</b> and <b>Max. Failure Time</b>.</li> <li>• Select <b>User-defined</b> to define the <b>Interval</b> and <b>Max. Failure Time</b>. The default values is <b>30 seconds</b> and <b>6 Times</b> respectively.</li> <li>• Select <b>Disable</b> to disable LCP Echo Type.</li> </ul>
Service Port	<ul style="list-style-type: none"> <li>• Select <b>Auto</b> for the LTE to automatically define the service port for the L2TP tunnel to use.</li> <li>• Select <b>1701 (for Cisco)</b> for the LTE to use port 1701 to connect to the Cisco L2TP server.</li> <li>• Select <b>User-defined</b> to define the service port (1~65535) for the L2TP tunnel to use.</li> </ul>
Back	Click <b>Back</b> to return to the previous screen without saving.
Cancel	Click <b>Cancel</b> to exit this screen without saving.
Apply	Click <b>Apply</b> to save your changes back to the LTE.

## 18.5 GRE

GRE 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 and another router over an Internet protocol network.

Figure 72 GRE Tunnel Example



Click **Configuration > Application > VPN > GRE** to open the following screen.

Figure 73 Configuration &gt; Application &gt; VPN &gt; GRE

The following table describes the labels in this screen.

Table 52 Configuration &gt; Application &gt; VPN &gt; GRE

LABEL	DESCRIPTION
Configuration	
GRE Tunnel	Select this to enable GRE tunneling on the LTE.
Max. Concurrent GRE Tunnels	Enter the maximum number of ongoing GRE tunnels allowed in the LTE.
Tunnel List	
Add	Click this to add a new GRE tunnel.
Delete	Click this to remove an existing GRE tunnel.
ID	This field is a sequential value, and it is not associated with a specific GRE tunnel.
Name	This displays the descriptive name of the GRE tunnel.
Enable	This displays if the GRE tunnel if is activated or not.
Remote Subnet	This displays the remote network IP to which this interface tunnels traffic.

Table 52 Configuration &gt; Application &gt; VPN &gt; GRE (continued)

LABEL	DESCRIPTION
Tunnel IP	This displays the IP address to use as the source address for the packets this WAN IP tunnels to the remote gateway. The remote gateway sends traffic to this IP address.
Remote IP	This displays the IP address of the remote client to which this WAN IP tunnels traffic.
MTU	This displays the Maximum Transmission Unit (MTU). This is the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the LTE divides it into smaller fragments.
Key	This displays the key for the GRE connection, a value between 0 ~ 9999999999. The GRE tunnel will request this key for packet transportation. The client needs to enter this key to authenticate the source of the packet.
TTL	This displays the Time To Live (TTL). This is a time limiter that defines the lifetime of a packet. Every time the packet is forwarded, it will reduce the TTL value by 1, if this time limiter reaches 0, the packet will be discarded. The default value is 255.
Keep-alive	This displays how often (in seconds) the LTE sends pings the IP to keep the GRE tunnel up.
Actions	Click the <b>Edit</b> button to modify an L2TP client 's configurations. Select it and click <b>Delete</b> to remove it.
Cancel	Click <b>Cancel</b> to exit this screen without saving.
Apply	Click <b>Apply</b> to save your changes back to the LTE.

## 18.5.1 Add GRE

After you enabled **GRE Tunnel** click add to open the following screen, and create a GRE tunnel.

Figure 74 GRE: Add

The screenshot shows the 'GRE: Add' configuration screen. At the top, there are tabs for 'L2TP Server', 'L2TP Client', 'GRE' (selected), and 'VPN Passthrough'. Below the tabs, the title 'GRE tunnel' is displayed. The configuration fields are as follows:

- Name:** A text input field.
- Enable:** A checkbox that is currently unchecked.
- Remote IP:** A text input field.
- TTL:** A text input field containing the value '255'.
- Key:** A text input field with '(Optional)' to its right.
- Keep Alive:** A checkbox that is unchecked, followed by the text 'Enable'.
- Ping IP:** A dropdown menu with a downward arrow.
- Interval:** A text input field containing '5', with '(seconds)' in red text below it.
- Tunnel IP:** A text input field containing 'IP:' followed by a text input field, and a dropdown menu containing 'MASK: -- select one --' with '(Optional)' to its right.
- MTU:** A text input field.
- Remote Subnet:** A text input field.

At the bottom of the screen, there are three buttons: 'Back' (grey), 'Cancel' (grey), and 'Apply' (blue).

The following table describes the labels in this screen.

Table 53 GRE: Add

LABEL	DESCRIPTION
Name	Enter a name for this GRE tunnel, this name must be 1~9 characters long.
Enable	Select this to enable the GRE tunnel.
Remote IP	Specify the IP address of the remote gateway to which this interface tunnels traffic.
TTL	Specify the Time To Live (TTL). This is a time limiter that defines the lifetime of a packet. Every time the packet is forwarded, it will reduce the TTL value by 1, if this time limiter reaches 0, the packet will be discarded. The default value is 255.
Key	This displays the key for the GRE connection, a value between 0 ~ 9999999999. The GRE tunnel will request this key for packet transportation. The client needs to enter this key to authenticate the source of the packet.
Keep Alive	The LTE can send periodic keep alive frames, so the GRE tunnel does not go down. Specify how often these frames are sent in seconds to keep the GRE tunnel up.
Tunnel IP	Specify the IP address to use as the source address for the packets this interface tunnels to the remote gateway. The remote gateway sends traffic to this IP address.
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the LTE divides it into smaller fragments. The default value is 2000.
Remote Subnet	Enter the remote subnet mask to which this interface tunnels traffic.
Back	Click <b>Back</b> to return to the previous screen without saving.
Cancel	Click <b>Cancel</b> to exit this screen without saving.
Apply	Click <b>Apply</b> to save your changes back to the LTE.

## 18.6 VPN Passthrough

Use this screen to allow VPN traffic through the LTE. Click **Configuration > Application > VPN > VPN Passthrough** to open the following screen.

Figure 75 Configuration &gt; Application &gt; VPN &gt; VPN Passthrough



L2TP Server   L2TP Client   GRE   **VPN Passthrough**

**VPN Passthrough Enable**

VPN Passthrough Enable :  IPSec  PPTP  L2TP

Reset   Apply

The following table describes the labels in this screen.

Table 54 Configuration > Application > VPN > VPN Passthrough

LABEL	DESCRIPTION
VPN Passthrough Enable	
IPSec	Select this check box to turn on the IPSec ALG (Application Layer Gateway) on the LTE to detect IPSec traffic and help build IPSec sessions through the LTE's if NAT is enabled.
PPTP	Enable this to turn on the PPTP ALG on the LTE to detect PPTP traffic and help build PPTP sessions through the LTE if NAT is enabled.
L2TP	Enable this to turn on the L2TP ALG on the LTE to detect L2TP traffic and help build L2TP sessions through the LTE if NAT is enabled.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.
Apply	Click <b>Apply</b> to save your changes.



# CHAPTER 19

## SMS

### 19.1 Overview

SMS (Short Message Service) allows you to send and view the text messages that the LTE received from mobile devices or the service provider.

When the SMS box is full the LTE will begin to delete older entries as it adds new ones.

#### 19.1.1 What You Can Do in this Chapter

Use the **SMS** screen to send new messages and view messages received on the LTE ([Section 19.2 on page 129](#)).

### 19.2 SMS Configuration

Use this screen to send text messages using the LTE and view messages received. To access this screen, click **Configuration > Application > SMS**.

Figure 76 Configuration &gt; Application &gt; SMS

The screenshot displays the SMS configuration page. At the top, there are three tabs: 'SMS Summary', 'New SMS', and 'SMS Inbox'. The 'SMS Summary' section shows statistics: Unread SMS (0), Received SMS (3), and Remaining SMS (0). The 'New SMS' section includes a 'Send' button, a 'Receivers' input field with a hint '(Use '+' for International Format and ';' to Compose Multiple Receivers)', a 'Text Message' text area, and a 'Length of Current Input : 0' indicator. The 'SMS Inbox List' section features 'Refresh', 'Delete', and 'Close' buttons. Below is a table of received messages with columns for ID, From Phone Number, Timestamp, SMS Text Preview, and Actions (Detail, Reply, Forward). At the bottom right, there are 'Refresh' and 'Apply' buttons.

The following table describes the labels in this screen.

Table 55 Configuration &gt; Application &gt; SMS

LABEL	DESCRIPTION
SMS Summary	Click <b>New SMS</b> to display the <b>New SMS</b> section. Click <b>SMS Inbox</b> to display only the <b>SMS Inbox List</b> .
Unread SMS	This shows the number of unread text messages in the SMS in-box.
Received SMS	This shows the number of text messages that the LTE received.
Remaining SMS	This shows the number of text messages that are to be sent.
New SMS	
Send	Click this button to send the new message.
Receivers	Enter the phone number to which you want to send a text message.

Table 55 Configuration &gt; Application &gt; SMS (continued)

LABEL	DESCRIPTION
Text Message	Enter the message content. You can type up to 160 characters in one message. If the message exceeds 160 characters, more than one SMS will be sent. The maximum number of SMS that can be sent is 20 (1400 characters total).
Result	This shows whether the message is sent successfully.
SMS Inbox List	
Refresh	Click this button to update the list.
Delete	Click this button to remove messages from the list.
Close	Click this button to hide the <b>SMS Inbox List</b> .
ID	This field displays the index number of the message.
From Phone Number	This field displays the mobile phone number from which the message is sent.
Timestamp	This field displays the date and time the message was received.
SMS Text Preview	This field displays the content of the message.
Actions	<p>Click <b>Detail</b> to view more details about the message.</p> <p>Click <b>Reply</b> to answer this message.</p> <p>Click <b>Forward</b> to send this message to a different number.</p>

# CHAPTER 20

## Voice Call

### 20.1 Overview

4G only supports all-IP-based packet-switched telephony services. When Voice service is enabled, the LTE supports Circuit Switched FallBack (CSFB) to deliver/receive circuit-switched voice calls and text messages via a 3G mobile network and then goes back to the 4G LTE network to transmit data packets.

With the voice service, users do not need a SIP account and SIP server to make phone calls over the Internet.

#### 20.1.1 What You Can Do in this Chapter

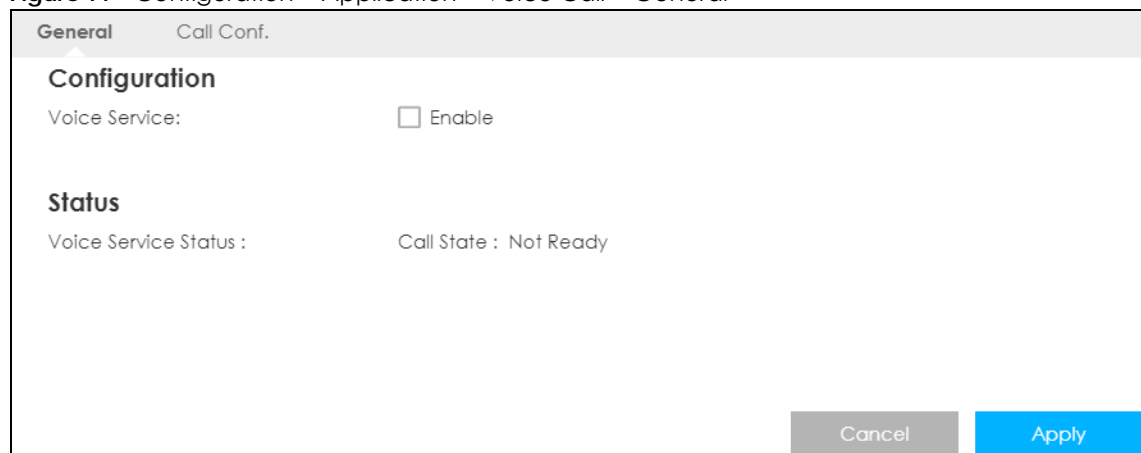
These screens allow you to configure your LTE to make phone calls over the Internet and your regular phone line, and to set up the phone you connect to the LTE.

- Use the **General** screen to enable voice calls on the LTE ([Section 20.2 on page 132](#)).
- Use the **Call Conf.** screen to maintain rules for handling incoming calls ([Section 20.3 on page 133](#)).

### 20.2 General Settings

Use this screen to enable voice service on the LTE. To access this screen, click **Configuration > Application > Voice Call > General**.

**Figure 77** Configuration > Application > Voice Call > General



The following table describes the labels in this screen.

Table 56 Configuration > Application > Voice Call > General

LABEL	DESCRIPTION
Configuration	
Voice Service	Select <b>Enable</b> to activate voice calls on the LTE.
Status	
Voice Service Status	<p>This shows the current state of the phone call.</p> <ul style="list-style-type: none"> <li><b>ready:</b> Voice service is enabled and the connection is up.</li> <li><b>not ready:</b> Voice service is disabled and the 3G/LTE connection is down.</li> <li><b>busy:</b> There is a voice call in progress or the callee's line is busy.</li> <li><b>ringing:</b> The phone is ringing for an incoming voice call.</li> <li><b>dialing:</b> The callee's phone is ringing.</li> <li><b>off hook:</b> The callee hung up or your phone was left off the hook.</li> </ul> <p>N/A means Voice service is not available.</p>
Apply	Click <b>Apply</b> to save the settings.
Cancel	Click <b>Cancel</b> to start configuring this screen again.

## 20.3 Call Configuration

Use this screen to maintain rules for handling incoming calls. To access this screen, click **Configuration > Application > Voice Call > Call Conf.**

Figure 78 Configuration > Application > Voice Call > Call Conf.

General Call Conf.

### Call Configuration

Call Waiting :  Enable

Call Forwarding :  Enable

### Call Forwarding Rule

ID	Scenario	Phone Number	Rule
1	All Calls		<input type="checkbox"/> Enable
2	No Answer		<input type="checkbox"/> Enable
3	Unreachable		<input type="checkbox"/> Enable
4	Busy		<input type="checkbox"/> Enable

Cancel Apply

The following table describes the labels in this screen.

Table 57 Configuration > Application > Voice Call > Call Conf.

LABEL	DESCRIPTION
Call Configuration	
Call Waiting	Select <b>Enable</b> to place a call on hold while you answer another incoming call on the same telephone number.

