

User's Guide

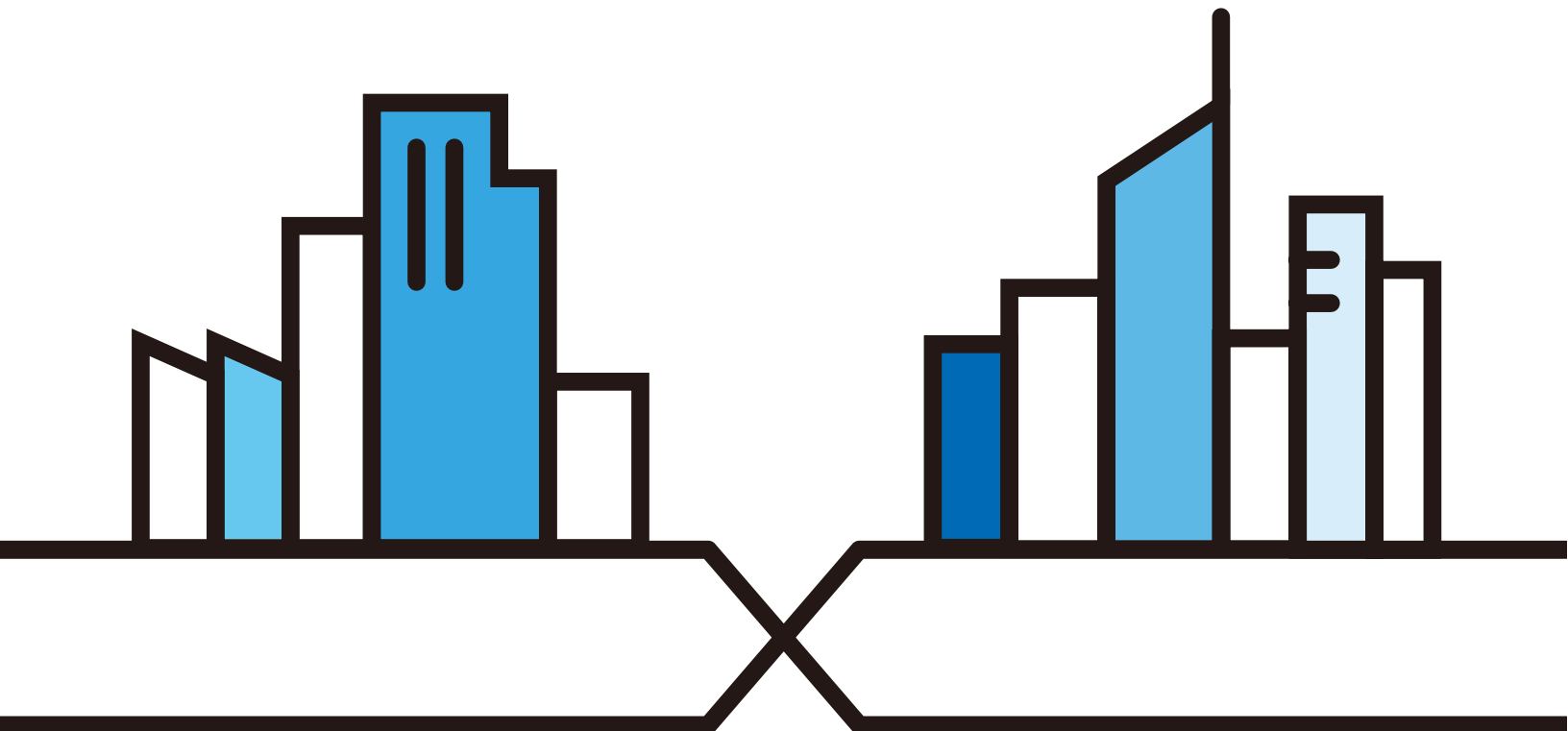
LTE3202-M430

4G LTE Indoor Router

Default Login Details

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

Version 1.00 Edition 1, 08/2018



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 to find other information on the LTE3202-M430.



Contents Overview

User's Guide	8
Introduction	9
The Web Configurator	14
Technical Reference	21
Setup Wizard	22
Status	24
Monitor	27
WAN Network	34
LAN	41
WLAN	46
Firewall	64
NAT	72
DDNS	77
Remote Management	79
Short Message	85
System	89
Troubleshooting	95

Table of Contents

Contents Overview	3
Table of Contents	4
Part I: User's Guide.....	8
Chapter 1	
Introduction	9
1.1 Overview	9
1.2 Applications	10
1.2.1 Wireless LAN (WiFi) Connection	10
1.3 Ways to Manage the LTE3202-M430	10
1.4 Good Habits for Managing the LTE3202-M430	10
1.5 Hardware Connections	10
1.5.1 LEDs	11
1.5.2 Rear Panel	12
Chapter 2	
The Web Configurator.....	14
2.1 Overview	14
2.2 Login Accounts	14
2.3 Accessing the Web Configurator	14
2.4 Navigating the Web Configurator	16
2.4.1 Title Bar	17
2.4.2 Navigation Panel	18
Part II: Technical Reference.....	21
Chapter 3	
Setup Wizard.....	22
3.1 Overview	22
3.2 Accessing the Wizard	22
3.3 Wizard Setup	22
Chapter 4	
Status.....	24

4.1 Overview	24
4.2 Status	24
Chapter 5	
Monitor	27
5.1 Overview	27
5.2 What You Can Do	27
5.3 The Log Screen	27
5.4 The DHCP Table Screen	28
5.5 The ARP Table Screen	29
5.6 The Packet Statistics Screen	30
5.7 The WLAN Station Status Screen	31
5.8 The LTE Modem Status Screen	31
Chapter 6	
WAN Network	34
6.1 Overview	34
6.1.1 What You Can Do in this Chapter	34
6.2 The Cellular Network Screen	35
6.3 The PIN Settings Screen	35
6.4 The APN Configuration Screen	36
6.5 The Network Selection Screen	37
6.6 Data Usage/Statistic Screen	38
6.7 The Operation Mode Screen	39
6.8 The Antenna Selection Screen	40
Chapter 7	
LAN	41
7.1 Overview	41
7.2 What You Can Do	41
7.3 What You Need To Know	41
7.4 The LAN IP Screen	42
7.5 The DHCP Server Screen	43
7.6 DNS Settings Screen	44
Chapter 8	
WLAN	46
8.1 Overview	46
8.1.1 What You Can Do in this Chapter	46
8.1.2 What You Need to Know	46
8.2 WiFi Settings Screen	47
8.3 MAC Filter Screen	50
8.4 WPS Screen	51

8.5 Technical Reference	52
8.5.1 Wireless Network Overview	52
8.5.2 Additional Wireless Terms	54
8.5.3 Wireless Security Overview	54
8.5.4 Signal Problems	56
8.5.5 WiFi Protected Setup (WPS)	57
Chapter 9	
Firewall.....	64
9.1 Overview	64
9.1.1 What You Can Do	64
9.1.2 What You Need To Know	65
9.2 The DoS Protection Screen	66
9.3 The ICMP Protection Screen	67
9.4 The ARP Protection Screen	67
9.5 URL Filter Screen	68
9.6 IPv4/Port Filter Screen	69
9.7 IPv6/Port Filter Screen	71
Chapter 10	
NAT	72
10.1 Overview	72
10.1.1 What You Can Do in this Chapter	72
10.2 The IP/Port Forwarding Screen	73
10.3 The DMZ Screen	74
10.4 The ALG Screen	74
10.5 The Pass Through Screen	75
Chapter 11	
DDNS	77
11.1 Overview	77
11.2 The DDNS Screen	77
Chapter 12	
Remote Management.....	79
12.1 Overview	79
12.1.1 What You Can Do in this Chapter	79
12.2 The Web Interface Screen	79
12.3 The TR069 Screen	80
12.4 The Telnet Screen	81
12.5 The UPnP Screen	82
12.5.1 Cautions with UPnP	82
12.6 The Bandwidth Management Screen	83

Chapter 13	
Short Message	85
13.1 Overview	85
13.1.1 What You Can Do in this Chapter	85
13.2 New SMS Screen	85
13.3 Inbox Screen	86
13.4 Outbox Screen	86
13.5 Draft Screen	87
13.6 SIM SMS Screen	88
Chapter 14	
System	89
14.1 Overview	89
14.1.1 What You Can Do in this Chapter	89
14.2 The General Screen	89
14.3 The User Account Screen	90
14.4 The Time Settings Screen	91
14.5 The Firmware Upgrade Screen	92
14.6 The Settings Profile Screen	93
14.6.1 Reset Settings	93
14.6.2 Import & Export Profile	94
14.7 The Reboot Screen	94
Chapter 15	
Troubleshooting	95
15.1 Overview	95
15.2 Power, and Hardware Installation	95
15.3 LTE3202-M430 Access and Login	95
15.4 Internet Access	97
15.5 Wireless Connections	98
15.6 Getting More Troubleshooting Help	98
Appendix A Customer Support	99
Appendix B Common Services	105
Appendix C Legal Information	108
Index	115

PART I

User's Guide

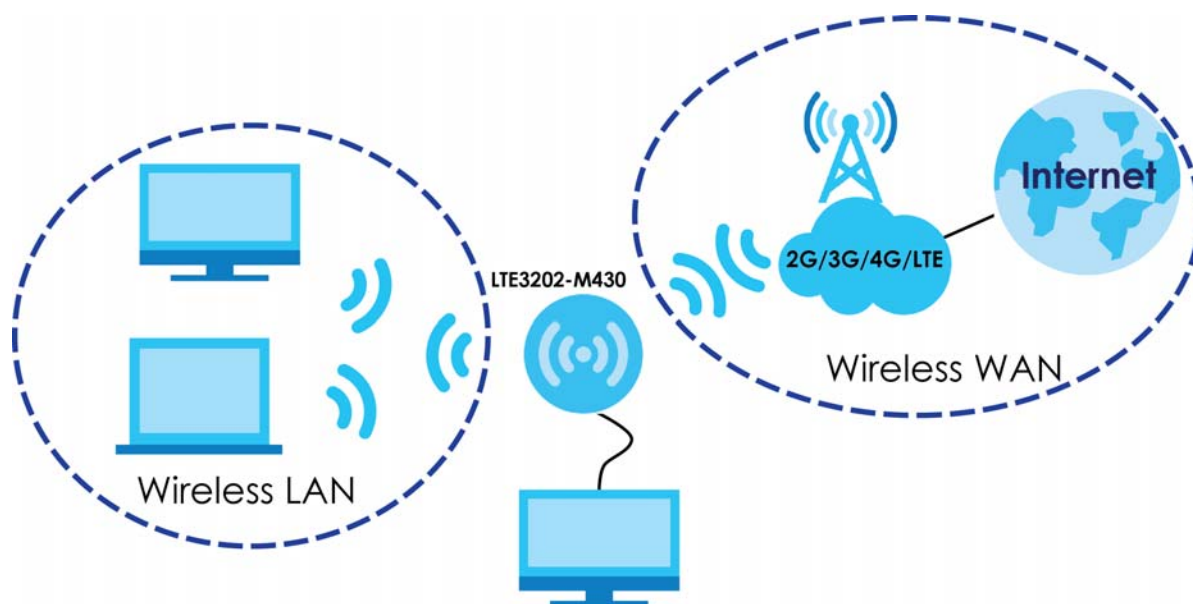
CHAPTER 1

Introduction

1.1 Overview

This chapter introduces the main features and applications of the LTE3202-M430.

The LTE3202-M430 is a 4G LTE indoor wireless router, which can connect to a mobile network and the Internet through a wireless WAN connection and provide easy network access to mobile users without additional wiring. You can set up a wireless network with other IEEE 802.11b/g/n compatible devices.



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

Your LTE3202-M430 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 LTE3202-M430 has two internal antennas. 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 LTE3202-M430 is starting up.

1.2 Applications

You can have the following networks with the LTE3202-M430:

- **Wired LAN.** You can connect network devices via the Ethernet ports of the LTE3202-M430 so that they can communicate with each other and access the Internet.
- **Wireless LAN.** Wireless clients can wirelessly connect to the LTE3202-M430 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 LAN (WiFi) Connection

The LTE3202-M430 is a wireless Access Point (AP) for wireless clients, such as notebook computers or PDAs 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 LTE3202-M430.