Table 57 Configuration &gt; Application &gt; Voice Call &gt; Call Conf. (continued)

LABEL	DESCRIPTION
Call Forwarding	Select <b>Enable</b> to forward incoming calls according to the call forwarding rules. Clear the check box if you do not want the LTE to forward any incoming calls.
Call Forwarding Rule	
ID	This is the index number of the call forwarding rule.
Scenario	<p>This shows the situations in which you want to forward incoming calls.</p> <p><b>All Calls:</b> the LTE forwards all incoming calls to the specified phone number.</p> <p><b>No Answer:</b> the LTE forwards incoming calls to the specified phone number if the call is unanswered.</p> <p><b>Unreachable:</b> the LTE forwards incoming calls to the specified phone number if the phone is turned off or lost its signal.</p> <p><b>Busy:</b> the LTE forwards incoming calls to the specified phone number if the phone port is busy.</p>
Phone Number	Enter the phone number to which you want to forward incoming calls.
Rule	<p>Select to turn on or turn off the rule.</p> <p>Note: If you enable the <b>All Calls</b> rule, other rules are not configurable/applicable.</p>
Cancel	Click this to set every field in this screen to its last-saved value.
Apply	Click this to save your changes and to apply them to the LTE.

# CHAPTER 21

## MGMT Interface

### 21.1 Overview

This chapter explains how to configure the LTE remote management. Remote Management allows you to manage your LTE from a remote location.

### 21.2 What You Can Do

- Use the **Local MGMT** screen to configure settings for HTTP or HTTPS access to the LTE and how to login and access user screens look ([Section 21.4 on page 135](#)).
- Use the **Remote Management** screen to through which interfaces users can use which services to manage the LTE ([Section 21.5 on page 137](#)).

### 21.3 What You Need To Know

Remote management over LAN or WAN will not work when:

- 1 The IP address in the Secured Client IP Address field ([Section 21.4 on page 135](#)) does not match the client IP address. If it does not match, the LTE will disconnect the session immediately.
- 2 There is a firewall rule that blocks it.

#### 21.3.1 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The LTE automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. You can change the timeout period in the **Maintenance > General** screen.

### 21.4 Local MGMT

To change your LTE's remote management settings, click **Configuration > Management > MGMT Interface** to open the **Local MGMT** screen.

Note: You must enable the remote management service in the **Configuration > Management > MGMT Interface > Local MGMT** screen for the settings in the **WWW** screen to take effect.

**Figure 79** Configuration > Management > MGMT Interface > Local MGMT

The screenshot shows the 'Local MGMT' configuration page. It features two tabs: 'Local MGMT' and 'Remote MGMT'. The page is organized into four sections, each with an 'Enable' checkbox and a 'Port' input field:

- HTTPS:** Port is set to 443.
- HTTP:** Port is set to 80.
- SSH:** The 'Enable' checkbox is unchecked, and the port is set to 22.
- Telnet:** The 'Enable' checkbox is unchecked, and the port is set to 23.

At the bottom right of the form, there are two buttons: a grey 'Cancel' button and a blue 'Apply' button.

The following table describes the labels in this screen.

**Table 58** Configuration > Management > MGMT Interface > Local MGMT

LABEL	DESCRIPTION
HTTPS	
Port	You may change the server port number for a HTTPS service if needed. However you must use the same port number in order to use that service for remote management.
HTTP	
Port	You may change the server port number for a HTTP service if needed. However you must use the same port number in order to use that service for remote management.
SSH	
Enable	Select this to enable Secure SHell (SSH) to securely access the LTE CLI interface. SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between hosts over an unsecured network.
Port	You may change the server port number for the SSH service if needed. However you must use the same port number in order to use that service for remote management.
Telnet	
Enable	Select this to allow a device to access the LTE CLI using this service.
Port	You may change the server port number for the Telnet service if needed. However you must use the same port number in order to use that service for remote management.
Cancel	Click <b>Cancel</b> to return the screen to its last-saved settings.
Apply	Click <b>Apply</b> to save your changes back to the LTE.



## 21.5 Remote MGMT

Use this screen to configure through which IP address the LTE can be accessed. You can also specify the port numbers the IP addresses must use to connect to the LTE. Click **Configuration > Management > MGMT Interface > Remote MGMT** to open the following screen.

Note: The firewall will be disabled when remote management is enabled. To activate the firewall, you'll need to create a new firewall rule to allow the remote management traffic to come in from the WAN side.

**Figure 80** Configuration > Management > MGMT Interface > Remote MGMT

The following table describes the labels in this screen.

**Table 59** Configuration > Management > MGMT Interface > Remote MGMT

LABEL	DESCRIPTION
HTTPS	
Enable	Select this check box to allow access to the LTE Device from the IP address and activate the HTTPS settings you've made in the <b>Local MGMT</b> screen.
IP address	This is the IP address of a computer that may use to access the LTE.
Netmask	This is the subnet mask identifying a computer that may access remotely to the LTE.
Port	This is the port number that the computer must use to access the LTE. If the HTTP Port number was changed to 8080 in the <b>Configuration &gt; Management &gt; MGMT Interface &gt; Local MGMT</b> screen, then this computer should use the same number. For example http://1.1.1.1:8080 where 1.1.1.1 is the IP address of the LTE.
SSH	
Enable	Select this to allow the computer with the IP address that matches the IP address to access the LTE CLI using SSH service.
IP address	Specify the IP address identifying the computer that can access the LTE using SSH service.
Netmask	This is the subnet mask of the computer that may access using SSH service.
Port	This is the port number that the computer must use to access the LTE.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.
Apply	Click <b>Apply</b> to save your changes back to the LTE.

# CHAPTER 22

# Bandwidth Management

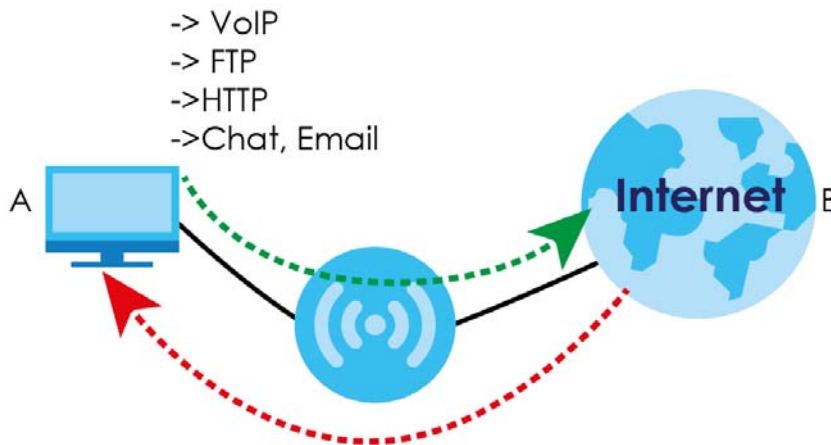
## 22.1 Overview

This chapter contains information about configuring bandwidth management and editing rules.

Zyxel's Bandwidth Management allows you to specify bandwidth management rules based on an application.

In the figure below, uplink traffic goes from the LAN device (A) to the WAN device (B). Bandwidth management is applied before sending the packets out to the WAN. Downlink traffic comes back from the WAN device (B) to the LAN device (A). Bandwidth management is applied before sending the traffic out to LAN.

**Figure 81** Bandwidth Management Example



You can allocate specific amounts of bandwidth capacity (bandwidth budgets) to individual applications (like VoIP, Web, FTP, and Email for example).

## 22.2 What You Can Do

Use the **General** screen to enable bandwidth management and assign bandwidth values as well as configure bandwidth managements rule for the services and applications ([Section 22.4 on page 139](#)).

## 22.3 What You Need To Know

The sum of the bandwidth allotments that apply to the WAN interface (LAN to WAN, WLAN to WAN) must be less than or equal to the upstream bandwidth that you configure in the **Bandwidth Management > General** screen ([Section 22.4 on page 139](#)).

The sum of the bandwidth allotments that apply to the LAN interface (WAN to LAN, WAN to WLAN) must be less than or equal to the downstream bandwidth that you configure in the **Bandwidth Management > General** screen ([Section 22.4 on page 139](#)).

## 22.4 General Settings

Use this screen to have the LTE apply bandwidth management, configure bandwidth management rules for the pre-defined services or applications, as well as configure bandwidth management rule for other services or applications that are not on the pre-defined list of LTE.

Click **Configuration > Management > Bandwidth MGMT** to open the bandwidth management **General** screen.

**Figure 82** Configuration > Management > Bandwidth MGMT > General

The following table describes the labels in this screen.

**Table 60** Configuration > Management > Bandwidth MGMT > General

LABEL	DESCRIPTION
Configuration	
QoS Types	Select the <b>Enable</b> check box to turn on QoS to improve your network performance.
System Resource Configuration	
Type of System Queue	Defines the system queues that are available for the QoS settings. The supported type of system queues are <b>Bandwidth Queue</b> and <b>Priority Queue</b> . The value ranges from 1 ~ 6.
WAN Interface	Select the LTE's interface through which traffic in this shaper applies.

Table 60 Configuration &gt; Management &gt; Bandwidth MGMT &gt; General (continued)

LABEL	DESCRIPTION
WAN Interface Resource	
Bandwidth of Upstream	Specify the total amount of bandwidth that you want to dedicate to uplink traffic. The recommendation is to set this to match the actual upstream data rate.  This is traffic from LAN/WLAN to WAN.
Bandwidth of Downstream	Specify the total amount of bandwidth that you want to dedicate to downlink traffic. The recommendation is to set this to match the actual downstream data rate.  This is traffic from WAN to LAN/WLAN.
Total Connections Sessions	Specify the total connection sessions of the selected WAN.
QoS Rule List	
Add	Click this button to create a new queue entry.
Delete	Click this button to delete the rule.
Clear	Click this button to remove all bandwidth management rules.
Restart	Click this button to begin configuring this screen afresh.
Interface	This field displays the LTE's interface through which traffic in this shaper applies.
Group	This field displays the IP address or a range of IP addresses of the destination computer for whom this rule applies.
Service Resource	This field displays the protocol and port used for the service.
Control Function	This field displays whether the maximum/minimum bandwidth allowed or a priority level is specified in the rule.
Direction	These read-only labels represent the physical interfaces. Bandwidth management applies to all traffic flowing out of the router through the interface, regardless of the traffic's source.
Sharing Method	This field displays the bandwidth allocation.
Time Schedule	This field displays the time schedule you set for this rule.
Enable	This field indicates whether the rule is active or not.
Actions	Click the <b>Edit</b> icon to edit the queue.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Apply	Click <b>Apply</b> to save your customized settings.

### 22.4.1 Add Bandwidth Management Rule

If you want to create a new bandwidth management rule for a service or application, click the **Add New Rule** icon in the **Advanced** screen. The following screen displays.

Figure 83 Bandwidth Management Rule Configuration

The screenshot shows a configuration window for a QoS rule. The 'General' tab is selected. The configuration is as follows:

- Interface: All WANs
- Group: Src. MAC Address
- Service: All
- Resource: Bandwidth
- Control Function: Set MINR & MAXR
- QoS Direction: Outbound
- Time Schedule: [0] Always
- Rule Enable:  Enable

Buttons: Back, Cancel, Apply

The following table describes the labels in this screen.

Table 61 Bandwidth Management Rule Configuration

LABEL	DESCRIPTION
QoS Rule Configuration	
Interface	Select the LTE's interface through which traffic in this shaper applies.
Group	Select to use the IP address or MAC address of the destination computer for whom this rule applies.
Service	Specify the service type of traffics that have to be applied with the QoS rule. It can be <b>All</b> , <b>DSCP</b> , <b>TOS</b> , <b>User-defined Service</b> , or <b>Well-known Service</b> . <ul style="list-style-type: none"> <li>Select <b>All</b> for all packets.</li> <li>Select <b>DSCP</b> for DSCP-type packets only.</li> <li>Select <b>TOS</b> for TOS-type packets only. You have to select a service type (Minimize-Cost, Maximize-Reliability, Maximize-Throughput, or Minimize-Delay) from the drop-down list as well.</li> <li>Select <b>User-defined Service</b> for user-defined packets only. You have to define the port range and protocol as well.</li> <li>Select <b>Well-known Service</b> for specific application packets only. You have to select the required service from the drop-down list as well.</li> </ul>
Resource	Specify the Resource Type and corresponding Control function for the QoS rule. The available Resource options are <b>Bandwidth</b> , <b>Connection Sessions</b> , <b>Priority Queues</b> , and <b>DiffServ Code Points</b> . <ul style="list-style-type: none"> <li><b>Bandwidth:</b> Select <b>Bandwidth</b> as the resource type for the QoS Rule, and you have to assign the minimum rate, maximum rate and rate unit as the bandwidth settings in the Control Function / Set MINR &amp; MAXR field.</li> <li><b>Connection Sessions:</b> Select <b>Connection Sessions</b> as the resource type for the QoS Rule, and you have to assign supported session number in the <b>Control Function / Set Session Limitation</b> field.</li> <li><b>Priority Queues:</b> Select <b>Priority Queues</b> as the resource type for the QoS Rule, and you have to specify a priority queue in the <b>Control Function/ Set Priority</b> field.</li> <li><b>DiffServ Code Points:</b> Select <b>DiffServ Code Points</b> as the resource type for the QoS Rule, and you have to select a DSCP marking from the <b>Control Function / DSCP Marking</b> drop-down list.</li> </ul>
Control Function	Select <b>Maximum Bandwidth</b> or <b>Minimum Bandwidth</b> and specify the maximum or minimum bandwidth allowed for the rule in <b>Kbps</b> (kilobytes per second) or <b>Mbps</b> (megabytes per second).

Table 61 Bandwidth Management Rule Configuration (continued)

LABEL	DESCRIPTION
QoS Direction	Specify the traffic flow direction for the packets to apply the QoS rule. It can be <b>Outbound</b> , <b>Inbound</b> , or <b>Both</b> . <ul style="list-style-type: none"> <li>• <b>Outbound</b>: Select <b>Outbound</b> to prioritize the traffics going to the Internet via the specified interface. Under such situation, the hosts specified in the <b>Group</b> field is a source group.</li> <li>• <b>Inbound</b>: Select <b>Inbound</b> to prioritize the traffics coming from the Internet via the specified interface. Under such situation, the hosts specified in the Group field is a destination group.</li> <li>• <b>Both</b>: Select <b>Both</b> to prioritize the traffics passing through the specified interface, both <b>Inbound</b> and <b>Outbound</b> are considered. Under such situation, the hosts specified in the <b>Group</b> field can be a source or destination group.</li> </ul>
Time Schedule	Apply <b>Time Schedule</b> to this rule; otherwise leave it as <b>(0) Always</b> .
Rule Enable	Select this check box to turn on the bandwidth management rule.
Back	Click <b>Back</b> to return to the previous screen.
Cancel	Click <b>Cancel</b> to exit this screen without saving.
Apply	Click <b>Apply</b> to save your customized settings.

See [Appendix B on page 178](#) for commonly used services and port numbers.

# CHAPTER 23

## Universal Plug-and-Play (UPnP)

### 23.1 Overview

This chapter introduces the UPnP feature in the Web Configurator.

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.

### 23.2 What You Need to Know

UPnP hardware is identified as an icon in the Network Connections folder (Windows 7). 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.

#### 23.2.1 NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the NAT chapter for more information on NAT.

#### 23.2.2 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 allows multicast messages on the LAN only.

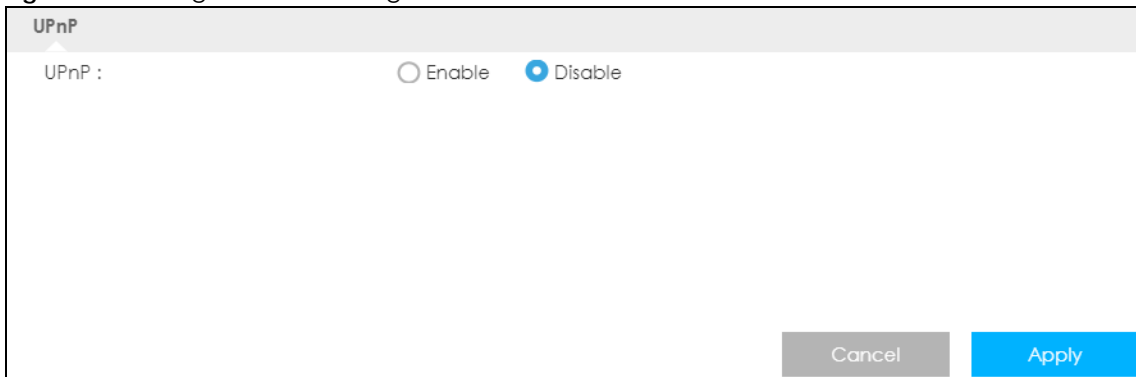
All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

## 23.3 UPnP Settings

Use this screen to enable UPnP on your LTE.

Click **Configuration > Management > UPnP** to display the screen shown next.

**Figure 84** Configuration > Management > UPnP



The following table describes the fields in this screen.

**Table 62** Configuration > Management > UPnP

LABEL	DESCRIPTION
UPnP	Select <b>Enable</b> to activate UPnP. Be aware that anyone could use a UPnP application to open the Web Configurator's login screen without entering the LTE's IP address (although you must still enter the password to access the Web Configurator).
Apply	Click <b>Apply</b> to save the setting to the LTE.
Cancel	Click <b>Cancel</b> to return to the previously saved settings.

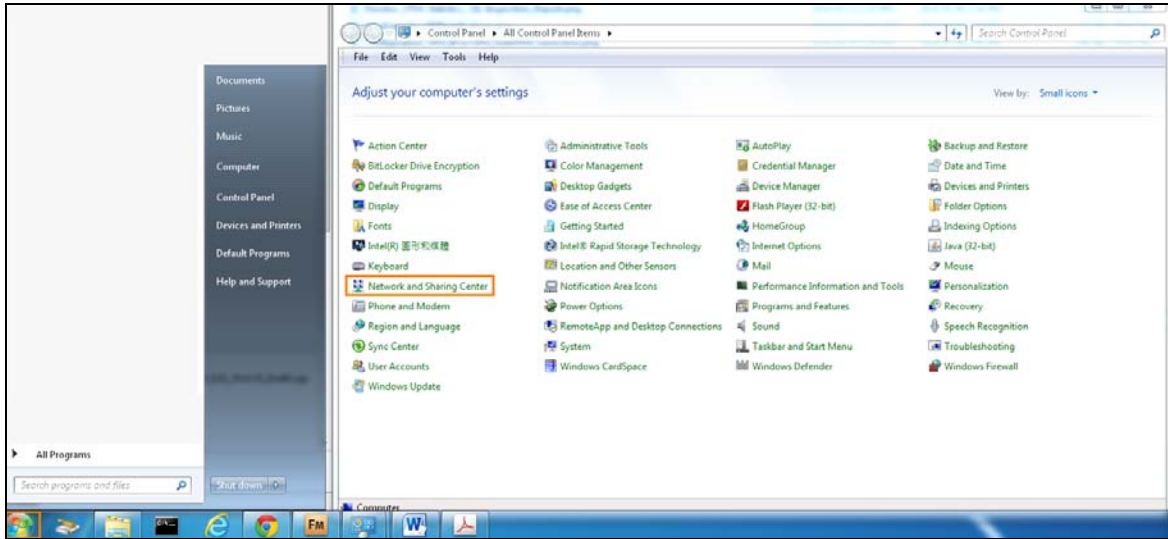
## 23.4 Turn on UPnP in Windows 7 Example

This section shows you how to use the UPnP feature in Windows 7. UPnP server is installed in Windows 7. Activate UPnP on the LTE by clicking **Network Setting > Home Networking > UPnP**.

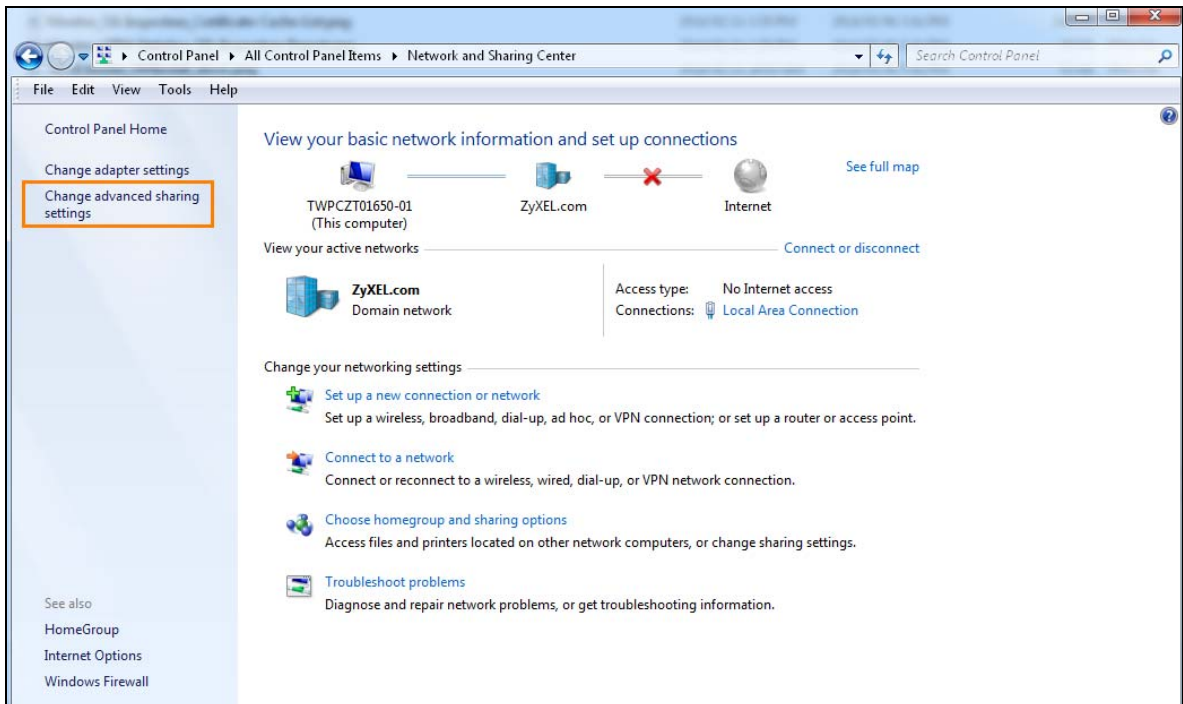
Make sure the computer is connected to the LAN port of the LTE. Turn on your computer and the LTE.

- 1 Click the start icon, **Control Panel** and then the **Network and Sharing Center**.

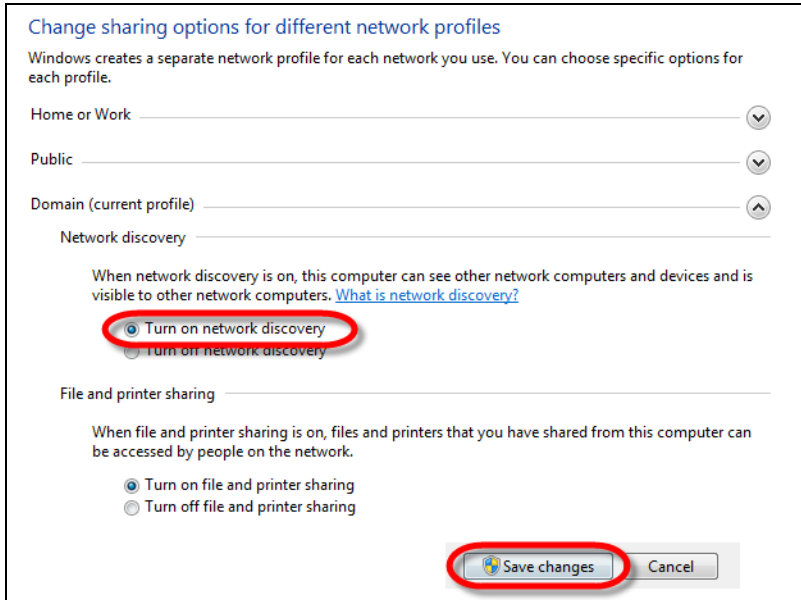




2 Click **Change Advanced Sharing Settings**.



3 Select **Turn on network discovery** and click **Save Changes**. Network discovery allows your computer to find other computers and devices on the network and other computers on the network to find your computer. This makes it easier to share files and printers.



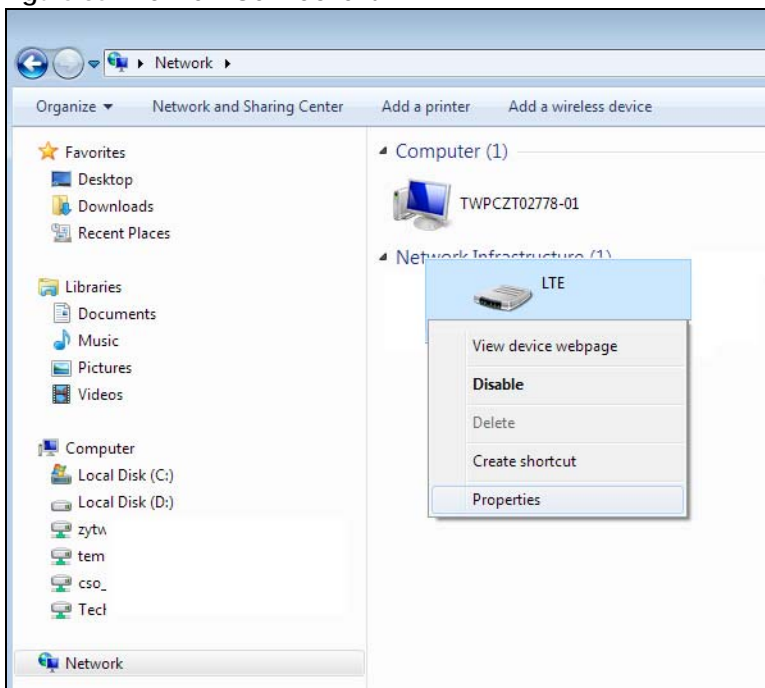
### 23.4.1 Auto-discover Your UPnP-enabled Network Device

Before you follow these steps, make sure you already have UPnP activated on the LTE and in your computer.

Make sure your computer is connected to the LAN port of the LTE.

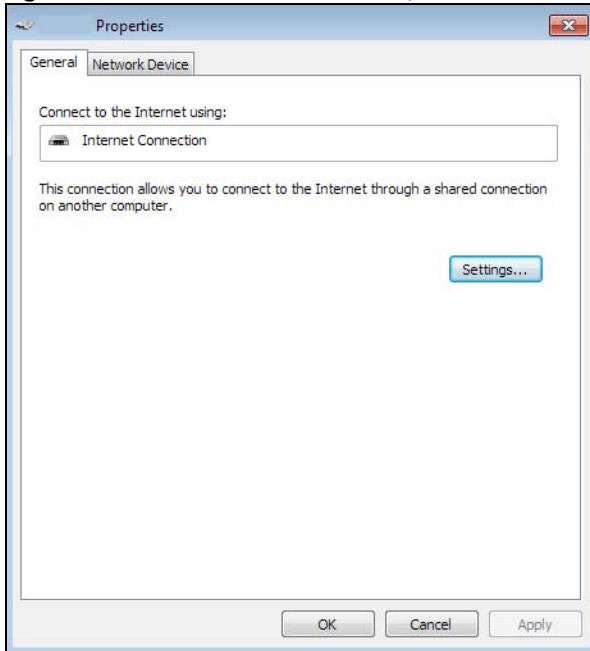
- 1 Open **Windows Explorer** and click **Network**.
- 2 Right-click the LTE icon and select **Properties**.

**Figure 85** Network Connections



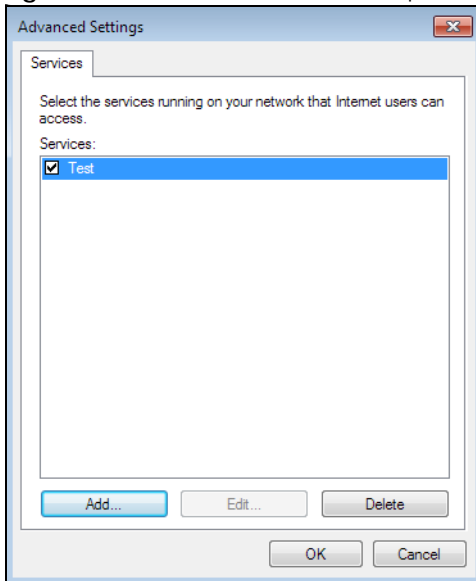
- 3 In the **Internet Connection Properties** window, click **Settings** to see port mappings.