1.3 Ways to Manage the LTE3202-M430

Use any of the following methods to manage the LTE3202-M430.

- **WPS (WiFi Protected Setup).** You can use the WPS button or the WPS section of the Web Configurator to set up a wireless network with your LTE3202-M430.
- **Web Configurator.** This is recommended for everyday management of the LTE3202-M430 using a (supported) web browser.
- **TR-069.** This is an auto-configuration server used to remotely configure your device.

1.4 Good Habits for Managing the LTE3202-M430

Do the following things regularly to make the LTE3202-M430 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 LTE3202-M430 to its factory default settings. If you backed up an earlier configuration file, you won't have to totally re-configure the LTE3202-M430; 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 LTE3202-M430 before you can use it.

1.5.1 LEDs

The following graphics display the front panel of the LTE3202-M430. You can check the LED lights to see the 2G/3G/4G connection status, signal strength, and the wireless connection status.

Figure 1 LTE3202-M430 Front Panel

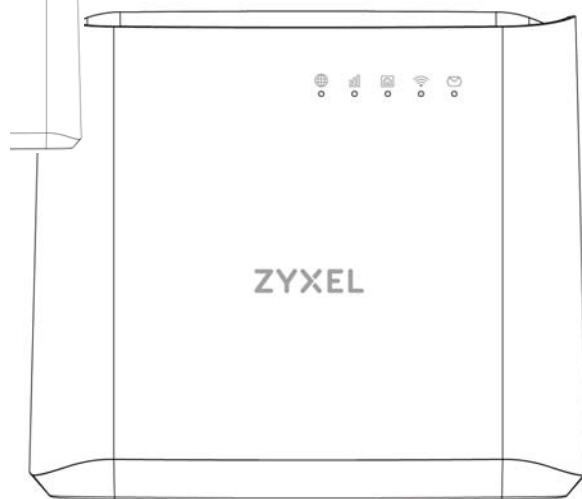
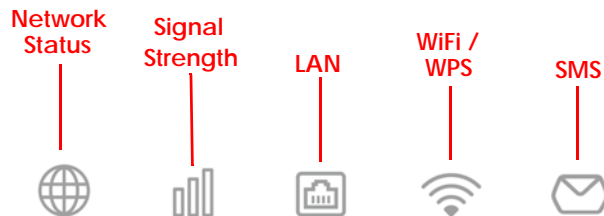


Figure 2 LEDs



The following table describes the LED lights.

Table 1 Front Panel LEDs

LED	COLOR	STATUS	DESCRIPTION
Network	Blue	On	The LTE3202-M430 is successfully connected to a 4G or LTE network.
		Blinking	The LTE3202-M430 is starting up.
	Green	On	The LTE3202-M430 is successfully connected to a 3G network.
	Yellow	On	The LTE3202-M430 is successfully connected to a 2G network.
	Red	On	The LTE3202-M430 is malfunctioning.
Blinking		The LTE3202-M430 is rebooting or has failed to connect to a 2G/3G/4G/LTE network.	
Signal Strength	Blue	On	A valid SIM card is inserted and the wireless WAN interface is enabled, this indicates the signal strength is excellent.
	Green	On	A valid SIM card is inserted and the wireless WAN interface is enabled, this indicates the signal strength is fair.
	Red	Blinking	A valid SIM card is inserted and the wireless WAN interface is enabled, this indicates the signal strength is poor.

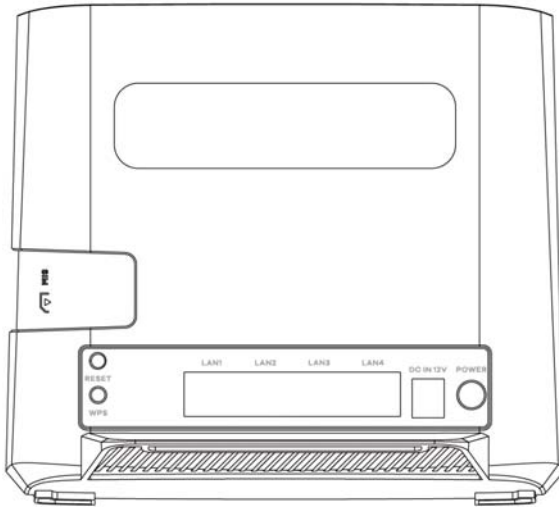
Table 1 Front Panel LEDs

LED	COLOR	STATUS	DESCRIPTION
LAN	Blue	On	The LTE3202-M430 has an Ethernet LAN connection.
		Blinking	The LTE3202-M430 is transmitting/receiving data through the Ethernet LAN connection.
		Off	The LTE3202-M430 does not detect an Ethernet LAN connection.
WiFi/WPS	Blue	On	The LTE3202-M430 is ready and the 2.4GHz wireless LAN is on, and is sending/receiving data through the wireless LAN.
		Blinking	The LTE3202-M430 is connecting to a 2.4GHz WiFi-Connection via WPS.
		Off	The LTE3202-M430 wireless LAN interface is not ready.
SMS	Blue	Blinking	The LTE3202-M430 has unread SMS messages.
		Off	The LTE3202-M430 has no unread SMS messages.

1.5.2 Rear Panel

To turn on the device, press the power button.

Figure 3 LTE3202-M430 Power Button



1.5.2.1 SIM Card Slot

The LTE3202-M430 comes with a built-in 2G/3G/4G/LTE module for mobile connections. To set up a mobile connection using the built-in 2G/3G/4G/LTE module, just insert a SIM card into the SIM card slot at the back of the LTE3202-M430.

Note: You must insert the SIM card into the card slot before turning on the LTE3202-M430.

1.5.2.2 The WPS Button

Your LTE3202-M430 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 rear panel of the LTE3202-M430 to activate WPS in order to quickly set up a wireless network with strong security.

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 LTE3202-M430.

Note: You must activate WPS in the LTE3202-M430 and in another wireless device within two minutes of each other.

1.5.2.3 Reset the LTE3202-M430

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**.

How to Use the Reset Button

- 1 Press the **Reset button** on the rear panel for two seconds to restart/reboot the LTE3202-M430.
- 2 Press the **Reset button** on the rear panel for more than five seconds to set the LTE3202-M430 back to its factory default configurations.

CHAPTER 2

The Web Configurator

2.1 Overview

This chapter describes how to access the LTE3202-M430 Web Configurator and provides an overview of its screens.

The Web Configurator is an HTML-based management interface that allows easy setup and management of the LTE3202-M430 via Internet browser. Use Internet Explorer 9.0 and later versions, Mozilla Firefox 21 and later versions, Safari 6.0 and later versions or Google Chrome 26.0 and later versions. 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. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

Refer to the Troubleshooting chapter ([Chapter 15 on page 95](#)) to see how to make sure these functions are allowed in Internet Explorer.

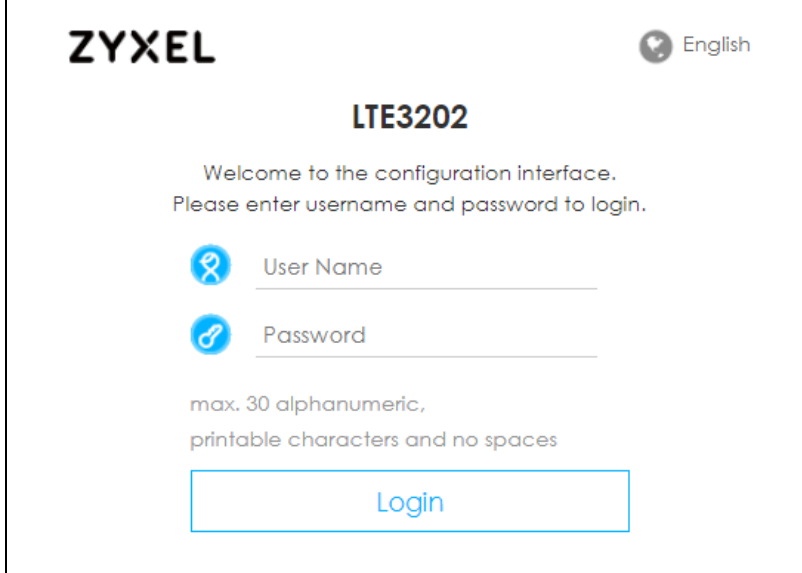
2.2 Login Accounts

There is one system account that you can use to log in to the LTE3202-M430: "**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

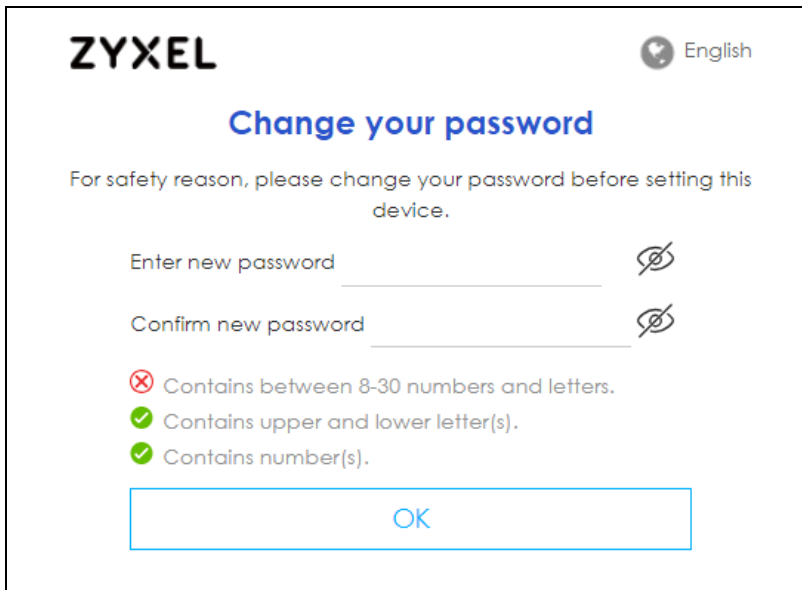
- 1 Make sure your LTE3202-M430 hardware is properly connected and prepare your computer or computer network to connect to the LTE3202-M430 (refer to the Quick Start Guide).
- 2 Launch your web browser.

- 3 Type "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.



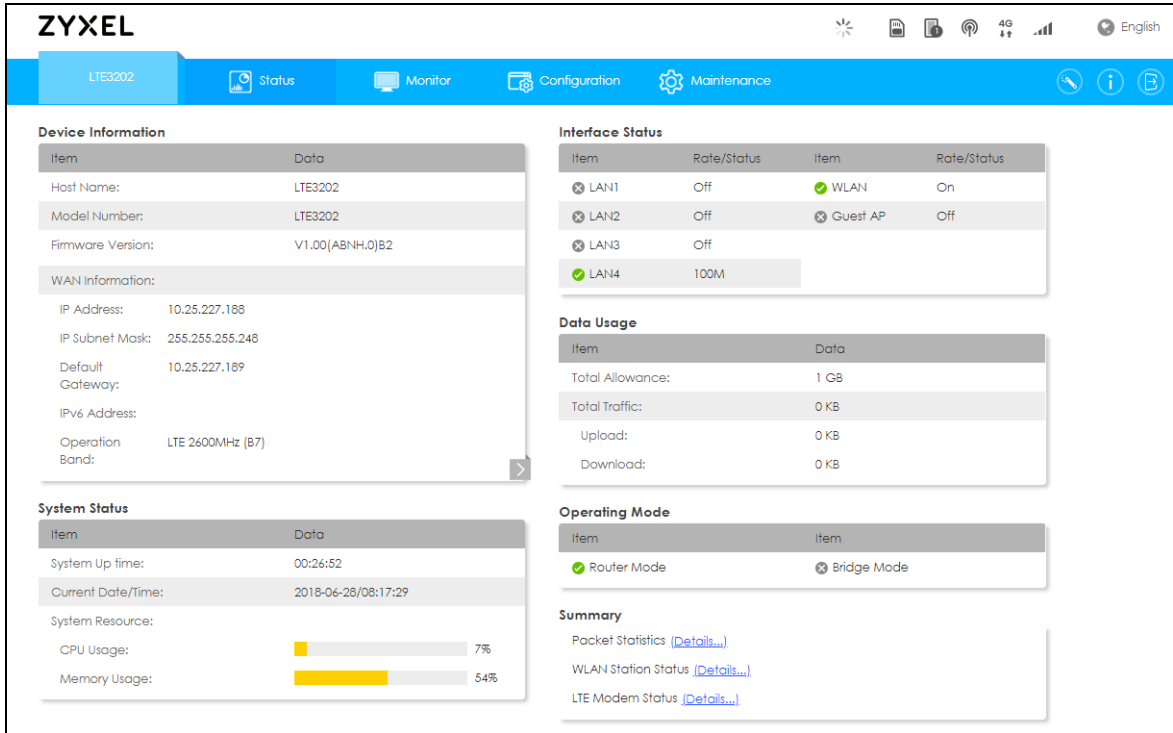
The screenshot shows the ZYXEL LTE3202 login interface. At the top left is the ZYXEL logo, and at the top right is a language selector set to "English". The device model "LTE3202" is centered. Below it, a welcome message reads: "Welcome to the configuration interface. Please enter username and password to login." There are two input fields: "User Name" with a key icon and "Password" with a key icon. Below the password field, a note states: "max. 30 alphanumeric, printable characters and no spaces". A blue "Login" button is at the bottom.