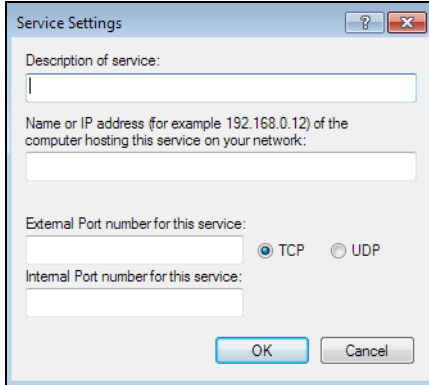
**Figure 86** Internet Connection Properties



- 4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

**Figure 87** Internet Connection Properties: Advanced Settings



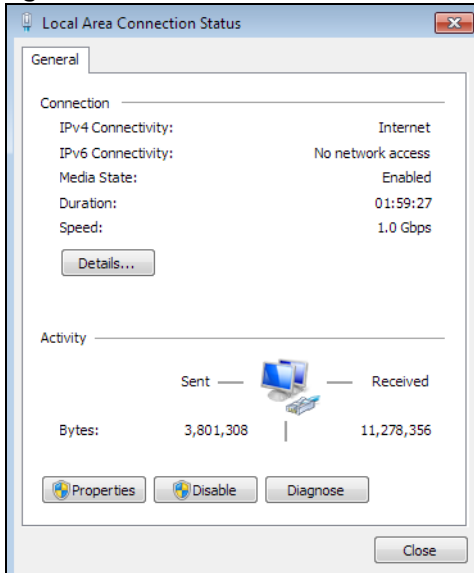
**Figure 88** Internet Connection Properties: Advanced Settings: Add

Note: When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

- 5 Click **OK**. Check the network icon on the system tray to see your Internet connection status.

**Figure 89** System Tray Icon

- 6 To see more details about your current Internet connection status, right click the network icon in the system tray and click **Open Network and Sharing Center**. Click **Local Area Network**.

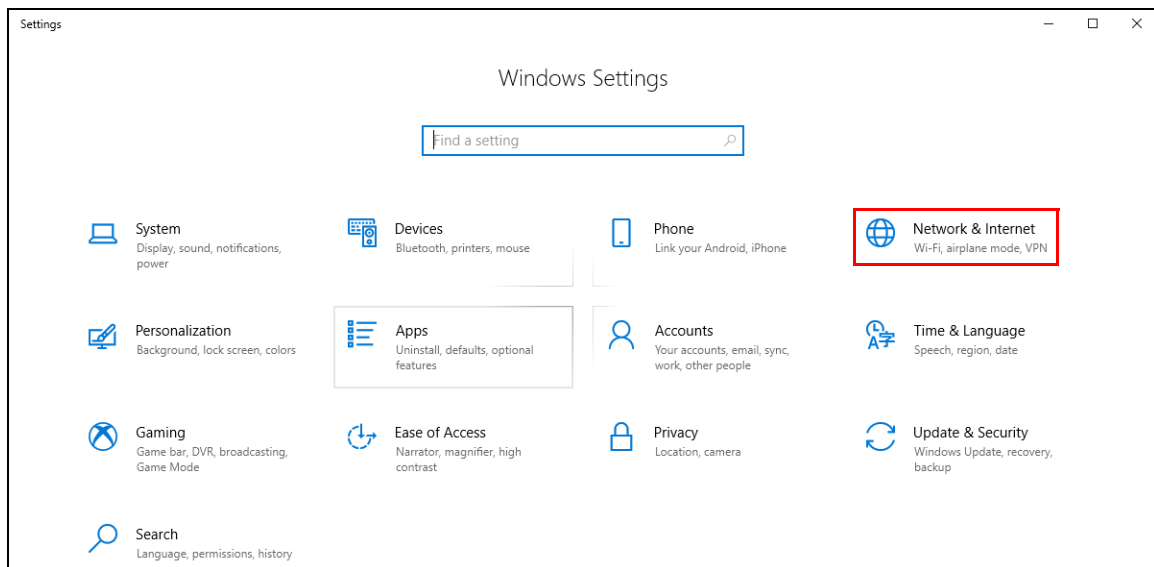
**Figure 90** Internet Connection Status

## 23.5 Turn on UPnP in Windows 10 Example

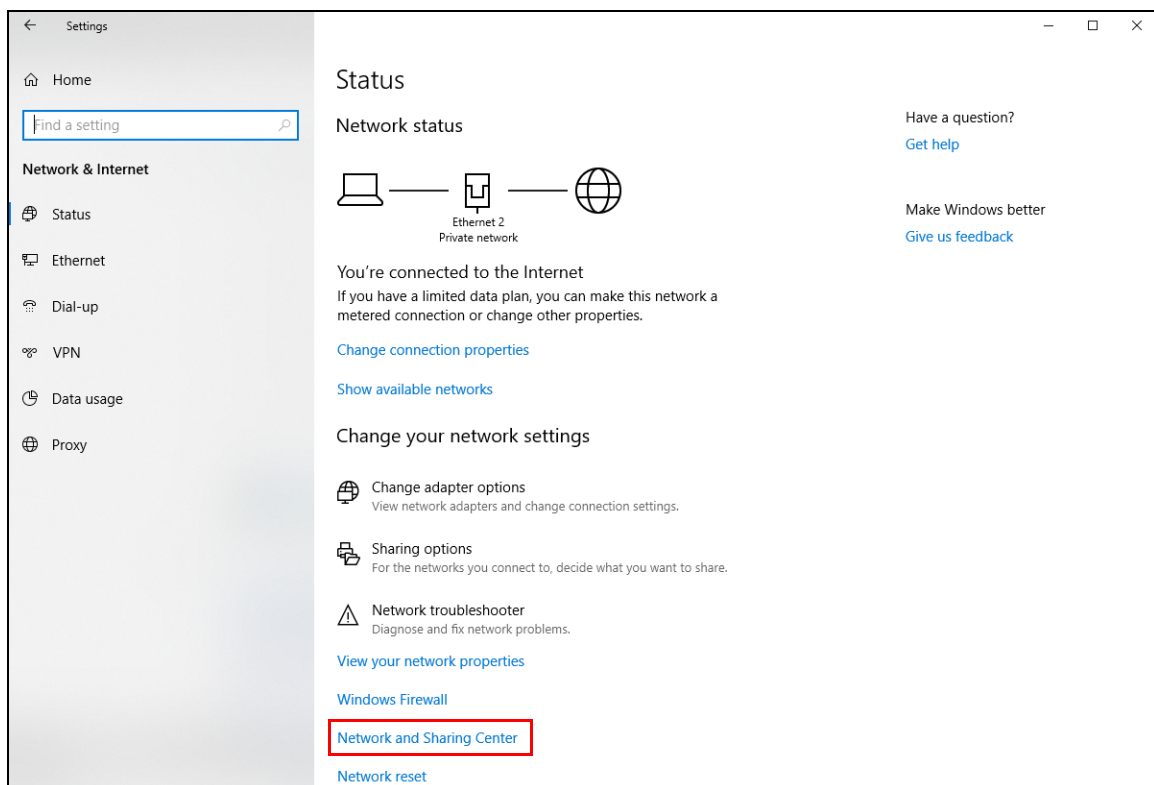
This section shows you how to use the UPnP feature in Windows 10. UPnP server is installed in Windows 10. Activate UPnP on the LTE by clicking **Network Setting > Home Networking > UPnP**.

Make sure the computer is connected to the LAN port of the LTE. Turn on your computer and the LTE.

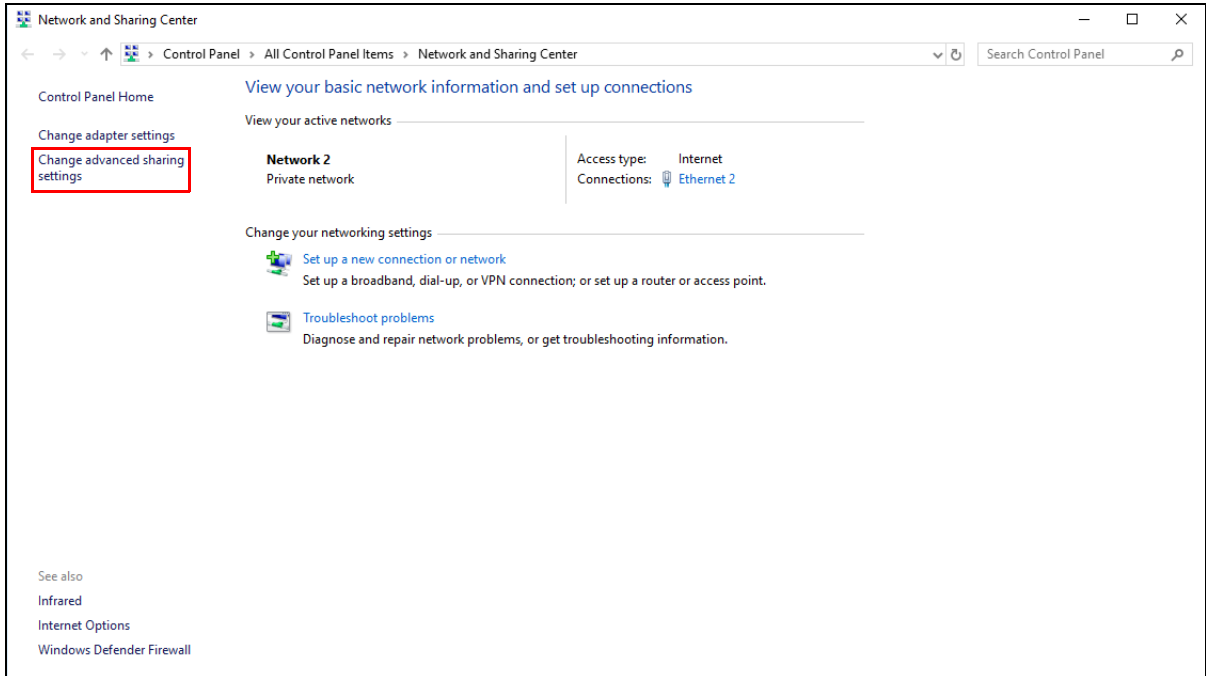
- 1 Click the start icon, **Settings** and then **Network & Internet**.



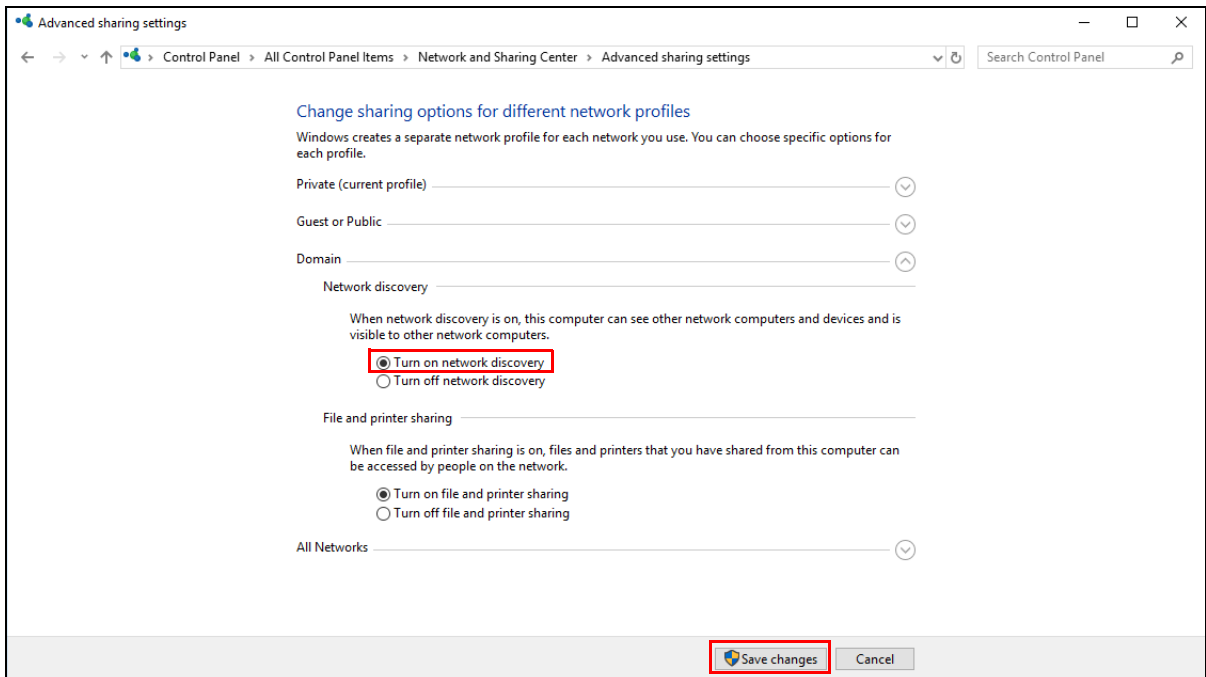
- 2 Click **Network and Sharing Center**.



- 3 Click **Change advanced sharing settings**.



- 4 Under **Domain**, select **Turn on network discovery** and click **Save Changes**. Network discovery allows your computer to find other computers and devices on the network and other computers on the network to find your computer. This makes it easier to share files and printers.



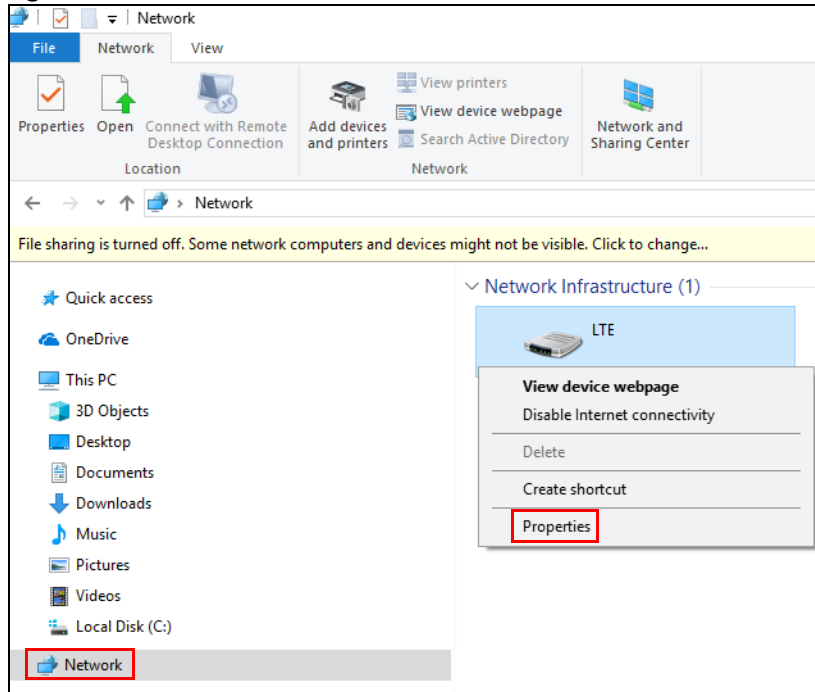
### 23.5.1 Auto-discover Your UPnP-enabled Network Device

Before you follow these steps, make sure you already have UPnP activated on the LTE and in your computer.

Make sure your computer is connected to the LAN port of the LTE.

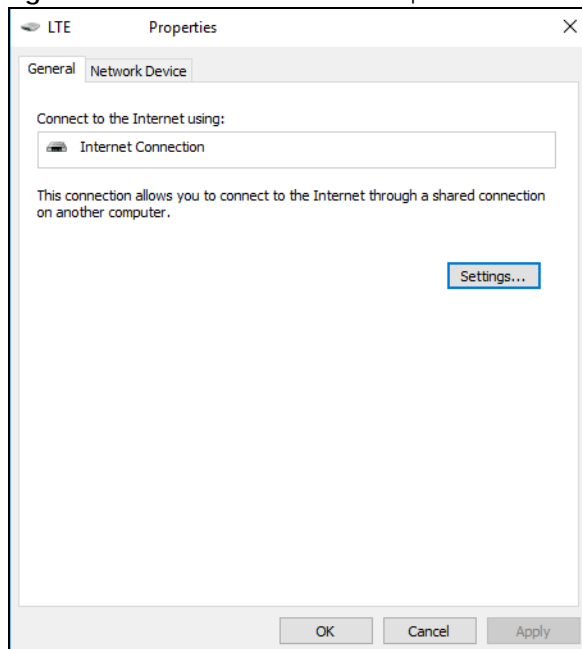
- 1 Open **File Explorer** and click **Network**.
- 2 Right-click the LTE icon and select **Properties**.

**Figure 91** Network Connections

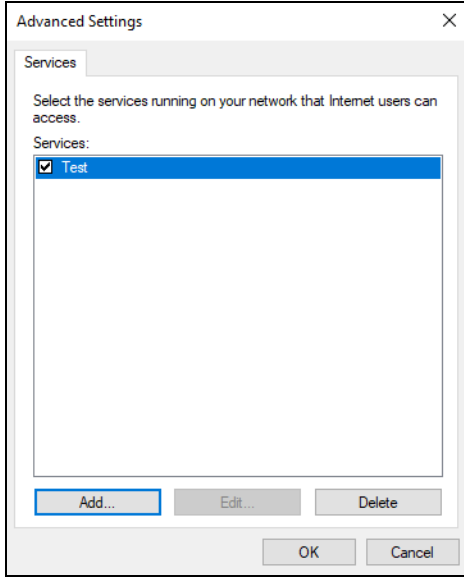
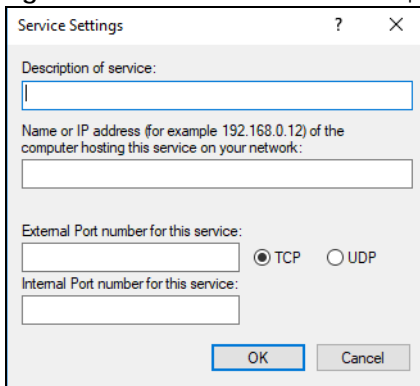


- 3 In the **Internet Connection Properties** window, click **Settings** to see port mappings.

**Figure 92** Internet Connection Properties

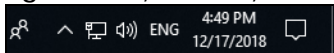


- 4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

**Figure 93** Internet Connection Properties: Advanced Settings**Figure 94** Internet Connection Properties: Advanced Settings: Add

Note: When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

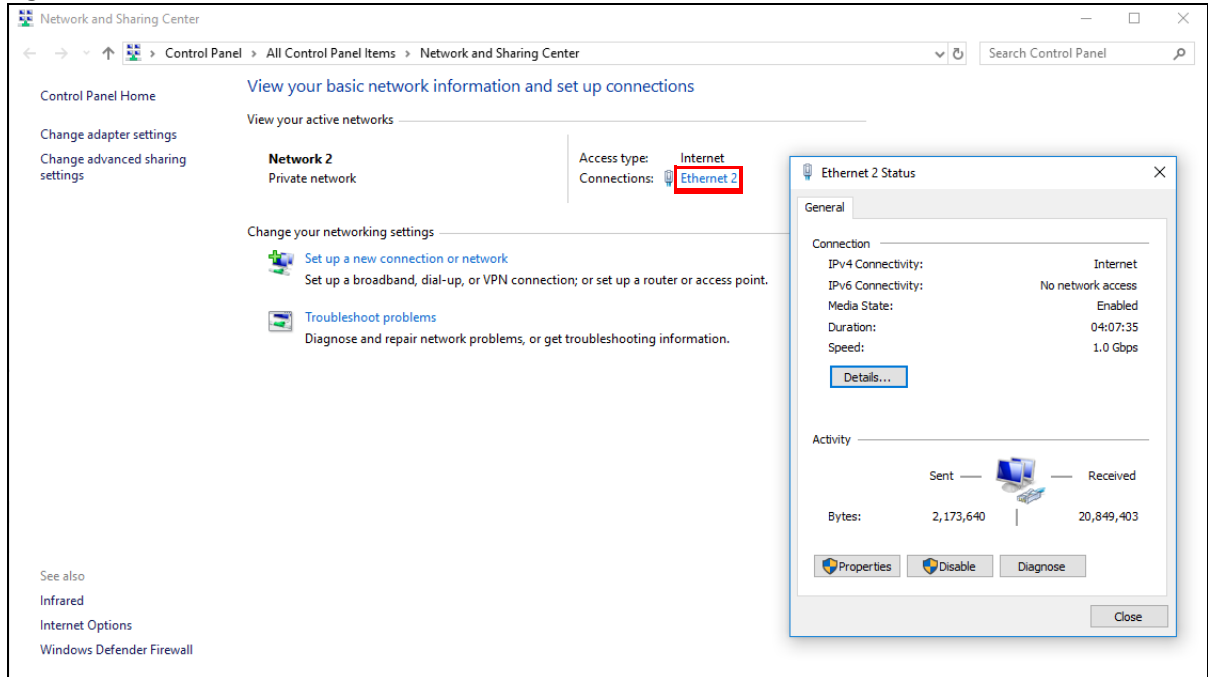
- 5 Click **OK**. Check the network icon on the system tray to see your Internet connection status.

**Figure 95** System Tray Icon

- 6 To see more details about your current Internet connection status, right click the network icon in the system tray and click **Open Network & Internet settings**. Click **Network and Sharing Center** and click the **Connections**.



Figure 96 Internet Connection Status



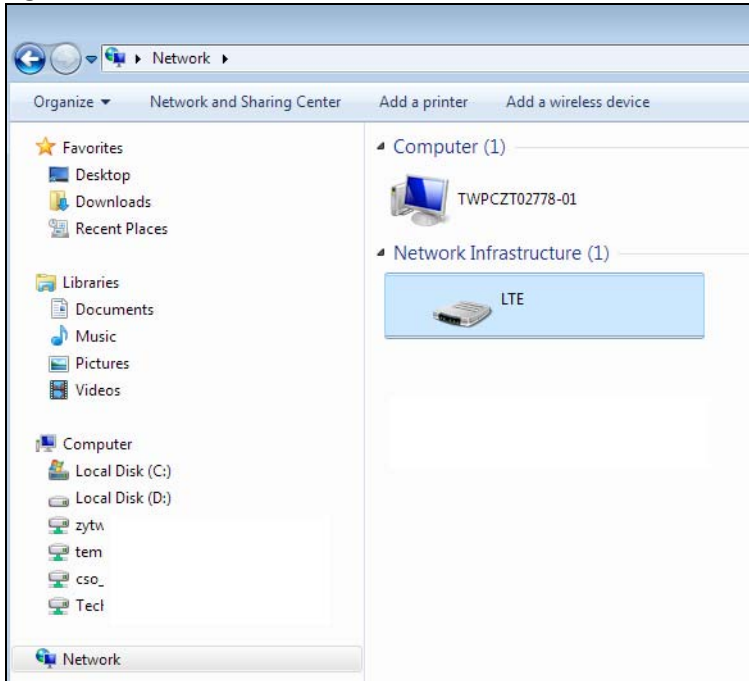
## 23.6 Web Configurator Easy Access in Windows 7

With UPnP, you can access the Web-based Configurator on the LTE without needing to find out the IP address of the LTE first. This comes helpful if you do not know the IP address of the LTE.

Follow the steps below to access the Web Configurator.

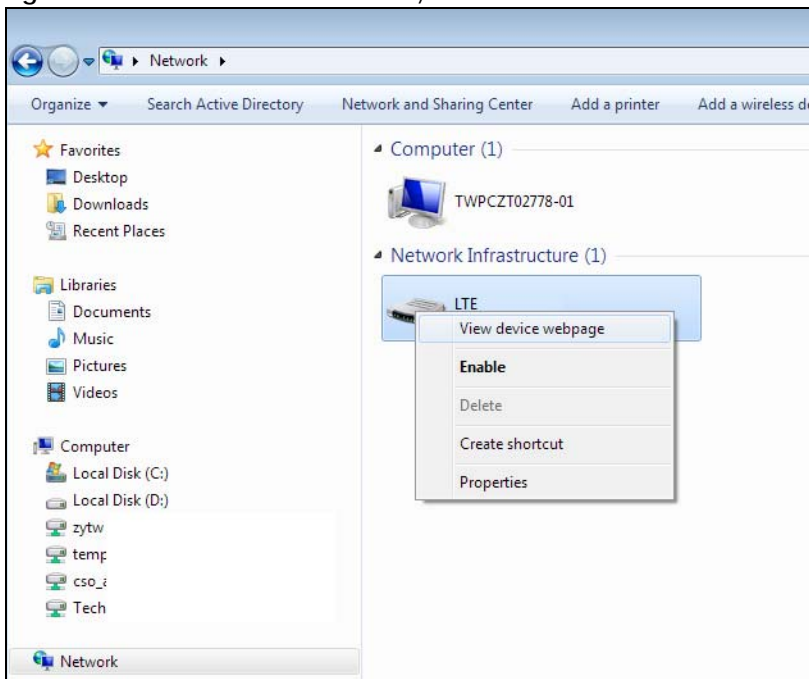
- 1 Open **Windows Explorer**.
- 2 Click **Network**.

Figure 97 Network Connections



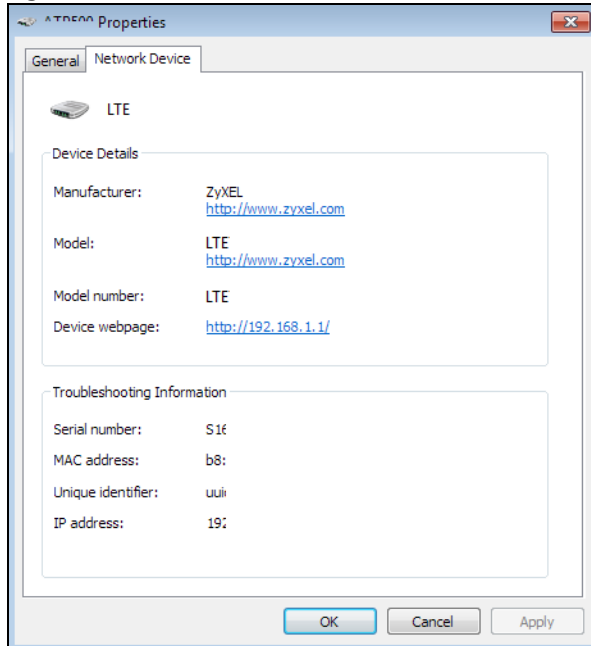
- 3 An icon with the description for each UPnP-enabled device displays under **Network Infrastructure**.
- 4 Right-click the icon for your LTE and select **View device webpage**. The Web Configurator login screen displays.

Figure 98 Network Connections: My Network Places



- 5 Right-click the icon for your LTE and select **Properties**. Click the **Network Device** tab. A window displays with information about the LTE.

**Figure 99** Network Connections: My Network Places: Properties: Example

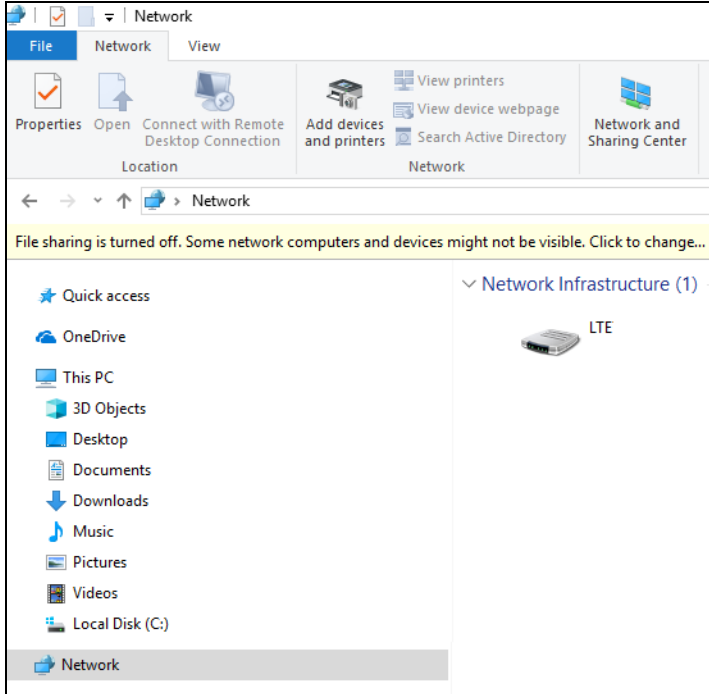


## 23.7 Web Configurator Easy Access in Windows 10

Follow the steps below to access the Web Configurator.

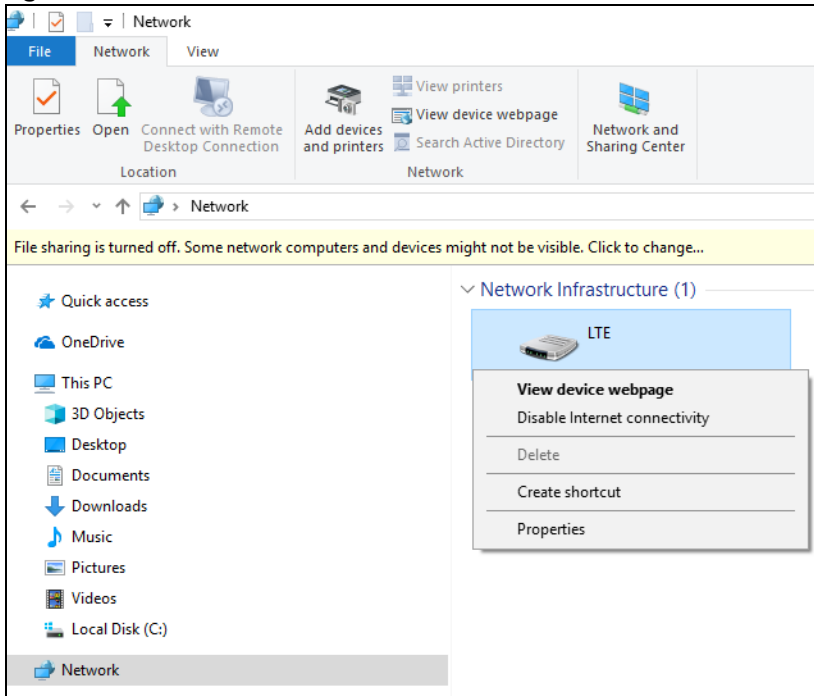
- 1 Open **File Explorer**.
- 2 Click **Network**.