- 4 Enter the **User Name** (default: "admin") and **Password** (default: "1234"). See [Section 2.2 on page 14](#) 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**.



The screenshot shows the ZYXEL "Change your password" screen. At the top left is the ZYXEL logo, and at the top right is a language selector set to "English". The title "Change your password" is centered. Below it, a message reads: "For safety reason, please change your password before setting this device." There are two input fields: "Enter new password" and "Confirm new password", both with eye icons. Below the fields, three password requirements are listed: "Contains between 8-30 numbers and letters." (marked with a red X), "Contains upper and lower letter(s)." (marked with a green check), and "Contains number(s)." (marked with a green check). A blue "OK" button is at the bottom.

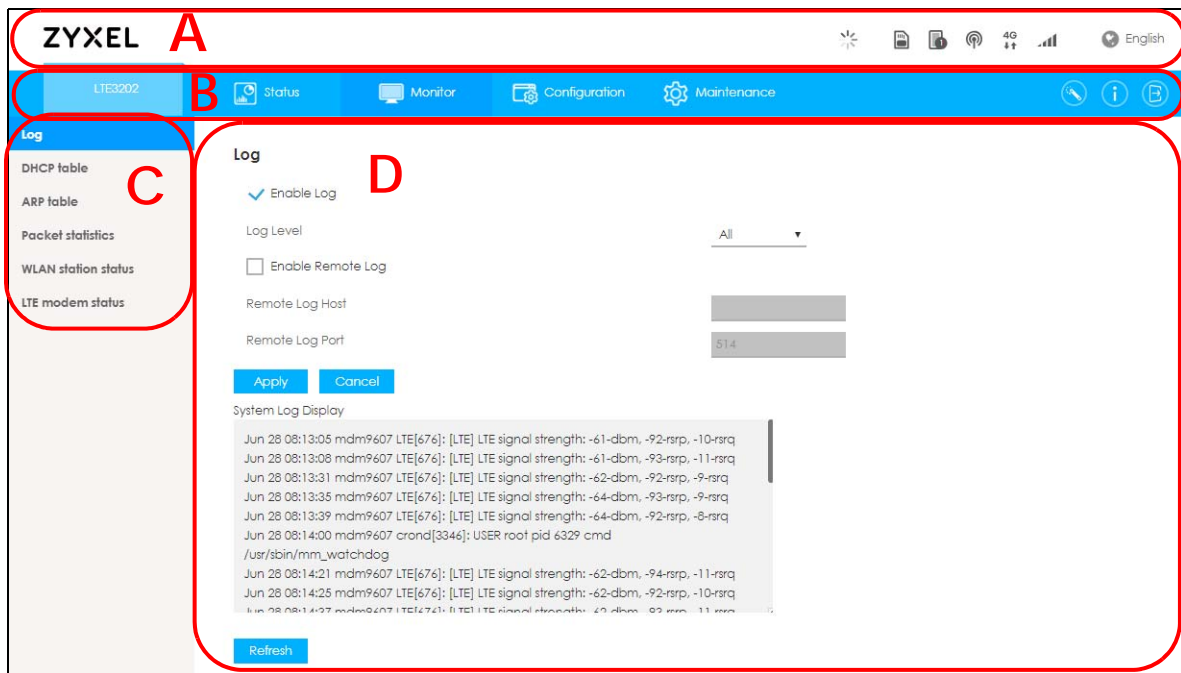
- 6 The **Home** screen appears.



2.4 Navigating the Web Configurator

The following summarizes how to navigate the web configurator from the **Home** screen.

Figure 4 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 5 Title Bar



The icons provide the following functions.

Table 2 Title Bar: Web Configurator Icons












LABEL	DESCRIPTION
SIM	<p>This shows the LTE3202-M430's SIM card status.</p> <ul style="list-style-type: none"> • This icon shows  if there is a SIM card inserted • This icon shows  if there is no SIM card inserted. • This icon shows  if the SIM card is blocked. • This icon shows  if there is a SIM card error.
Roaming 	This appears when the LTE3202-M430 is connected to another service provider's mobile network using roaming.
Clients 	This shows the number of the clients currently connected to the LTE3202-M430.
WiFi 	<p>This shows whether the LTE3202-M430's WiFi LAN network is enabled.</p> <p>The following icons  displays when the WiFi LAN network is disabled.</p>
WAN Connection 	This displays the type of mobile data connection the LTE3202-M430 has to the ISP.

Table 2 Title Bar: Web Configurator Icons (continued)

LABEL	DESCRIPTION
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.
Language 	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 LTE3202-M430 features. The following sections introduce the LTE3202-M430's navigation panel menus and their screens.

Figure 6 Navigation Panel



The following table describes the icons in the Navigation Panel.

Table 3 Title Bar: Web Configurator Icons

LABEL	DESCRIPTION
Setup Wizard 	Click this icon to open the Setup Wizard for the LTE3202-M430.
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.

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

Table 4 Navigation Panel

MENU	SUB-MENU	DESCRIPTION
Status		This screen shows the LTE3202-M430's general device, system and interface status information. Use this screen to access the summary statistics tables.
Monitor		
Log		Use this screen to view the list of activities recorded by your LTE3202-M430.
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.

Table 4 Navigation Panel

MENU	SUB-MENU	DESCRIPTION
WLAN station status		Use this screen to view the wireless stations that are currently associated to the LTE3202-M430's 2.4GHz 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		
WAN network	Cellular Network	Use this screen to specify the type of the mobile network to which the LTE3202-M430 is connected, and how you want the LTE3202-M430 to connect to an available mobile network.
	PIN Settings	Use this screen to enable PIN code authentication and enter the PIN code.
	APN Configuration	Use this screen to configure user-defined connection profiles.
	Network Selection	Use this screen to view available Public Land Mobile Networks (PLMNs) and select a preferred network.
	Data Usage / Statistics	Use this screen to specify limiting amount of package data consumed and view its statistics.
	Operating Mode	Use this screen to select whether the LTE3202-M430 operates in router or bridge mode.
	Antenna Selection	Use this screen to specify which antennas the LTE3202-M430 uses for signal transmission.
LAN network	LAN IP	Use this screen to configure LAN IP address and subnet mask.
	DHCP Server	Use this screen to enable the LTE5366's DHCP server, and assign IP addresses to specific individual computers based on their MAC addresses and to have DNS servers assigned by the DHCP server.
	DNS Settings	Use this screen to configure the DNS servers.
WLAN	WiFi Settings	Use this screen to enable the wireless LAN and configure wireless LAN and wireless security settings.
	MAC Filter	Use the MAC filter screen to allow or deny wireless stations based on their MAC addresses from connecting to the LTE3202-M430.
	WPS	Use this screen to use WPS to connect to a wireless device.
Firewall	DOS protection	Use this screen to enable/disable DoS protection.
	ICMP Protection	Use this screen to enable/disable PING requests in the LTE3202-M430 interfaces.
	ARP Protection	Use this screen to enable Address Resolution Protocol (ARP) protection.
	URL Filter	Use this screen to configure URL firewall rules.
	IPv4 Port Filter	Use this screen to create IPv4 firewall rules.
	IPv6 Port Filter	Use this screen to create IPv6 firewall rules.
NAT	IP/Port Forwarding	Use this screen to configure servers behind the LTE3202-M430 and forward incoming service requests to the server(s) on your local network.
	DMZ	Use this screen to set the IP address of your network DMZ (if you have one) for the LTE3202-M430.
	ALG	Use this screen to enable or disable SIP (VoIP) ALG (Application Layer Gateway) in the LTE3202-M430.
	Pass through	Use this screen to enable/disable the ALGs (Application Layer Gateway) in the LTE3202-M430.

Table 4 Navigation Panel

MENU	SUB-MENU	DESCRIPTION
DDNS		Use this screen to set up dynamic DNS.
Remote Management	Web interface	Use this screen to modify the server port for the HTTPS service.
	TR069	Use this screen to configure your LTE3202-M430 to be managed by an ACS.
	Telnet	Use this screen to specify which interfaces allow Telnet access.
	UPnP	Use this screen to enable UPnP on the LTE3202-M430.
	Bandwidth Management	Use this screen to set the upstream bandwidth and edit a bandwidth management rule.
Short Message	New SMS	Use this screen to send short messages.
	Inbox	Use this screen to view messages received by the LTE3202-M430.
	Outbox	Use this screen to view messages sent from the LTE3202-M430.
	Draftbox	Use this screen to view messages that are stored in the LTE3202-M430.
	SIM SMS	Use this screen to view messages received on the SIM card.
Maintenance		
General		Use this screen to view and change administrative settings such as system and domain names.
User Account		Use this screen to change the user name and password of your LTE3202-M430.
Time Settings		Use this screen to change your LTE3202-M430's time and date.
Firmware Upgrade		Use this screen to upload firmware to your LTE3202-M430.
Settings Profile		Use this screen to backup and restore the configuration of your LTE3202-M430.
Reboot		Use this screen to reset your LTE3202-M430 back to its factory defaults.

PART II

Technical Reference

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 type "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 navigation panel to open the Wizard screen.

Figure 7 Wizard Icon



3.3 Wizard Setup

- 1 The first Wizard screen displays showing the main steps in the Wizard setup. Enter your **APN** (Access Point Name) **Profile** provided by your service provider. Select the **Auto** option if you did not configure an APN connection profile. If you have a limited data plan, you can specify the limited amount of the package data, and a reminder for when the percentage of the package data usage. Click **Next** to continue.

Figure 8 Setup Wizard > WAN Setting

Setup Wizard

Step 1.
WAN Setting

Step 2.
WiFi Setting

Step 3.
Apply Settings

APN Profile: Manual ▾

APN: internet

Username:

Password:

Authentication: None ▾

PDP type: IPv4 ▾

Data usage limit: Monthly data plan 1 GB ▾

Threshold 80 %

[Next >](#)

- This screen shows the default **SSID Name** and **WiFi Key** for the LTE3202-M430's wireless network. Use this screen to configure the LTE3202-M430 wireless network settings. If you set up a new **WiFi Key** and **SSID Name**, the wireless clients will lose their wireless connection and will need to use the new wireless settings. Click **Next** to continue.

Figure 9 Setup Wizard > WiFi Setting

Setup Wizard

Step 1.
WAN Setting

Step 2.
WiFi Setting

Step 3.
Apply Settings

SSID Name ZyxeI_35B4

Security mode Security WPA2 ▾

Cypher mode AES ▾

WiFi key 123456789

Guest AP

[< Back](#) [Next >](#)

- Click **Apply** to save your settings. Otherwise, click **Back** to go back to the previous screen.

Table 5 Apply Settings

Setup Wizard

Step 1.
WAN Setting

Step 2.
WiFi Setting

Step 3.
Apply Settings

Apply the configurations

Applying settings may cause the WiFi to disconnect and lose connection to this website. Please check all the changes before you click "Apply".