Figure 100 Network Connections



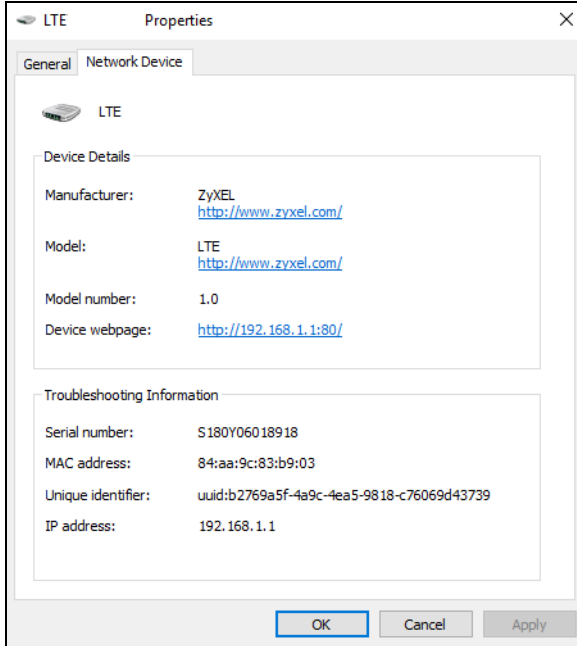
- 3 An icon with the description for each UPnP-enabled device displays under **Network Infrastructure**.
- 4 Right-click the icon for your LTE and select **View device webpage**. The Web Configurator login screen displays.

Figure 101 Network Connections: Network Infrastructure



- 5 Right-click the icon for your LTE and select **Properties**. Click the **Network Device** tab. A window displays information about the LTE.

Figure 102 Network Connections: Network Infrastructure: Properties: Example



# CHAPTER 24

## TR-069

### 24.1 Overview

This chapter explains how to configure the LTE's TR-069 auto-configuration settings.

### 24.2 TR-069 Settings

TR-069 defines how Customer Premise Equipment (CPE), for example your LTE, 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, modify settings, perform firmware upgrades as well as monitor and diagnose the LTE. You have to enable the device to be managed by the ACS and specify the ACS IP address or domain name and username and password.

Click **Configuration > Management > TR-069** to open the following screen. Use this screen to configure your LTE to be managed by an ACS.

**Figure 103** Configuration > Management > TR-069

TR069	
TR069 :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Inform :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Inform Interval :	86400
ACS URL :	
ACS Username :	
ACS Password :	
ConnectionRequest Port :	51005
Connection Request Username :	
Connection Request Password :	
<input type="button" value="Cancel"/> <input type="button" value="Apply"/>	

The following table describes the fields in this screen.

Table 63 Configuration > Management > TR-069

LABEL	DESCRIPTION
TR069	Select <b>Enable</b> to allow the LTE to be managed remotely by an ACS via TR-069. Otherwise, select <b>Disable</b> .
Inform	Select <b>Enable</b> for the LTE to send periodic inform via TR-069 on the WAN. Otherwise, select <b>Disable</b> .
Inform Interval	Enter the time interval (in seconds) at which the LTE sends information to the auto-configuration server.
ACS URL	Enter the URL or IP address of the auto-configuration server.
ACS Username	Enter the TR-069 user name for authentication with the auto-configuration server.
ACS Password	Enter the TR-069 password for authentication with the auto-configuration server.
Connection Request Port	Enter the port number for TR-069 connection requests.
Connection Request Username	Enter the connection request user name.  When the ACS makes a connection request to the LTE, this user name is used to authenticate the ACS.
Connection Request Password	Enter the connection request password.  When the ACS makes a connection request to the LTE, this password is used to authenticate the ACS.
Cancel	Click <b>Cancel</b> to exit this screen without saving.
Apply	Click <b>Apply</b> to save your changes.

# CHAPTER 25

## Maintenance

### 25.1 Overview

Use the system screens to configure general LTE settings.

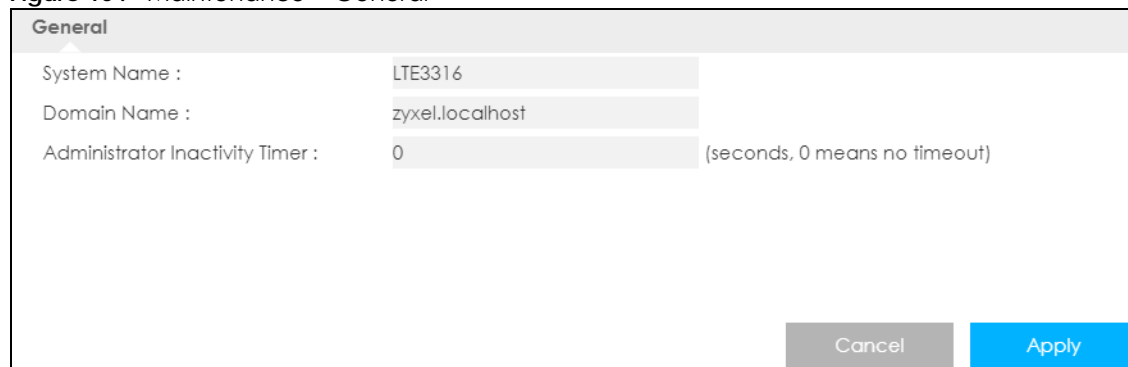
#### 25.1.1 What You Can Do in this Chapter

- Use the **General** screen to view basic information about the LTE and restart the LTE ([Section 25.2 on page 160](#)).
- Use the **User Account** screen to set the domain name and change the LTE's system password ([Section 25.3 on page 161](#)).
- Use the **Time Setting** screen to change the LTE's time and date and configure daylight saving time ([Section 25.4 on page 162](#)).
- Use the **Firmware Upgrade** screen to upload new firmware to your LTE ([Section 25.5 on page 164](#)).
- Use the **Module Upgrade** screen to upload firmware for the built-in LTE module ([Section 25.6 on page 165](#)).
- Use the **Backup/Restore** screen to reset your device settings back to the factory default, backup configuration, and restoring configuration ([Section 25.7 on page 166](#)).
- Use the **Reboot** screen to restart your LTE ([Section 25.8 on page 167](#)).

### 25.2 General Settings

Use this screen to set the management session timeout period. To access this screen, click **Maintenance > General**.

**Figure 104** Maintenance > General



General	
System Name :	LTE3316
Domain Name :	zyxel.localhost
Administrator Inactivity Timer :	0 (seconds, 0 means no timeout)

Cancel Apply



The following table describes the labels in this screen.

Table 64 System > System Information

LABEL	DESCRIPTION
System Name	<b>System Name</b> is a unique name to identify the LTE in an Ethernet network.
Domain Name	Enter the domain name you want to give to the LTE.
Administrator Inactivity timer	Type how many minutes a management session can be left idle before the session times out. The default is 300 seconds. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Cancel	Click <b>Cancel</b> to exit this screen without saving.
Apply	Click this button to save your changes back to the LTE.

## 25.3 User Account

It is strongly recommended that you change your LTE's system password.

If you forget your LTE's password (or IP address), you will need to reset the device. See [Section 25.7 on page 166](#) for details.

Click **Account > Account**. The screen appears as shown.

Figure 105 Maintenance > User Account

The screenshot shows the 'User Account' screen with the following fields and values:

- Username: admin
- Old Password: (empty)
- New Password: (empty)
- Retype to Confirm: (empty)
- Group: Administrator

Buttons: Cancel (grey), Apply (blue)

The following table describes the labels in this screen.

Table 65 Maintenance > Account

LABEL	DESCRIPTION
User Account Entries	
#	This is the index number of the entry.
User Name	This field displays the name of the user.
Group	This field displays the login account type of the user.
Modify	Click the <b>Edit</b> icon to edit this user account.

## 25.3.1 Modify a User Account

Use this screen to edit a users account. Click the **Modify** icon next to the user account you want to configure. The screen shown next appears.

**Figure 106** Maintenance > Account > Modify

The screenshot shows a web interface titled 'User Account' with a sub-section 'Account Setup'. It contains the following fields and values:

- Username : admin
- Old Password : [Empty text box]
- New Password : [Empty text box]
- Retype to Confirm : [Empty text box]
- Group : Administrator

At the bottom right, there are two buttons: a grey 'Cancel' button and a blue 'Apply' button.

The following table describes the labels in this screen.

**Table 66** Maintenance > Account > Modify

LABEL	DESCRIPTION
Account Setup	
Username	Enter a descriptive name for the user account. The user name can be up to 15 alphanumeric characters (0-9, A-Z, a-z, -, _ with no spaces).
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 an asterisk (*) for each character you type.
Retype to Confirm	Type the new password again in this field.
Group	This shows the type of login account.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Apply	Click <b>Apply</b> to save your changes back to the LTE.

## 25.4 Time Settings

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

Figure 107 Maintenance &gt; Time

The following table describes the labels in this screen.

Table 67 Maintenance &gt; Time

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your LTE. Each time you reload this page, the LTE synchronizes the time with the time server.
Current Date	This field displays the date of your LTE. Each time you reload this page, the LTE synchronizes the date with the time server.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you select <b>Manual</b> , enter the new time in this field and then click <b>Apply</b> .
New Date (yyyy/mm/dd)	This field displays the last updated date from the time server or the last date configured manually. When you select <b>Manual</b> , enter the new date in this field and then click <b>Apply</b> .
Get from Time Server	Select this radio button to have the LTE get the time and date from the time server you specified below.
User Defined Time Server Address	Select <b>User Defined Time Server Address</b> and enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Get from Cellular Network	Select this radio button to have the LTE get the time and date from the cellular network of the SIM card.
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).

Table 67 Maintenance &gt; Time (continued)

LABEL	DESCRIPTION
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 <b>Daylight Savings</b> . The <b>at</b> 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 <b>Second, Sunday, March</b> and select <b>2</b> in the <b>at</b> 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 <b>Last, Sunday, March</b> . The time you select in the <b>at</b> field depends on your time zone. In Germany for instance, you would select <b>2</b> because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected <b>Daylight Savings</b> . The <b>at</b> 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 <b>First, Sunday, November</b> and select <b>2</b> in the <b>at</b> 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 <b>Last, Sunday, October</b> . The time you select in the <b>at</b> field depends on your time zone. In Germany for instance, you would select <b>2</b> because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Apply	Click <b>Apply</b> to save your changes back to the LTE.

## 25.5 Firmware Upgrade

Find firmware at [www.zyxel.com](http://www.zyxel.com) in a file that uses the version number and project code with a "\*.bin" extension, e.g., "V1.00(AAYE.0).bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Click **Maintenance > Firmware Upgrade**. Follow the instructions in this screen to upload firmware to your LTE.

Figure 108 Maintenance &gt; Firmware Upgrade

**Firmware Upgrade**

**Firmware Upgrade**

To upgrade the internal device firmware, browse to the location of the binary (.BIN) upgrade file and click Upload. Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure.

File Path:  No file chosen

The following table describes the labels in this screen.

Table 68 Maintenance > Firmware Upgrade

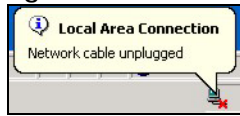
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse...</b> to find it.
Choose File	Click <b>Browse...</b> to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click <b>Upload</b> to begin the upload process. This process may take up to two minutes.

Note: Do not turn off the LTE while firmware upload is in progress!

After you see the **Firmware Upload In Process** screen, wait two minutes before logging into the LTE again.

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

Figure 109 Network Temporarily Disconnected



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

If the upload was not successful, an error message appears. Click **Return** to go back to the **Firmware Upgrade** screen.

## 25.6 Module Upgrade

Use this screen to upload new firmware specific to the built-in LTE module on the LTE in order to improve the LTE module's reliability and performance. Click **Maintenance > Module Upgrade** to open the following screen.

Note: When you are using the **Maintenance > Module Upgrade** screen to upload the LTE Series firmware which is downloaded from the Zyxel web site or FTP site, you are also uploading firmware for the LTE module.

Note: Use this screen to upload LTE firmware only when you are instructed by our technical support team and provided with new LTE firmware release.

The upload process uses HTTP (HyperText Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

**Do not turn off the LTE while firmware upload is in progress!**

Figure 110 Maintenance &gt; Module Upgrade

The following table describes the labels in this screen.

Table 69 Maintenance &gt; Module Upgrade

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse...</b> to find it.
Choose File	Click <b>Browse...</b> to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click <b>Upload</b> to begin the upload process. This process may take up to two minutes.

## 25.7 Configuration Backup/Restore

Backup configuration allows you to back up (save) the LTE's current configuration to a file on your computer. Once your LTE 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.

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

Click **Maintenance > Backup/Restore**. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

Figure 111 Maintenance &gt; Backup/Restore

The following table describes the labels in this screen.

Table 70 Maintenance > Backup/Restore

LABEL	DESCRIPTION
Backup Configuration	
Backup	Click <b>Backup</b> to save the LTE's current configuration to your computer.
Restore Configuration	
File Path	Type in the location of the file you want to upload in this field or click <b>Browse...</b> to find it.
Choose File	Click <b>Browse...</b> to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click <b>Upload</b> to begin the upload process.  Note: Do not turn off the LTE while configuration file upload is in progress.  After you see a "configuration upload successful" screen, you must then wait one minute before logging into the LTE again. The LTE automatically restarts in this time causing a temporary network disconnect.  If you see an error screen, click Back to return to the Backup/Restore screen.
Reset to Defaults	
Reset	Pressing the <b>Reset</b> button in this section clears all user-entered configuration information and returns the LTE to its factory defaults.  You can also press the <b>RESET</b> button on the rear panel to reset the factory defaults of your LTE. Refer to the chapter about introducing the Web Configurator for more information on the <b>RESET</b> button.