[< Back](#) [Apply](#)

CHAPTER 4

Status

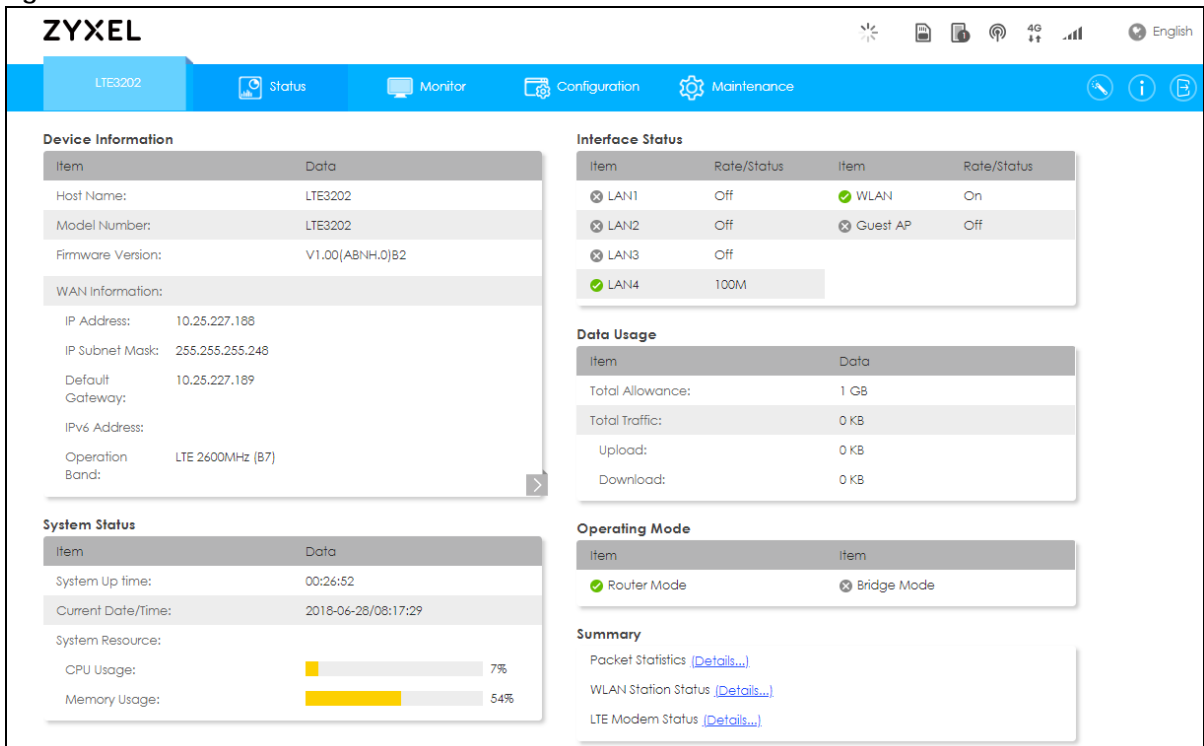
4.1 Overview

Use the **Status** screen to check status information about the LTE3202-M430.

4.2 Status

This screen is the first thing you see when you log into the LTE3202-M430. It also appears every time you click the **Status** icon in the navigation panel. The **Status** screen displays the LTE3202-M430's connection mode, wireless LAN information and traffic statistics.

Figure 10 Status



The following table describes the labels in this screen.

Table 6 Status

LABEL	DESCRIPTION
Device Information	
Host Name	This is the System Name you enter in the Maintenance > General 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	
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 LTE3202-M430 on the WAN.
Operation Band	This shows the network type and the frequency band used by the mobile network to which the LTE3202-M430 is connecting.
System Status	
Item	This column shows the type of data the LTE3202-M430 is recording.
Data	This column shows the actual data recorded by the LTE3202-M430.
System Up time	This is the total time the LTE3202-M430 has been on.
Current Date/Time	This field displays your LTE3202-M430's present date and time.
System Resource	
CPU Usage	This displays what percentage of the LTE3202-M430's processing ability is currently used. When this percentage is close to 100%, the LTE3202-M430 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 LTE3202-M430 is using.
Interface Status	
Item	This displays the LTE3202-M430 port types. The port types are: WAN , LAN and WLAN .
Rate/Status	For the LAN and WAN ports, this field displays Off (line is down) or On (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. For the 2.4GHz WLAN, it displays On when the 2.4GHz WLAN is enabled or Off 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.
Data Usage	
Total Allowance	This displays the limiting amount of the package data,
Total Traffic	This displays the total traffic flows transmitting from/to the LTE3202-M430.
Upload	This indicates the amount of transmitted data (in KB) on the LTE3202-M430.
Download	This indicated the amount of received data (in KB) on the LTE3202-M430.
Operating Mode	
This is the device mode to which the LTE3202-M430's wireless LAN is set - Router Mode or Bridge Mode .	
Summary	
Packet Statistics	Click Details... to go to the Monitor > Packet statistics screen (Section 5.6 on page 30). Use this screen to view port status and packet specific statistics.

Table 6 Status


LABEL	DESCRIPTION
WLAN Station Status	Click Details... to go to the Monitor > WLAN station status screen (Section 5.7 on page 31). Use this screen to view the wireless stations that are currently associated to the LTE3202-M430's 2.4GHz wireless LAN.
LTE Modem Status	Click Details... to go to the Monitor > LTE modem status screen (Section 5.8 on page 31). 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 5

Monitor

5.1 Overview

This chapter discusses read-only information related to the device state of the LTE3202-M430.

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 LTE3202-M430.

5.2 What You Can Do

- Use the **Log** screen to see the logs for the activity on the LTE3202-M430 ([Section 5.3 on page 27](#)).
- Use the **DHCP Table** screen to view information related to your DHCP status ([Section 5.4 on page 28](#)).
- Use the **ARP Table** screen to view the mapping of IP and MAC addresses ([Section 5.5 on page 29](#)).
- Use the **Packet Statistics** screen to view port status, packet statistics, the system up time ([Section 5.6 on page 30](#)).
- Use the **WLAN station status** screen to view the wireless stations that are currently associated to the LTE3202-M430 ([Section 5.7 on page 31](#)).
- 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 5.8 on page 31](#)).

5.3 The Log Screen

The Web Configurator allows you to look at all of the LTE3202-M430's logs in one location.

Figure 11 Monitor > Log

Log

Enable Log

Log Level All ▾

Enable Remote Log

Remote Log Host

Remote Log Port

System Log Display

```

/usr/sbin/mm_watchdog
Jul 3 05:31:01 mdm9607 LTE[676]: [LTE] LTE signal strength: -57-dbm, -91-rsrp, -10-rsrq
Jul 3 05:31:16 mdm9607 LTE[676]: [LTE] LTE signal strength: -64-dbm, -94-rsrp, -11-rsrq
Jul 3 05:31:23 mdm9607 LTE[676]: [LTE] LTE signal strength: -57-dbm, -91-rsrp, -11-rsrq
Jul 3 05:31:27 mdm9607 LTE[676]: [LTE] LTE signal strength: -59-dbm, -93-rsrp, -11-rsrq
Jul 3 05:31:55 mdm9607 LTE[676]: [LTE] LTE signal strength: -65-dbm, -92-rsrp, -9-rsrq
Jul 3 05:31:59 mdm9607 LTE[676]: [LTE] LTE signal strength: -59-dbm, -93-rsrp, -11-rsrq
Jul 3 05:32:00 mdm9607 crond[3346]: USER root pid 20694 cmd
/usr/sbin/mm_watchdog
Jul 3 05:32:02 mdm9607 LTE[676]: [LTE] LTE signal strength: -64-dbm, -92-rsrp, -9-rsrq

```

The following table describes the labels on this screen.

Table 7 Monitor > Log

LABEL	DESCRIPTION
Enable Log	Select this to enable Log
Log Level	
Enable Remote Log	Select this to send the logs to a remote host.
Remote Log Host	Enter the remote host's IP address.
Remote Log Port	Enter the port used for this service.
Apply	Click Apply to save your changes back to the LTE3202-M430.
Cancel	Click Cancel to reload the previous configuration for this screen.
Refresh	Click Refresh to renew the Log screen.

5.4 The DHCP Table Screen

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 LTE3202-M430's LAN as a DHCP server or disable it. When configured as a server, the LTE3202-M430 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 LTE3202-M430's DHCP server.

Figure 12 Monitor > DHCP Table

No.	Status	Host Name	IP Address	MAC Address	Reserve
<div style="display: flex; justify-content: space-around;"> Apply Cancel </div>					

The following table describes the labels on this screen.

Table 8 Monitor > DHCP Table

LABEL	DESCRIPTION
No.	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.
Apply	Click Apply to save your changes back to the LTE3202-M430.
Cancel	Click Cancel to reload the previous configuration for this screen.

5.5 The ARP Table Screen

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 mapping(s).

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

Figure 13 Monitor > ARP Table

No.	IP Address	MAC Address	Device	State
1	192.168.1.9	00:e0:4c:68:02:18	lan	completed

The following screen describes the labels on this screen.

Table 9 Monitor > ARP Table

LABEL	DESCRIPTION
No.	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.
Device	This is the type of interface used by the device. <ul style="list-style-type: none"> • LAN indicates a LAN interface where 0 represents LAN1 or LAN2. • WLAN indicates a connection via WiFi network.
State	This column shows the current status of the connection.

5.6 The Packet Statistics Screen

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".

Figure 14 Monitor > Packet Statistics

Packet Statistics								
No.	Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
1	WWAN	up	4011	3081	0	434848	417774	00:00:10:24
2	LAN	up	22637	45131	0	13808349	13731100	04:21:22:34
3	WLAN	up	275	25312	0	62902	5968080	04:21:22:34

The following table describes the labels on this screen.

Table 10 Monitor > Packet Statistics

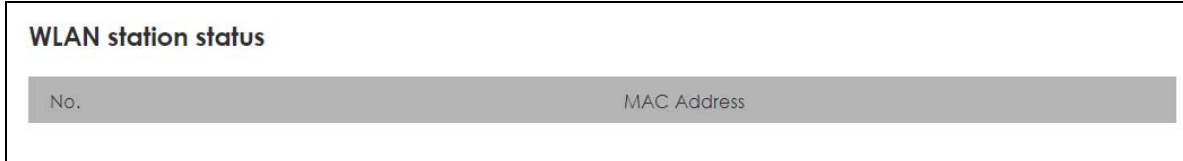
LABEL	DESCRIPTION
No.	This is the index number of the entry.
Port	This is the LTE3202-M430's interface type.
Status	For the LAN ports, this displays the port speed and duplex setting or Down when the line is disconnected. For the WAN port, it displays Up when the mobile data connection is up, Connecting when the LTE3202-M430 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 LTE3202-M430 has been for each session.

5.7 The WLAN Station Status Screen

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 LTE3202-M430's 2.4GHz 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 15 Monitor > WLAN station status



The screenshot shows a window titled "WLAN station status". Below the title is a table with two columns: "No." and "MAC Address". The table is currently empty.

The following table describes the labels on this screen.

Table 11 Monitor > WLAN station status

LABEL	DESCRIPTION
No.	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.

5.8 The LTE Modem Status Screen

Click **Monitor > LTE modem status** to open the following screen

Figure 16 Monitor > LTE modem status

LTE Modem Status									
Modem Information									
Module Name	IMEI/MEID	HW Version		FW Version					
LTE3202	357407090001997	01		V1.00(ABNH.0)B2					
SIM Status									
SIM	PIN Code Status		PIN Code Remaining Times		PUK Code Remaining Times				
PRESENT	PIN is disabled		3		10				
Service Information									
Operator	MCC	MNC	LAC	TAC	Cell ID	Service Type	Operation Band	RSSI	
	466	1		59242	56410647	LTE	4G 2600MHz (B7)	-60	
Register Status	Ecio	CS Attached Status		PS Attached Status		Roaming Status	IMSI	SMSC	MSISDN
Registered		Attached		Attached		Not Roaming	466011801 891892		
RSRP	RSRQ	SINR	PLMN	MIMO	Support Band List				
-92	-11	13	4661	2T2R	GSM band: 3,8,2/WCDMA band: 1,2,8/LTE band: 1,3,7,8,20,28,38,40				

The following table describes the labels on this screen.

Table 12 Monitor > LTE modem status

LABEL	DESCRIPTION
Modem Information	
Module Name	This displays the name of the built-in LTE module.
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	
SIM	This displays the status of the inserted SIM card. N/A displays if there is no SIM card inserted.
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.
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.

Table 12 Monitor > LTE modem status

LABEL	DESCRIPTION
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 LTE3202-M430 is connecting.
Operation Band	This displays the network type and the frequency band used by the mobile network to which the LTE3202-M430 is connecting.
RSSI	This displays the received signal strength indicator (RSSI), that is, the received signal strength in dBm.
Register Status	This displays the packet switched network registration status.
Ecio	This displays the ratio (in dB) of the received energy per chip and the interference level.
CS Attached Status	This displays the Circuit Switched network registration status.
PS Attached Status	This displays the Packet switched Domain Attachment status.
Roaming Status	This displays whether the LTE3202-M430 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.
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 LTE3202-M430, 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 LTE3202-M430.

CHAPTER 6

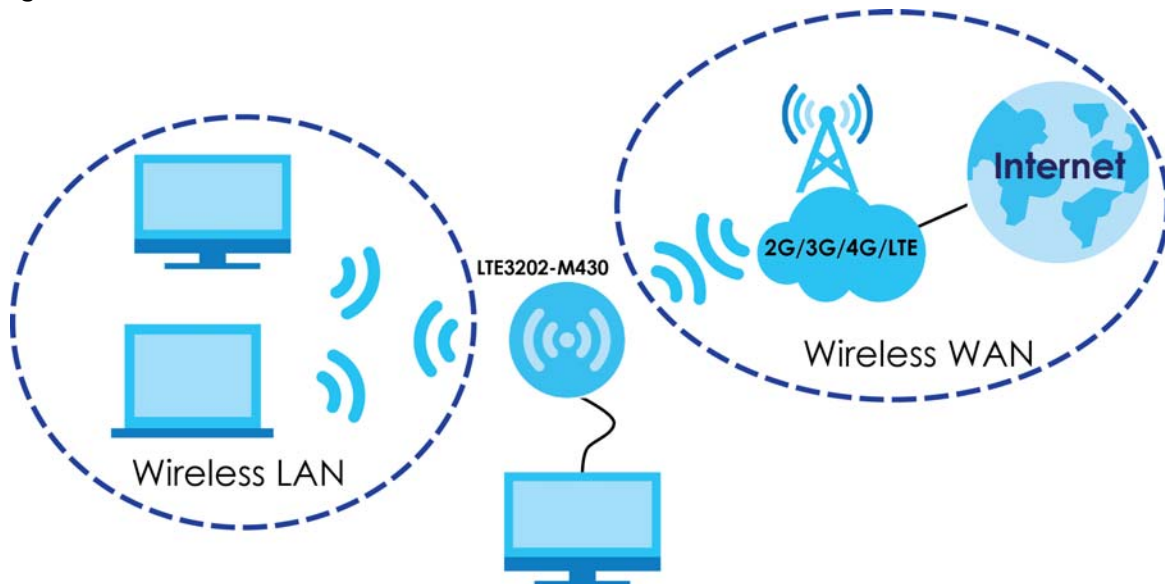
WAN Network

6.1 Overview

This chapter discusses the LTE3202-M430's **WAN network** screens. Use these screens to configure your LTE3202-M430 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.

Figure 17 LAN/Wireless LAN and Wireless WAN



6.1.1 What You Can Do in this Chapter

- Use the **Cellular Network** screen to configure the WAN settings on the LTE3202-M430 for Internet access ([Section 6.2 on page 35](#)).
- Use the **PIN Settings** screen to enable or disable PIN code authentication ([Section 6.3 on page 35](#)).
- Use the **APN Configuration** screen to configure user-defined connection profiles ([Section 6.4 on page 36](#)).
- Use the **Network Selection** screen to display available Public Land Mobile Networks and select a preferred network for roaming ([Section 6.5 on page 37](#)).
- Use the **Data Usage/Statistic** screen to specify limiting the amount of the package data and view the LTE3202-M430's traffic statistics ([Section 6.6 on page 38](#)).
- Use the **Operating Mode** screen to change your LTE3202-M430 mode of operation ([Section 6.7 on page 39](#)).

- Use the **Antenna Selection** screen to configure which antennas the LTE3202-M430 uses (Section 6.8 on page 40)

6.2 The Cellular Network Screen

Use this screen to change your LTE3202-M430's Internet access settings. Click **Configurariion > WAN network > Cellular Network**. The screen appears as shown next.

Figure 18 Configuration > WAN network > Cellular Network

The screenshot shows the 'Cellular Network' configuration screen. It includes the following elements:

- Network Type:** A dropdown menu currently set to 'Auto'.
- Roaming:** A checkbox that is currently unchecked, labeled 'Enable'.
- Connection Control:** A dropdown menu currently set to 'Manual', with a blue 'Disconnect' button to its right.
- Buttons:** Two blue buttons at the bottom: 'Apply' and 'Cancel'.

The following table describes the labels in this screen.

Table 13 Configuration > WAN network > Internet Status

LABEL	DESCRIPTION
Cellular Network	
Network Type	Select the type of the network (4G , 3G , or 2G) to which you want the LTE3202-M430 to connect and click Apply to save your settings. Otherwise, select Auto to have the LTE3202-M430 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 LTE3202-M430 switches to another available mobile network.
Roaming	Select this check box to enable data roaming on the LTE3202-M430. 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 LTE3202-M430 is kept connected to the Internet when you are traveling outside the geographical coverage area of the network to which you are registered.
Connection Control	Select Auto to connect to the mobile network automatically if there is an available mobile network. Otherwise, select Manual .
Apply	Click Apply to save your changes back to the LTE3202-M430.
Cancel	Click Cancel to reload the previous configuration for this screen.

6.3 The PIN Settings Screen

Use this screen to turn on or turn off PIN code authentication on the inserted SIM card. Click **Configuration > WAN network > PIN Settings**. The screen appears as shown next.

Figure 19 Configuration > WAN Network > PIN Settings

The following table describes the labels in this screen.

Table 14 Configuration > WAN network > PIN Settings

LABEL	DESCRIPTION
PIN Protection	
Enable PIN Protection	Select this to turn on PIN code authentication. Otherwise, click deselect the checkbox to turn off 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.
PIN Code	Enter the default or existing PIN code for the inserted SIM card.
Apply	Click Apply to save your changes back to the LTE3202-M430.
Cancel	Click Cancel to reload the previous configuration for this screen.

6.4 The APN Configuration Screen

Use this screen to view or configure a connection profile. A connection profile defines the parameters that you need to connect to a mobile network, such as the APN, user name and password. Click **Configuration > WAN network > APN Configuration**. The screen appears as shown next.

Figure 20 Copnfiguration > WAN network > APN Configuration

The following table describes the labels in this screen.

Table 15 Configuration > WAN network > APN Configuration

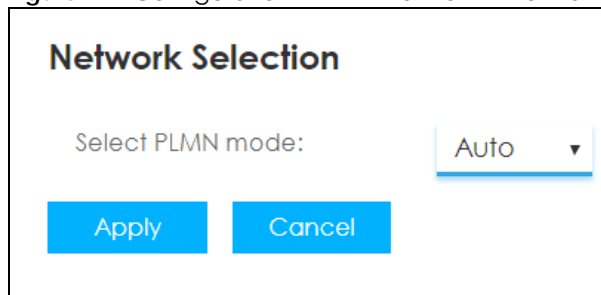
LABEL	DESCRIPTION
APN Profile	Select Auto to reload the default profile. Otherwise, select Manual to configure a connection profile.
APN	This field displays the Access Point Name (APN) in the profile. Enter the Access Point Name (APN) provided by your service provider. Connections with different APNs may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charging method. You can enter up to 30 printable ASCII characters. Spaces are allowed.
Username	This field displays the user name in the profile. Type the user name (of up to 31 printable ASCII characters) given to you by your service provider.
Password	This field displays the password in the profile. Type the password (of up to 31 printable ASCII characters) associated with the user name above.
Authentication	The LTE3202-M430 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 used by the service provider. Otherwise, select Auto to have the LTE3202-M430 accept this automatically. Select None , to accept neither.
PDP type	<ul style="list-style-type: none"> • Select Default to use the ISP's default settings. • Select IP if you want the LTE3202-M430 to run IPv4 only. • Select IPv4v6 to allow the LTE3202-M430 to run IPv4 and IPv6 at the same time. • Select IPv6 if you want the LTE3202-M430 to run IPv6 only.
Apply	Click Apply to save your changes back to the LTE3202-M430.
Reset	Click Reset to reload the previous configuration for this screen.

6.5 The Network Selection Screen

This screen allows you to view available Public Land Mobile Networks (PLMNs) and select your preferred network when the LTE3202-M430 is outside the geographical coverage area of the network to which you are registered and roaming is enabled.

Click **Configuration > WAN network > Network Selection**. The screen appears as shown next.

Figure 21 Configuration > WAN network > Network Selection



The following table describes the labels in this screen.

Table 16 Configuration > WAN network > Network Selection

LABEL	DESCRIPTION
Select PLMN Mode	Select Auto to have the LTE3202-M430 automatically connect to the first available mobile network using roaming when it is outside the coverage area of the original service provider's network. Select Manual to display the network list and manually select a preferred network.
Apply	Click Apply to save your changes back to the LTE3202-M430.
Cancel	Click Cancel to reload the previous configuration for this screen.

6.6 Data Usage/Statistic Screen

This screen allows you to configure limiting the amount of the package data and view the LTE3202-M430's traffic statistics.

Click **Configuration > WAN network > Data Usage/Statistic**. The screen appears as shown next.

Figure 22 Configuration > WAN network > Data Usage/Statistic

Data Usage/ Statistic

Package Data Limit Setting

Enable data limit

Total allowance: GB ▾

Notify me when data usage reaches: %

Reset date:
 Date of each month

Apply
Reset

Reset Network Statistics

Reset all of the statistic and history Reset

Current Connection Statistics

Data flow: 0KB

Sent: 0KB

Received: 0KB

Current Connection Time: 00:04:19

Total Connections Statistics

From: 0701

Data flow: 78KB/1GB

Sent: 10KB

Received: 68KB

Total Connection Time: 56:06:28

The following table describes the labels in this screen.

Table 17 Configuration > WAN network > Data Usage/Statistic

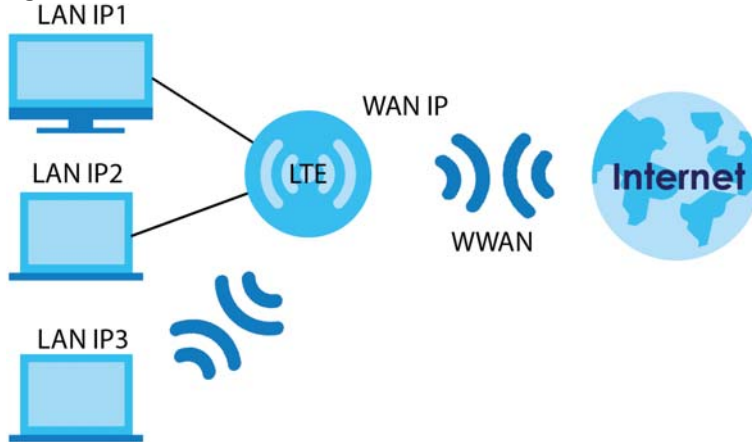
LABEL	DESCRIPTION
Package Data Limit Setting	
Enable data limit	Select the check box to enable data limits.
Total allowance	Specify the limiting the amount of the package data (in GB) in this field.
Notify me when data usage reaches	Specify the reminding percentage of the package data usage in this field.
Reset date	Specify the date that you want the LTE3202-M430 to restart calculating the amount of the package data per month.
Apply	Click Apply to save your changes back to the LTE3202-M430.
Reset	Click Reset to reload the previous configuration for this screen.
Reset Network Statistics	
Reset all of the statistics and history	Click Reset to remove all traffic statistics.
Current Connection Statistics	
Data Flow	This indicates the current traffic flow transmitting from/to the LTE3202-M430.
Sent	This indicates the number of transmitted packets on the LTE3202-M430.
Received	This indicates the number of received packets on the LTE3202-M430.
Current Connection Time	This indicates how long the LTE3202-M430 has been connected to a 4G/3G/2G network, this time returns to 0 each time the LTE3202-M430 is rebooted.
Total Connection Statistics	
From	This displays the start month and date (mmdd) for the statistics.
Data Flow	This indicates total traffic flows transmitting from/to the LTE3202-M430.
Sent	This indicates the number of transmitted packets on the LTE3202-M430.
Received	This indicates the number of received packets on the LTE3202-M430.
Total Connection Time	This indicates how long the LTE3202-M430 has been connected to a 4G/3G/2G network from the first time this device is booted until the LTE3202-M430 is reset to factory-default settings.