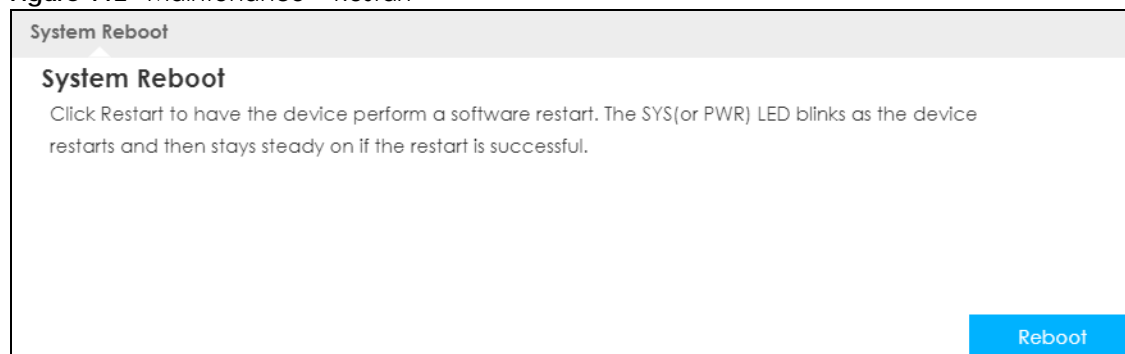
Note: If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default LTE IP address (192.168.1.1).

## 25.8 System Reboot

System restart allows you to reboot the LTE without turning the power off.

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

Figure 112 Maintenance > Restart



Click **Restart** to have the LTE reboot. This does not affect the LTE's configuration.

# CHAPTER 26

# Troubleshooting

## 26.1 Overview

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

- [Power, and Hardware Installation](#)
- [LTE Access and Login](#)
- [Internet Access](#)
- [Wireless Connections](#)

## 26.2 Power, and Hardware Installation

---

[The LTE does not turn on. None of the LEDs turn on.](#)

---

- 1 Make sure the LTE is correctly installed (refer to your Quick Start Guide).
- 2 Press the power button to turn the LTE on. See [Section 1.5.2 on page 16](#) and [Section 1.5.1 on page 15](#).
- 3 If the problem continues, contact the vendor.

## 26.3 LTE Access and Login

---

[I forgot the password for the LTE.](#)

---

- 1 The default IP address is 192.168.1.1.
- 2 If you changed the IP address and have forgotten it, you have to reset the device to its factory defaults. See [Section 1.5.2.3 on page 18](#).

---

[I cannot see or access the \*\*Login\*\* screen in the Web Configurator.](#)

---



- 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 [LTE Access and Login](#).
- 2 Make sure the LTE is correctly installed and turned on. See the Quick Start Guide and [Section 1.5.2 on page 16](#).
- 3 Make sure your Internet browser does not block pop-up windows and has JavaScript.
- 4 Make sure your computer is connected to the LTE and is in the same subnet as the LTE.
- 5 Reset the device to its factory defaults, and try to access the LTE with the default IP address. See [Section 1.5.2.3 on page 18](#).
- 6 Disconnect your computer from the Internet (Wireless and/or Ethernet) and then insert the LTE again.
- 7 If the problem continues, contact the vendor.

---

[I forgot the password.](#)

---

- 1 The default password is **1234**.
- 2 If this does not work, you have to reset the device to its factory defaults. See [Section 1.5.2.3 on page 18](#).

---

[I can see the Login screen, but I cannot log in to the LTE.](#)

---

- 1 Make sure you have entered the user name and password correctly. The default password is **1234**. This fields are case-sensitive, so make sure [Caps Lock] is not on.
- 2 This can happen when you fail to log out properly from your last session. Try logging in again after five minutes.
- 3 Disconnect and connect to the LTE again.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 1.5.2.3 on page 18](#).

## 26.4 Internet Access

---

[I cannot access the Internet through a 3G/4G wireless WAN connection.](#)

---

- 1 Make sure you insert a 4G SIM card into the card slot before turning on the LTE.
- 2 Make sure your mobile access information (such as APN) is entered correctly in the WAN screen. These fields are case-sensitive, so make sure [Caps Lock] is not on. Check with your service provider for the correct APN if you don't have it.
- 3 Make sure your SIM card's account is valid and has an active data plan. Check your service contract or contact your service provider directly.
- 4 If you are using a pre-paid SIM card, insert the SIM card on another mobile device to check if the SIM card still works. If the SIM card works without any problems on another mobile device, contact the vendor. Otherwise, contact your service provider.
- 5 If the problem continues, contact your ISP.

---

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

---

- 1 Reboot the LTE.
- 2 If the problem continues, contact your ISP.

---

The Internet connection is slow or intermittent.

---

- 1 There might be a lot of traffic on the network. If the LTE is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
- 2 Check the signal strength. If the signal strength is low, try moving the LTE closer to the ISP's base station if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).
- 3 Reboot the LTE.
- 4 If the problem continues, contact the network administrator or vendor.

## 26.5 Wireless Connections

---

I cannot access the LTE or ping any computer from the WLAN.

---

- 1 Make sure the wireless LAN is enabled on the LTE.
- 2 Make sure the wireless adapter (installed on your computer) is working properly.

- 3 Make sure the wireless adapter (installed on your computer) is IEEE 802.11 compatible and supports the same wireless standard as the LTE's active radio.
- 4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the LTE.
- 5 Check that both the LTE and your computer are using the same wireless and wireless security settings.

---

[I can only see newer logs. Older logs are missing.](#)

---

When a log reaches the maximum number of log messages, new log messages automatically overwrite existing log messages, starting with the oldest existing log message first.

## 26.6 Getting More Troubleshooting Help

Search for support information for your model at [www.zyxel.com](http://www.zyxel.com) for more troubleshooting suggestions.

# APPENDIX A

## Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a Zyxel office for the region in which you bought the device.

See <https://www.zyxel.com/homepage.shtml> and also [https://www.zyxel.com/about\\_zyxel/zyxel\\_worldwide.shtml](https://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml) for the latest information.

Please have the following information ready when you contact an office.

### Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

### Corporate Headquarters (Worldwide)

#### Taiwan

- Zyxel Communications Corporation
- <https://www.zyxel.com>

### Asia

#### China

- Zyxel Communications (Shanghai) Corp.
- Zyxel Communications (Beijing) Corp.
- Zyxel Communications (Tianjin) Corp.
- <https://www.zyxel.com/cn/zh/>

#### India

- Zyxel Technology India Pvt Ltd
- <https://www.zyxel.com/in/en/>

#### Kazakhstan

- Zyxel Kazakhstan
- <https://www.zyxel.kz>

## **Korea**

- Zyxel Korea Corp.
- <http://www.zyxel.kr>

## **Malaysia**

- Zyxel Malaysia Sdn Bhd.
- <http://www.zyxel.com.my>

## **Pakistan**

- Zyxel Pakistan (Pvt.) Ltd.
- <http://www.zyxel.com.pk>

## **Philippines**

- Zyxel Philippines
- <http://www.zyxel.com.ph>

## **Singapore**

- Zyxel Singapore Pte Ltd.
- <http://www.zyxel.com.sg>

## **Taiwan**

- Zyxel Communications Corporation
- <https://www.zyxel.com/tw/zh/>

## **Thailand**

- Zyxel Thailand Co., Ltd
- <https://www.zyxel.com/th/th/>

## **Vietnam**

- Zyxel Communications Corporation-Vietnam Office
- <https://www.zyxel.com/vn/vi>

## **Europe**

### **Belarus**

- Zyxel BY
- <https://www.zyxel.by>

### **Belgium**

- Zyxel Communications B.V.
- <https://www.zyxel.com/be/nl/>

- <https://www.zyxel.com/be/fr/>

## **Bulgaria**

- Zyxel България
- <https://www.zyxel.com/bg/bg/>

## **Czech Republic**

- Zyxel Communications Czech s.r.o
- <https://www.zyxel.com/cz/cs/>

## **Denmark**

- Zyxel Communications A/S
- <https://www.zyxel.com/dk/da/>

## **Estonia**

- Zyxel Estonia
- <https://www.zyxel.com/ee/et/>

## **Finland**

- Zyxel Communications
- <https://www.zyxel.com/fi/fi/>

## **France**

- Zyxel France
- <https://www.zyxel.fr>

## **Germany**

- Zyxel Deutschland GmbH
- <https://www.zyxel.com/de/de/>

## **Hungary**

- Zyxel Hungary & SEE
- <https://www.zyxel.com/hu/hu/>

## **Italy**

- Zyxel Communications Italy
- <https://www.zyxel.com/it/it/>

## **Latvia**

- Zyxel Latvia
- <https://www.zyxel.com/lv/lv/>

## **Lithuania**

- Zyxel Lithuania
- <https://www.zyxel.com/lt/lt/>

## **Netherlands**

- Zyxel Benelux
- <https://www.zyxel.com/nl/nl/>

## **Norway**

- Zyxel Communications
- <https://www.zyxel.com/no/no/>

## **Poland**

- Zyxel Communications Poland
- <https://www.zyxel.com/pl/pl/>

## **Romania**

- Zyxel Romania
- <https://www.zyxel.com/ro/ro>

## **Russia**

- Zyxel Russia
- <https://www.zyxel.com/ru/ru/>

## **Slovakia**

- Zyxel Communications Czech s.r.o. organizacna zlozka
- <https://www.zyxel.com/sk/sk/>

## **Spain**

- Zyxel Communications ES Ltd
- <https://www.zyxel.com/es/es/>

## **Sweden**

- Zyxel Communications
- <https://www.zyxel.com/se/sv/>

## **Switzerland**

- Studerus AG
- <https://www.zyxel.ch/de>
- <https://www.zyxel.ch/fr>

## **Turkey**

- Zyxel Turkey A.S.
- <https://www.zyxel.com/tr/tr/>

## **UK**

- Zyxel Communications UK Ltd.
- <https://www.zyxel.com/uk/en/>

## **Ukraine**

- Zyxel Ukraine
- <http://www.ua.zyxel.com>

## **South America**

### **Argentina**

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

### **Brazil**

- Zyxel Communications Brasil Ltda.
- <https://www.zyxel.com/br/pt/>

### **Colombia**

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

### **Ecuador**

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

### **South America**

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

## **Middle East**

### **Israel**

- Zyxel Communications Corporation
- <http://il.zyxel.com/>



## **Middle East**

- Zyxel Communications Corporation
- <https://www.zyxel.com/me/en/>

## **North America**

### **USA**

- Zyxel Communications, Inc. - North America Headquarters
- <https://www.zyxel.com/us/en/>

## **Oceania**

### **Australia**

- Zyxel Communications Corporation
- <https://www.zyxel.com/au/en/>

## **Africa**

### **South Africa**

- Nology (Pty) Ltd.
- <https://www.zyxel.com/za/en/>

# APPENDIX B

## Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name:** This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol:** This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s):** This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP, UDP, or TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description:** This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 71 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example <a href="http://www.zyxel.com">www.zyxel.com</a> ) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by email.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.

Table 71 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get email from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one email server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.

Table 71 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

# APPENDIX C

## Legal Information

### Copyright

Copyright © 2020 by Zyxel Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of Zyxel Communications Corporation.

Published by Zyxel Communications Corporation. All rights reserved.

### Disclaimer

Zyxel does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Zyxel further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

### Regulatory Notice and Statement

#### UNITED STATES of AMERICA



The following information applies if you use the product within USA area.

#### FCC EMC Statement

- The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:
  - (1) This device may not cause harmful interference, and
  - (2) This device must accept any interference received, including interference that may cause undesired operation.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the device.
- This product has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
- If this device does cause harmful interference to radio or television reception, which is found by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
  - Reorient or relocate the receiving antenna
  - Increase the separation between the devices
  - Connect the equipment to an outlet other than the receiver's
  - Consult a dealer or an experienced radio/TV technician for assistance

The following information applies if you use the product with RF function within USA area.

#### FCC Radiation Exposure Statement

- This device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must be at least 20 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.

#### CANADA

The following information applies if you use the product within Canada area.

#### Industry Canada ICES Statement

CAN ICES-3 (B)/NMB-3(B)

#### Industry Canada CS-03 Statement

- This product meets the applicable Innovation, Science and Economic Development Canada technical specifications.
- The Ringer Equivalence Number (REN) indicates the maximum number of devices allowed to be connected to a telephone interface. The termination of an interface may consist of any combination of devices subject only to the requirement that the sum of the RENs of all the devices not exceed five.

Déclaration de conformité

- Le présent produit est conforme aux spécifications techniques applicables d'Innovation, Sciences et Développement économique Canada.
- L'indice d'équivalence de la sonnerie (IES) sert à indiquer le nombre maximal de dispositifs qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme des IES de tous les dispositifs n'excède pas cinq.

**Industry Canada RSS-GEN & RSS-247 statement**

- This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.
- This radio transmitter has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

If the product with 5G wireless function operating in 5150-5250 MHz and 5725-5850 MHz, the following attention must be paid,

- The device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.
- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-to-point operation as appropriate; and
- The worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in Section 6.2.2(3) of RSS 247 shall be clearly indicated.

If the product with 5G wireless function operating in 5250-5350 MHz and 5470-5725 MHz, the following attention must be paid.

- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit.
- Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.
- Le présent émetteur radio de modèle s'il fait partie du matériel de catégoriel) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Lorsque la fonction sans fil 5G fonctionnant en 5150-5250 MHz and 5725-5850 MHz est activée pour ce produit, il est nécessaire de porter une attention particulière aux choses suivantes

- Les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5 725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée pour l'exploitation point à point et l'exploitation non point à point, selon le cas;
- Les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élévation, et énoncée à la section 6.2.2 3) du CNR-247, doivent être clairement indiqués.

Lorsque la fonction sans fil 5G fonctionnant en 5250-5350 MHz et 5470-5725 MHz est activée pour ce produit, il est nécessaire de porter une attention particulière aux choses suivantes.

- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis pour les dispositifs utilisant les bandes de 5 250 à 5 350 MHz et de 5 470 à 5 725 MHz doit être conforme à la limite de la p.i.r.e.

**Industry Canada radiation exposure statement**

This device complies with IC radiation exposure limits set forth for an uncontrolled environment. This device should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

**Déclaration d'exposition aux radiations:**

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

**EUROPEAN UNION**



The following information applies if you use the product within the European Union.