6.7 The Operation Mode Screen

The LTE3202-M430 supports two operation modes: Router Mode and Bridge Mode.

- **Router mode:** This is the default operating mode of the LTE3202-M430. Use the router mode if you want to use routing functions, such as firewall, DHCP, NAT, and so on. The following figure shows an example of the LTE3202-M430 in router mode.

Figure 23 LTE3202-M430 in Router Mode



- **Bridge Mode:** Select this mode if you already have a router in your network, and you don't want to reconfigure your network. If you don't have a router, you'll need multiple IP addresses from your ISP for your clients.

Use this screen to change the LTE3202-M430's operating mode. Click **Configuration > WAN network > Operation Mode** to open the following screen.

Figure 24 Configuration > WAN network > Operation Mode

6.8 The Antenna Selection Screen

Click **Configuration > WAN network > Antenna Selection** to open the following screen.

The LTE3202-M430 has two internal antennas, you can also install two external antennas to improve your wireless WAN signal strength. The LTE3202-M430 uses the internal antennas by default. If you installed external antennas, select **External** for the LTE3202-M430 to use these to detect the WAN network. Click **Apply** to save your settings, otherwise select **Cancel**.

Figure 25 Configuration > WAN network > Antenna Selection

CHAPTER 7

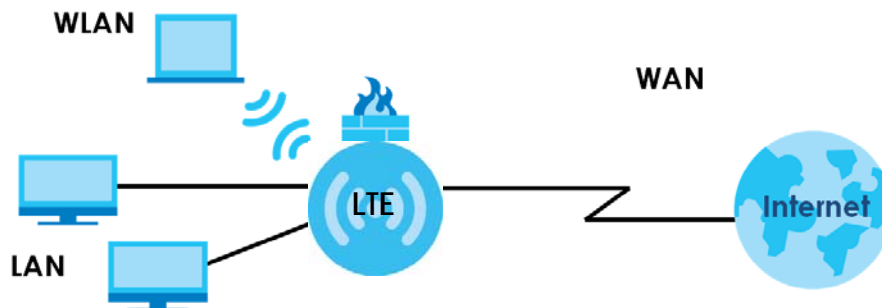
LAN

7.1 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 26 LAN Example



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

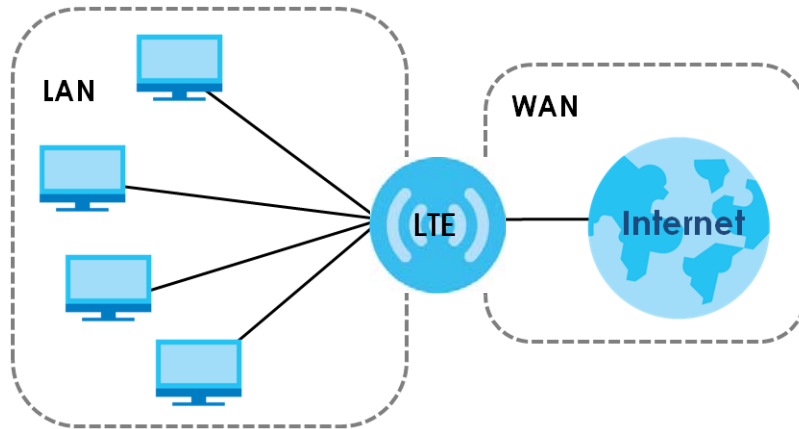
7.2 What You Can Do

- Use the **LAN IP** screen to configure the LTE3202-M430's LAN IP address ([Section 7.4 on page 42](#)).
- Use the **DHCP Server** screen to enable the DHCP server on the LTE3202-M430 ([Section 7.5 on page 43](#)).
- Use the **DNS Settings** screen to configure the LTE3202-M430's DNS settings ([Section 7.6 on page 44](#)).

7.3 What You Need To Know

The actual physical connection determines whether the LTE3202-M430 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 27 LAN and WAN IP Addresses



The LAN parameters of the LTE3202-M430 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.

7.4 The LAN IP Screen

To access this screen, click **Configuration** > **LAN network** > **LAN IP**. Use this screen to view or configure the management IP address for your LTE3202-M430. Click **Apply** to save your changes back to the LTE3202-M430, or click **Cancel** to reload the previous configuration for this screen.

Note: If you change the LTE3202-M430's IP address, you need to use the new IP address to access the LTE3202-M430's web configurator.

Figure 28 Configuration > LAN network > LAN IP

LAN IP

IP address

Subnet mask . . .

The following table describes the labels in this screen.

Table 18 Router > LAN IP

LABEL	DESCRIPTION
IP Address	This shows the default LAN IP address. Enter the new IP address for the LTE3202-M430's LAN interface if you want to change it.
Subnet Mask	This shows the default subnet mask. Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Apply	Click Apply to save your changes back to the LTE3202-M430.
Cancel	Click Cancel to reload the previous configuration for this screen.

7.5 The DHCP Server Screen

The LTE3202-M430 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. To access this screen, click **Configuration > LAN network > DHCP Server**.

Figure 29 Configuration > LAN network > DHCP Server

DHCP Settings

DHCP Enable Disable

DHCP range 100 ~ 200

DHCP lease time(s) 86400

Apply Cancel

Static DHCP List

Static IP 1 /30 Add New Delete All

	IP address	MAC address	Action
1	192.168.1.200	aa:bb:11:22:cc:dd	Edit Delete

Apply Cancel

The following table describes the labels in this screen.

Table 19 Router > DHCP Server

LABEL	DESCRIPTION
DHCP Settings	
DHCP	Select to Enable or Disable the DHCP server on the LTE3202-M430.

Table 19 Router > DHCP Server

LABEL	DESCRIPTION
DHCP range	The LTE3202-M430 is pre-configured with a pool of 240 IP addresses starting from 192.168.0.10 to 192.168.0.250. Specify the first and last of the contiguous addresses in the IP address range.
DHCP 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.
Apply	Click Apply to save your changes back to the LTE3202-M430.
Cancel	Click Cancel to reload the previous configuration for this screen.
Static DHCP List	
Static IP	This displays how many Static IP addresses are configured in the LTE3202-M430.
Add New	Click Add New to create a new entry.
Delete all	Click Delete All to remove all entries.
	This field displays the index number of the static IP address entry.
IP Address	This field displays the IP address that the LTE3202-M430 assigns to a device with the entry's MAC address.
MAC Address	This field displays the MAC address of the device to which the LTE3202-M430 assigns the entry's IP address.
Action	Click Edit to go to the screen where you can edit the static IP address. Click Delete to remove the static IP address entry.
Apply	Click this button to save your changes back to the LTE3202-M430.
Cancel	Click Cancel to reload the previous configuration for this screen.

7.6 DNS Settings Screen

Click **Router > DNS Settings** to configure the LTE3202-M430's DNS settings. The following screen displays.

Figure 30 Router > DNS Settings

LAN IP

DNS Mode Auto Manual

Primary DNS

Secondary DNS

The following table describes the labels in this screen.

Table 20 Router > DNS Settings

LABEL	DESCRIPTION
DNS Mode	Select Auto if your ISP dynamically assigns DNS server information (and the LTE3202-M430's WAN IP address). Otherwise, select Manual if you have the IP address of a DNS server.
Primary DNS	Select Manual if you have the IP address of a DNS server.
Secondary DNS	Enter the DNS server's IP address in the field.
Apply	Click this button to save your changes back to the LTE3202-M430.
Cancel	Click Cancel to reload the previous configuration for this screen.

CHAPTER 8

WLAN

8.1 Overview

This chapter describes the LTE3202-M430's **WLAN** screens. Use these screens to set up your LTE3202-M430's wireless LAN connection.

8.1.1 What You Can Do in this Chapter

- Use the **WiFi Settings** screen to enable the wireless LAN, enter the SSID and select the wireless security mode ([Section 8.2 on page 47](#)).
- Use the **MAC Filter** screen to deny wireless clients based on their MAC addresses from connecting to the LTE3202-M430 ([Section 8.3 on page 50](#)).
- Use the **WPS** screen to activate WPS via PBC or PIN configuration ([Section 8.4 on page 51](#)).

8.1.2 What You Need to Know

Wireless Basics

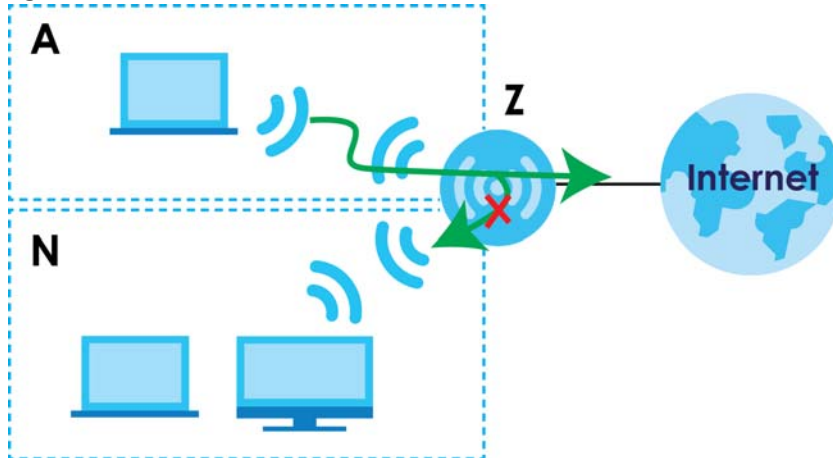
“Wireless” is essentially radio communication. In the same way that walkie-talkie radios send and receive information over the airwaves, wireless networking devices exchange information with one another. A wireless networking device is just like a radio that lets your computer exchange information with radios attached to other computers. Like walkie-talkies, most wireless networking devices operate at radio frequency bands that are open to the public and do not require a license to use. However, wireless networking is different from that of most traditional radio communications in that there are a number of wireless networking standards available with different methods of data encryption.

Guest WLAN

Guest WLAN allows you to set up a wireless network where users can access the Internet via the LTE3202-M430 (**Z**), but not other networks connected to the **Z**. In the following figure, a guest user can access the Internet from the guest wireless network **A** via **Z** but not the home or company network **N**.

Note: The home or company network **N** and Guest WLAN network are independent networks.

Figure 31 Guest Wireless LAN Network



See [Section 8.5 on page 52](#) for advanced technical information on wireless networks.

8.2 WiFi Settings Screen

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

Note: If you are configuring the LTE3202-M430 from a computer connected to the wireless LAN and you change the LTE3202-M430'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 LTE3202-M430's new settings.

To access this screen, click **Configuration > WLAN > WiFi Settings**.

Figure 32 Configuration > WLAN > WiFi Settings

WLAN Settings

Basic

Enable

WiFi network mode Auto b/g/n ▼

bandwidth 20MHz ▼

Channel Auto ▼

SSID Name Zyxel_35B4

SSID Broadcast

Maximum stations 16

Security mode WPA2-PSK ▼

Cypher mode AES ▼

WiFi key 9Q57KDMCDJ

Apply Cancel

Guest AP

Enable

SSID Name Zyxel_LTE3202

SSID Broadcast

Maximum stations 15

Security mode Security WPA2 ▼

Cypher mode AES ▼

WiFi key 9Q57KDMCDJ

Apply Cancel

The following table describes the labels in this screen.

Table 21 Configuration > WLAN > WiFi Settings

LABEL	DESCRIPTION
Basic / Guest AP	
Enable	Select the check box to enable the wireless LAN of the LTE3202-M430.

Table 21 Configuration > WLAN > WiFi Settings

LABEL	DESCRIPTION
WiFi network mode	<p>You can select from the following:</p> <ul style="list-style-type: none"> • b only: allows either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the LTE3202-M430. In this mode, all wireless devices can only transmit at the data rates supported by IEEE 802.11b. • g only: allows IEEE 802.11g compliant WLAN devices to associate with the Device. IEEE 802.11b compliant WLAN devices can associate with the LTE3202-M430 only when they use the short preamble type. • n only: allows IEEE 802.11n compliant WLAN devices to associate with the LTE3202-M430. This can increase transmission rates, although IEEE 802.11b or IEEE 802.11g clients will not be able to connect to the LTE3202-M430. • Auto b/g: allows either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the LTE3202-M430. The LTE3202-M430 adjusts the transmission rate automatically according to the wireless standard supported by the wireless devices. • Auto g/n: allows either IEEE 802.11g or IEEE 802.11n compliant WLAN devices to associate with the LTE3202-M430. The transmission rate of your LTE3202-M430 might be reduced. • Auto b/g/n: allows IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the LTE3202-M430. The transmission rate of your LTE3202-M430 might be reduced.
Bandwidth	<p>Select the wireless channel width used by LTE3202-M430.</p> <p>A standard 20MHz channel offers transfer speeds of up to 144Mbps (2.4GHz) whereas a 40MHz channel uses two standard channels and offers speeds of up to 300Mbps (2.4GHz).</p> <p>Because not all devices support 40 MHz channels, select wifi 2040 to allow the LTE3202-M430 to adjust the channel bandwidth automatically.</p> <p>40MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The wireless clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal.</p> <p>Select 20MHz if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding.</p>
Channel	<p>Set the channel depending on your particular region.</p> <p>Select a channel or use Auto to have the LTE3202-M430 automatically determine a channel to use. If you are having problems with wireless interference, changing the channel may help. Try to use a channel that is as many channels away from any channels used by neighboring APs as possible. The channel number which the LTE3202-M430 is currently using then displays next to this field.</p>
SSID Name	<p>The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID.</p> <p>Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.</p>
SSID Broadcast	<p>Select this check box to show the SSID in the outgoing beacon frame so a wireless client can obtain the SSID through scanning using a site survey tool. If you don't select this option the SSID will remain hidden.</p>
Maximum Stations	<p>Specify the maximum amount of wireless clients that can connect to the LTE3202-M430. For example, if this field is set to 16, then the 17th wireless client will not be able to connect to the LTE3202-M430's wireless network.</p>
Security mode	<p>Select WPA2-PSK or WPA/WPA2-PSK to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as this device. After you select to use a security, additional options appears in this screen. Or you can select None (Open) to allow any client to associate this network without authentication.</p> <p>Note: If the WPS function is enabled (default), only No Security and WPA2-PSK are available in this field.</p>

Table 21 Configuration > WLAN > WiFi Settings

LABEL	DESCRIPTION
Cypher mode	Select the type of security you want to use (TKIP or AES) to secure traffic on your WDS. Otherwise, select No Security . Select TKIP to enable Temporal Key Integrity Protocol (TKIP) security on your WDS. This option is compatible with other ZyXEL access points that support WDS security. Use this if the other access points on your network support WDS security but do not have an AES option. AES provides superior security to TKIP. Use AES if the other access points on your network support it for the WDS.
WiFi key	Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols). You must also set the peer device to use the same pre-shared key.
Apply	Click Apply to save your changes back to the LTE3202-M430.
Cancel	Click Cancel to reload the previous configuration for this screen.

8.3 MAC Filter Screen

This screen allows you to configure the LTE3202-M430 to exclude specific devices from accessing the LTE3202-M430 (**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 addresses of the devices to configure this screen.

Use this screen to view your LTE3202-M430's MAC filter settings and add new MAC filter rules. Click **Configuration > WLAN > MAC Filter**. The screen appears as shown.

Figure 33 Configuration > WLAN > MAC Filter

WLAN MAC Filter

MAC Filter mode

MAC Filter method: Blacklist description ▾

Blacklist: 1/10 Add New Delete All

	MAC address	Description	Action
1	aa:bb:11:22:33:aa	PC1	Edit Delete

Apply Cancel

The following table describes the labels in this screen.

Table 22 Configuration > WLAN > MAC Filter

LABEL	DESCRIPTION
MAC Filter Mode	Select the checkbox to prohibit devices with the MAC addresses you configured.
MAC Filter method	Select Whitelist description to permit access to the LTE3202-M430, MAC addresses not listed will be denied access to the LTE3202-M430. Select Blacklist description to block access to the LTE3202-M430, MAC addresses not listed will be allowed to access the LTE3202-M430.
Blacklist/Whitelist	This displays how many entries you have in the Whitelist description/Blacklist description summary tables.
Add New	Click Add New to create a MAC Filtering rule.
Delete All	Click Delete All to remove all MAC Filtering rules.
MAC address	This field displays the MAC addresses of the wireless devices that are allowed or denied access to the LTE3202-M430. Click Add New or Edit to enter or change the MAC address of the wireless devices that are allowed or denied access to the LTE3202-M430 in this field. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Description	This field displays the name of the MAC address entry. Click Add New or Edit to enter a descriptive name to identify the MAC address entry. You can enter up to 20 printable ASCII characters. Spaces are allowed.
Action	Click Edit to go to the screen where you can edit the rule. Click Delete to remove the MAC address entry.
Apply	Click Apply to save your changes back to the LTE3202-M430.
Cancel	Click Cancel to reload the previous configuration for this screen.

8.4 WPS Screen

Use this screen to configure WiFi Protected Setup (WPS) on your LTE3202-M430.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Set up each WPS connection between two devices. Both devices must support WPS. See [Section 8.5.5.3 on page 59](#) for more information about WPS.

Click **Configuration > WLAN > WPS**. The following screen displays.

Figure 34 Configuration > WLAN > WPS: PBC Method

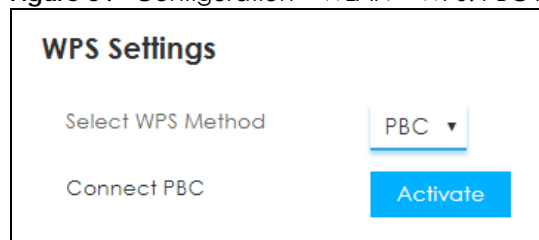


Figure 35 Configuration > WLAN > WPS: PIN Method

The following table describes the labels in this screen.

Table 23 Configuration > WLAN > WPS

LABEL	DESCRIPTION
WPS Settings	
Select WPS Method	<ul style="list-style-type: none"> Select PBC to set up a WPS wireless network using Push Button Configuration (PBC). If you select PBC, click Activate to add another WPS-enabled wireless device (within wireless range of the LTE3202-M430) to your wireless network. You may either click Activate or press physical button on the LTE3202-M430 rear panel. <p>Note: You must press the other wireless device's WPS button within two minutes of pressing this button.</p> <ul style="list-style-type: none"> Select PIN to set up a WPS wireless network by entering the PIN of the client into the LTE3202-M430.
Enter device PIN	<p>This field is available only when you set Select WPS Method to PIN.</p> <p>Select this option and enter the PIN of the device that you are setting up a WPS connection with and click Apply to authenticate and add the wireless device to your wireless network.</p> <p>You can find the PIN either on the outside of the device, or by checking the device's settings.</p> <p>Note: You must also activate WPS on that device within two minutes to have it present its PIN to the LTE3202-M430.</p>

8.5 Technical Reference

This section discusses wireless LANs in depth.

8.5.1 Wireless Network Overview

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

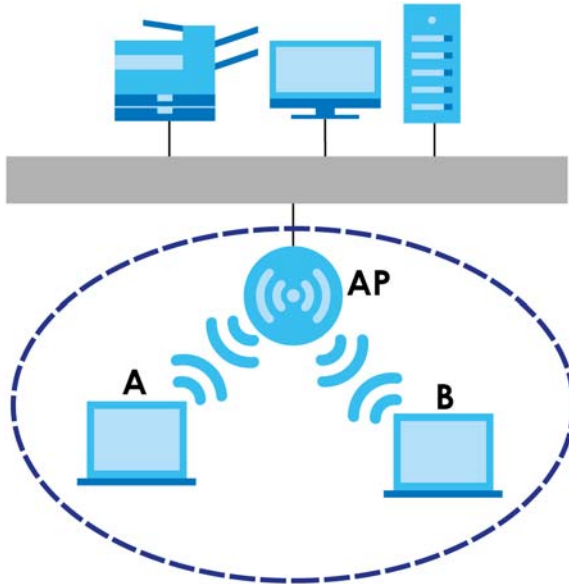
- A wireless client is a radio connected to a user's computer.
- An access point is a radio with a wired connection to a network, which can connect with numerous wireless clients and let them access the network.
- A bridge is a radio that relays communications between access points and wireless clients,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

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

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

The following figure provides an example of a wireless network.

Figure 36 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** use the access point (**AP**) to interact with the other devices (such as the printer) or with the Internet. Your LTE3202-M430 is the AP.

Every wireless network must follow these basic guidelines.

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

Radio Channels

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

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

8.5.2 Additional Wireless Terms

The following table describes some wireless network terms and acronyms used in the LTE3202-M430's Web Configurator.

Table 24 Additional Wireless Terms

TERM	DESCRIPTION
RTS/CTS Threshold	<p>In a wireless network which covers a large area, wireless devices are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through.</p> <p>By setting this value lower than the default value, the wireless devices must sometimes get permission to send information to the LTE3202-M430. The lower the value, the more often the devices must get permission.</p> <p>If this value is greater than the fragmentation threshold value (see below), then wireless devices never have to get permission to send information to the LTE3202-M430.</p>
Preamble	A preamble affects the timing in your wireless network. There are two preamble modes: long and short. If a device uses a different preamble mode than the LTE3202-M430 does, it cannot communicate with the LTE3202-M430.
Authentication	The process of verifying whether a wireless device is allowed to use the wireless network.
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.

8.5.3 Wireless Security Overview

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

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

These security standards vary in effectiveness. Some can be broken, such as the old Wired Equivalent Protocol (WEP). Using WEP is better than using no security at all, but it will not keep a determined attacker out. Other security standards are secure in themselves but can be broken if a user does not use them properly. For example, the WPA-PSK security standard is very secure if you use a long key which is difficult for an attacker's software to guess - for example, a twenty-letter long string of apparently random numbers and letters - but it is not very secure if you use a short key which is very easy to guess - for example, a three-letter word from the dictionary.

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

A good way to come up with effective security keys, passwords and so on is to use obscure information that you personally will easily remember, and to enter it in a way that appears random and does not include real words. For example, if your mother owns a 1970 Dodge Challenger and her favorite movie is

Vanishing Point (which you know was made in 1971) you could use "70dodchal71vanpoi" as your security key.

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

8.5.3.1 SSID

Normally, the LTE3202-M430 acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the LTE3202-M430 does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

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

8.5.3.2 MAC Address Filter

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

You can use the MAC address filter to tell the LTE3202-M430 which devices are allowed or not allowed to use the wireless network. If a device is allowed to use the wireless network, it still has to have the correct information (SSID, channel, and security). If a device is not allowed to use the wireless network, it does not matter if it has the correct information.

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

8.5.3.3 User Authentication

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

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

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



-
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.

8.5.3.4 Encryption

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

The types of encryption you can choose depend on the type of authentication. (See [Section 8.5.3.3 on page 55](#) for information about this.)

Table 25 Types of Encryption for Each Type of Authentication

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

For example, if the wireless network has a RADIUS server, you can choose **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no encryption, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every device in the wireless network supports. For example, suppose you have a wireless network with the LTE3202-M430 and you do not have a RADIUS server. Therefore, there is no authentication. Suppose the wireless network has two devices. 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. The other types of encryption are better than none at all, but it is still possible for unauthorized wireless devices to figure out the original information pretty quickly.

When you select **WPA2** or **WPA2-PSK** in your LTE3202-M430, you can also select an option (**WPA compatible**) to support WPA as well. In this case, if some of the devices 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 compatible** option in the LTE3202-M430.

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

8.5.4 Signal Problems

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

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

8.5.5 WiFi Protected Setup (WPS)

Your LTE3202-M430 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.

8.5.5.1 Push Button Configuration

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

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

Take the following steps to set up WPS using the button.