**Declaration of Conformity with Regard to EU Directive 2014/53/EU (Radio Equipment Directive, RED)**

- Compliance information for wireless products relevant to the EU and other Countries following the EU Directive 2014/53/EU (RED). And this product may be used in all EU countries (and other countries following the EU Directive 2014/53/EU) without any limitation except for the countries mentioned below table:
- In the majority of the EU and other European countries, the 5GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable. The requirements for any country may evolve. Zyxel recommends that you check with the local authorities for the latest status of their national regulations for the 5GHz wireless LANs.
- If this device for operation in the band 5150-5350 MHz, it is for indoor use only.
- This equipment should be installed and operated with a minimum distance of 20cm between the radio equipment and your body.

- The maximum RF power operating for each band as follows:
- WCDMA band I
  - the band 1922.6MHz to 1977.4MHz is 193.64mW
- WCDMA band III
  - the band 1712.6MHz to 1782.4MHz is 228.56mW
- WCDMA band VIII
  - the band 882.6MHz to 912.4MHz is 198.15mW
- LTE band 1
  - the band 882.6MHz to 912.4MHz is 223.87mW
- LTE band 3
  - the band 1922.5MHz to 1977.5MHz is 251.19mW
- LTE band 7
  - the band 2502.5MHz to 2567.5MHz is 218.78mW
- LTE band 8
  - the band 880.7MHz to 914.3MHz is 186.21mW
- LTE band 20
  - the band 834.5MHz to 859.5MHz is 186.21mW
- LTE band 28
  - the band 704.5MHz to 746.5MHz is 206.06mW
- LTE band 38
  - the band 2572.5MHz to 2617.5MHz is 247.17mW
- LTE band 40
  - the band 2302.5MHz to 2397.5MHz is 231.21mW
- 802.11b
  - the band 2400MHz to 2483.5MHz is 84.3mW
- 802.11g
  - the band 2400MHz to 2483.5MHz is 95.72mW
- 802.11n
  - the band 2400MHz to 2483.5MHz is 96.83mW
- 802.11ac
  - the band 5150MHz to 5350MHz is 195.88mW
- 802.11ac
  - the band 5470MHz to 5725MHz is 392.64mW

Български (Bulgarian)	<p>С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/ЕС.</p> <p><b>National Restrictions</b></p> <ul style="list-style-type: none"> <li>• The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check <a href="http://www.bipt.be">http://www.bipt.be</a> for more details.</li> <li>• Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie <a href="http://www.bipt.be">http://www.bipt.be</a> voor meer gegevens.</li> <li>• Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez <a href="http://www.ibpt.be">http://www.ibpt.be</a> pour de plus amples détails.</li> </ul>
Español (Spanish)	<p>Por medio de la presente Zyxel declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/UE.</p>
Čeština (Czech)	<p>Zyxel tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU.</p>
Dansk (Danish)	<p>Undertegnede Zyxel erklærer herved, at følgende udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU.</p> <p><b>National Restrictions</b></p> <ul style="list-style-type: none"> <li>• In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage.</li> <li>• I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.</li> </ul>
Deutsch (German)	<p>Hiermit erklärt Zyxel, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU befindet.</p>
Eesti keel (Estonian)	<p>Käesolevaga kinnitab Zyxel seadme vastavust direktiivi 2014/53/EL põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.</p>
Ελληνικά (Greek)	<p>ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Ζyxel ΔΗΛΩΝΕΙ ΟΤΙ ΕΞΟΤΙΣΜΟΣ ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/ΕΕ.</p>
English	<p>Hereby, Zyxel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.</p>
Français (French)	<p>Par la présente Zyxel déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/UE.</p>
Hrvatski (Croatian)	<p>Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 2014/53/UE.</p>

Íslenska (Icelandic)	Hér með lýsir, Zyxel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53/UE.
Italiano (Italian)	Con la presente Zyxel dichiara che questa attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/UE. <b>National Restrictions</b> <ul style="list-style-type: none"> <li>This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check <a href="http://www.sviluppoeconomico.gov.it/">http://www.sviluppoeconomico.gov.it/</a> for more details.</li> <li>Questo prodotto è conforme alle specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare <a href="http://www.sviluppoeconomico.gov.it/">http://www.sviluppoeconomico.gov.it/</a> per maggiori dettagli.</li> </ul>
Latviešu valoda (Latvian)	Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 2014/53/ES būtiskajām prasībām un citiem ar to saistītajiem noteikumiem. <b>National Restrictions</b> <ul style="list-style-type: none"> <li>The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check <a href="http://www.esd.lv">http://www.esd.lv</a> for more details.</li> <li>2.4 GHz frekvenču joslas izmantošanai ārpus telpām nepieciešama atļauja no Elektronisko sakaru direkcijas. Vairāk informācijas: <a href="http://www.esd.lv">http://www.esd.lv</a>.</li> </ul>
Lietuvių kalba (Lithuanian)	Šiuo Zyxel deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/ES Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, Zyxel nyilatkozik, hogy a berendezés megfelel a vonatkozó alapvető követelményeknek és az 2014/53/EU irányelv egyéb előírásainak.
Malti (Maltese)	Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-ftigijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Direttiva 2014/53/UE.
Nederlands (Dutch)	Hierbij verklaart Zyxel dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU.
Polski (Polish)	Niniejszym Zyxel oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/UE.
Português (Portuguese)	Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/UE.
Română (Romanian)	Prin prezenta, Zyxel declară că acest echipament este în conformitate cu cerințele esențiale și alte prevederi relevante ale Directivei 2014/53/UE.
Slovenčina (Slovak)	Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EÚ.
Slovenščina (Slovene)	Zyxel izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU.
Suomi (Finnish)	Zyxel vakuuttaa täten että laitteet tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska (Swedish)	Härmed intygar Zyxel att denna utrustning står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU.
Norsk (Norwegian)	Erklærer herved Zyxel at dette utstyret er i samsvar med de grunnleggende kravene og andre relevante bestemmelser i direktiv 2014/53/EU.

**Notes:**

- Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 2014/53/EU has also been implemented in those countries.
- The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).



## List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CZ	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Switzerland	CH
Ireland	IE	Sweden	SE
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

## Safety Warnings

- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Do not expose your device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do not install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do not open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks.
- Only qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do not allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Please use the provided or designated connection cables/power cables/ adaptors. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adaptor or cord is prohibited. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- CAUTION: Risk of explosion if battery is replaced by an incorrect type, dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,
  - For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;
  - For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.

## Environment Statement

## ErP (Energy-related Products)

Zyxel products put on the EU market in compliance with the requirement of the European Parliament and the Council published Directive 2009/125/EC establishing a framework for the setting of ecodesign requirements for energy-related products (recast), so called as "ErP Directive (Energy-related Products directive) as well as ecodesign requirement laid down in applicable implementing measures, power consumption has satisfied regulation requirements which are:

- Network standby power consumption < 8W, and/or
- Off mode power consumption < 0.5W, and/or
- Standby mode power consumption < 0.5W.

(Wireless setting, please refer to "Wireless" chapter for more detail.)

## European Union - Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.



台灣



以下訊息僅適用於產品具有無線功能且銷售至台灣地區

- 第十二條 經型式認證合格之低功率射頻電機，非經許可，公司，商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。
- 第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。
- 無線資訊傳輸設備忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用，俟無干擾之虞，始得繼續使用。
- 無線資訊傳輸設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作，發射的信號應維持於操作頻帶中。
- 使用無線產品時，應避免影響附近雷達系統之操作。
- 若使用高增益指向性天線，該產品僅應用於固定式點對點系統。

以下訊息僅適用於產品屬於專業安裝並銷售至台灣地區

- 本器材須經專業工程人員安裝及設定，始得設置使用，且不得直接販售給一般消費者。

安全警告 - 為了您的安全，請先閱讀以下警告及指示：





- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸：
  - 任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
  - 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不適當的材料。
- 雷雨天氣時，不要安裝，使用或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請插在正確的電壓供給插座（如：北美 / 台灣電壓 110V AC，歐洲是 230V AC）。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。

- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
  - 對永久連接之設備，在設備外部須安裝可觸及之斷電裝置；
  - 對插接式之設備，插座必須接近安裝之地點而且是易於觸及的。

## About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

### Explanation of the Symbols

SYMBOL	EXPLANATION
	Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction.
	Direct current (DC): DC is the unidirectional flow or movement of electric charge carriers.
	Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor.
	Class II equipment: The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation.

## Viewing Certifications

Go to <http://www.zyxel.com> to view this product's documentation and certifications.

## Zyxel Limited Warranty

Zyxel warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized Zyxel local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, Zyxel will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of Zyxel. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

### Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. Zyxel shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at [http://www.zyxel.com/web/support\\_warranty\\_info.php](http://www.zyxel.com/web/support_warranty_info.php).

## Registration

Register your product online at [www.zyxel.com](http://www.zyxel.com) to receive e-mail notices of firmware upgrades and related information.

## Open Source Licenses

This product may contain in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at [www.zyxel.com](http://www.zyxel.com). If you cannot find it there, contact your vendor or Zyxel Technical Support at [support@zyxel.com.tw](mailto:support@zyxel.com.tw).

To obtain the source code covered under those Licenses, please contact your vendor or Zyxel Technical Support at [support@zyxel.com](mailto:support@zyxel.com).

# Index

## A

access [20](#)  
ACS [158](#)  
ActiveX [115](#)  
Address Assignment [52](#)  
Auto Configuration Server, see ACS [158](#)

## B

Bandwidth management  
overview [138](#)

## C

certifications [185](#)  
    viewing [187](#)  
channel [65](#)  
Configuration  
    restore [167](#)  
configuration [13](#)  
    static route [162](#)  
contact information [172](#)  
content filtering  
    by keyword (in URL) [114](#)  
Cookies [115](#)  
cookies [20](#)  
copyright [181](#)  
customer support [172](#)

## D

Daylight saving [164](#)  
DDNS [102](#)  
    see also Dynamic DNS  
    service providers [102, 117](#)

DHCP [88](#)  
    see also Dynamic Host Configuration Protocol  
DHCP server [87, 88](#)  
disclaimer [181](#)  
DNS [91](#)  
DNS Server [52](#)  
DNS server [91](#)  
Domain Name System [91](#)  
Domain Name System. See DNS.  
Dynamic DNS [102](#)  
Dynamic Host Configuration Protocol [88](#)  
DynDNS [102, 117](#)  
DynDNS see also DDNS [102, 117](#)

## E

encryption [66](#)  
    and local (user) database [67](#)  
    key [67](#)  
    WPA compatible [67](#)  
ESSID [170](#)

## F

Firefox [20](#)  
Firewall  
    guidelines [110](#)  
    ICMP packets [111](#)  
Firmware upload [164](#)  
    file extension  
    using HTTP

## G

General wireless LAN screen [67](#)

**H**

hardware connections [15](#)

**I**

IGMP [52](#)  
    see also Internet Group Multicast Protocol  
    version  
IGMP version [52](#)  
installation [13](#)  
interface group [107](#)  
Internet Explorer [20](#)  
Internet Group Multicast Protocol [52](#)  
Internet Protocol version 6 [53](#)  
IP Address [87, 95](#)  
IP Pool [89](#)  
IPv6 [53](#)  
    addressing [53](#)  
    prefix [53](#)  
    prefix length [53](#)

**J**

Java [115](#)  
    permissions [20](#)  
JavaScripts [20](#)

**L**

LAN [86](#)  
    IP pool setup [88](#)  
LAN overview [86](#)  
LAN setup [86](#)  
Language [167](#)  
LEDs [15](#)  
local (user) database [66](#)  
    and encryption [67](#)  
Local Area Network [86](#)

**M**

MAC [77](#)  
MAC address [65](#)  
MAC address filter [65](#)  
MAC address filtering [77](#)  
MAC filter [77](#)  
maintenance [13](#)  
management [13](#)  
managing the device  
    good habits [14](#)  
Media access control [77](#)  
Multicast [52](#)  
    IGMP [52](#)

**N**

NAT [93, 94](#)  
    overview [93](#)  
    port forwarding [99](#)  
    see also Network Address Translation  
    server sets [99](#)  
NAT Traversal [143](#)  
Netscape Navigator [20](#)  
Network Address Translation [93, 94](#)

**O**

overview [13](#)

**P**

Pool Size [89](#)  
pop-up windows [20](#)  
Port forwarding [95, 99](#)  
    default server [95, 100](#)  
    example [100](#)  
    local server [95](#)  
    port numbers  
    services

**Q**

Quality of Service (QoS) [80](#)

**R**

RADIUS server [66](#)

remote management

TR-069 [158](#)

Remote Procedure Calls, see RPCs [158](#)

Restore configuration [167](#)

Roaming [79](#)

RPPCs [158](#)

RTS/CTS Threshold [65, 79](#)

**S**

Scheduling [83](#)

screen resolution [20](#)

Service and port numbers [113, 142](#)

Service Set [68, 76](#)

Service Set IDentification [68, 76](#)

Service Set IDentity. See SSID.

setup

static route [162](#)

SIM card [15](#)

SSID [65, 68, 76](#)

Static DHCP [90](#)

Static Route [104](#)

static route

configuration [162](#)

status [40](#)

Subnet Mask [87](#)

supported browsers [20](#)

System restart [167](#)

**T**

TCP/IP configuration [88](#)

Time setting [162](#)

TR-069 [158](#)

ACS setup [158](#)

trigger port [100](#)

Trigger port forwarding [100](#)

example [101](#)

process [101](#)

Turning on UPnP

Windows 7 example [144](#)

**U**

Universal Plug and Play [143](#)

Application [143](#)

Security issues [143](#)

UPnP [143](#)

UPnP-enabled Network Device

auto-discover [146, 150](#)

URL Keyword Blocking [115](#)

use [13](#)

user authentication [66](#)

local (user) database [66](#)

RADIUS server [66](#)

User Name [103](#)

**W**

WAN (Wide Area Network) [51](#)

warranty [187](#)

note [187](#)

Web Configurator [20](#)

access [20](#)

easy access [153](#)

requirements [20](#)

supported browsers [20](#)

web configurator [13](#)

Web Proxy [115](#)

WEP Encryption [72, 74](#)

wireless channel [170](#)

wireless LAN [170](#)

wireless LAN scheduling [83](#)

Wireless network

basic guidelines [64](#)

channel [65](#)

- encryption [66](#)
- example [64](#)
- MAC address filter [65](#)
- overview [64](#)
- security [65](#)
- SSID [65](#)
- Wireless security [65](#)
  - overview [65](#)
  - type [65](#)
- wireless security [170](#)
- Wireless tutorial [32](#)
- WPA compatible [67](#)