- 1 Ensure that the two devices you want to set up are within wireless range of one another.
- 2 Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the LTE3202-M430, see [Section 8.4 on page 51](#)).
- 3 Press the button on one of the devices (it doesn't matter which). For the LTE3202-M430 you must press the WPS button for more than three seconds.
- 4 Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through an secure connection to the enrollee.

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

8.5.5.2 PIN Configuration

Each WPS-enabled device has its own PIN (Personal Identification Number). This may either be static (it cannot be changed) or dynamic (in some devices you can generate a new PIN by clicking on a button in the configuration interface).

Use the PIN method instead of the push-button configuration (PBC) method if you want to ensure that the connection is established between the devices you specify, not just the first two devices to activate WPS in range of each other. However, you need to log into the configuration interfaces of both devices to use the PIN method.

When you use the PIN method, you must enter the PIN from one device (usually the wireless client) into the second device (usually the Access Point or wireless router). Then, when WPS is activated on the first

device, it presents its PIN to the second device. If the PIN matches, one device sends the network and security information to the other, allowing it to join the network.

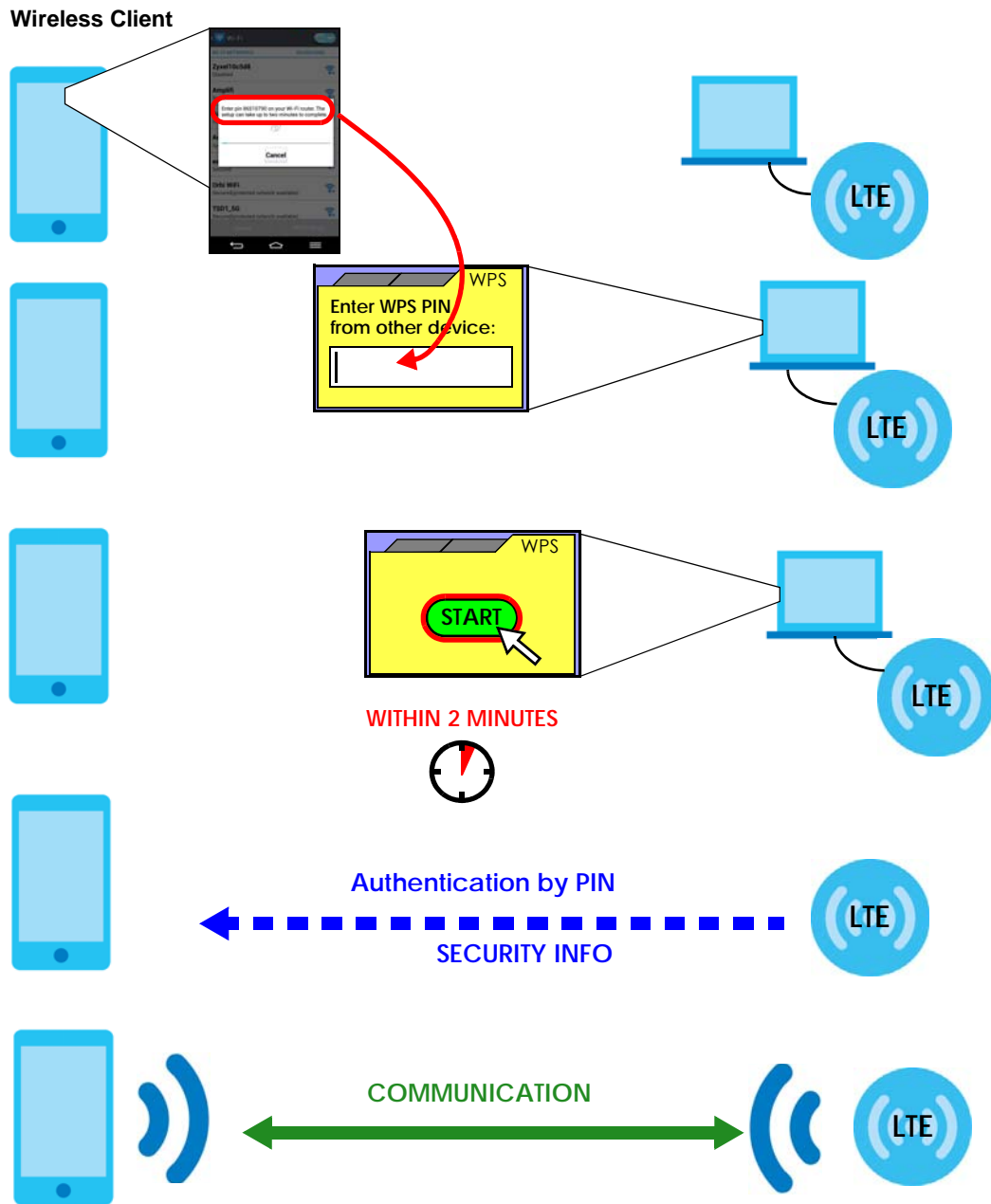
Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

- 1** Ensure WPS is enabled on both devices.
- 2** Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this.
- 3** Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide for how to find the WPS PIN - for the LTE3202-M430, see [Section 8.4 on page 51](#)).
- 4** Enter the client's PIN in the AP's configuration interface.
- 5** If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client - it does not matter which.
- 6** Start WPS on both devices within two minutes.
- 7** Use the configuration utility to activate WPS, not the push-button on the device itself.
- 8** On a computer connected to the wireless client, try to connect to the Internet. If you can connect, WPS was successful.

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

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

Figure 37 Example WPS Process: PIN Method

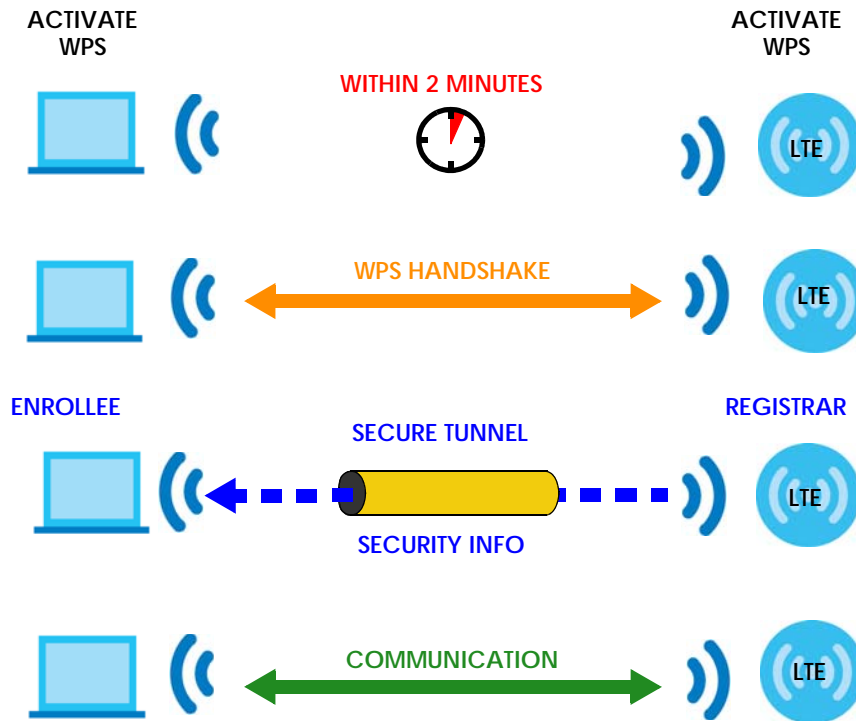


8.5.5.3 How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings). The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPA-PSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is already part of a network, it sends the existing information. If not, it generates the SSID and WPA(2)-PSK randomly.

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

Figure 38 How WPS works



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

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

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

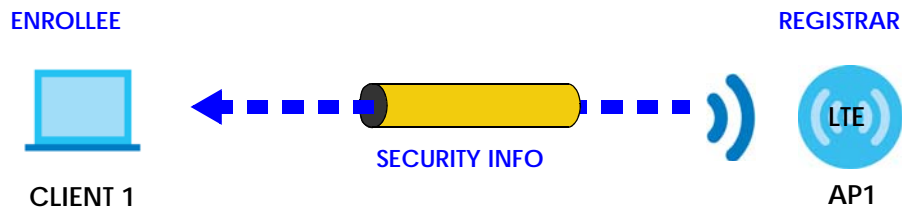
By default, a WPS device is "unconfigured". This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled device has connected to another device using WPS, it becomes "configured". A configured wireless client can still act as enrollee or registrar in subsequent WPS connections, but a configured access point can no longer act as enrollee. It will be the registrar in all subsequent WPS connections in which it is involved. If you want a configured AP to act as an enrollee, you must reset it to its factory defaults.

8.5.5.4 Example WPS Network Setup

This section shows how security settings are distributed in an example WPS setup.

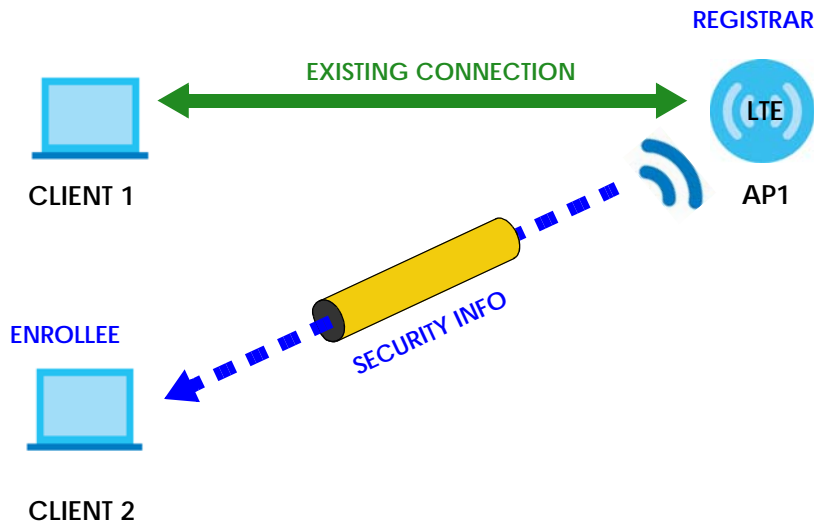
The following figure shows an example network. In step 1, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information.

Figure 39 WPS: Example Network Step 1



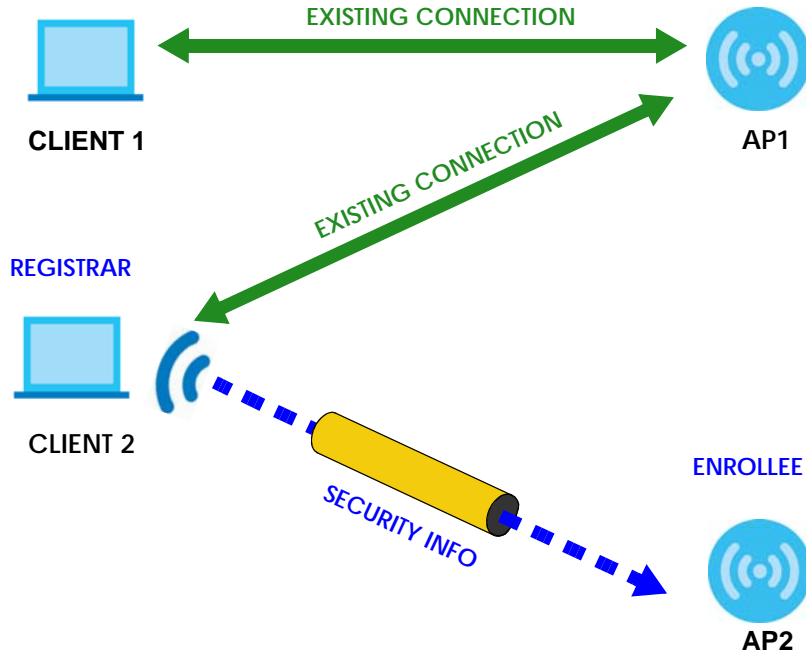
In step 2, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar, since it is configured (it already has security information for the network). **AP1** supplies the existing security information to **Client 2**.

Figure 40 WPS: Example Network Step 2



In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

Figure 41 WPS: Example Network Step 3



8.5.5.5 Limitations of WPS

WPS has some limitations of which you should be aware.

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

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

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

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

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

You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point's configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the access

point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.

CHAPTER 9

Firewall

9.1 Overview

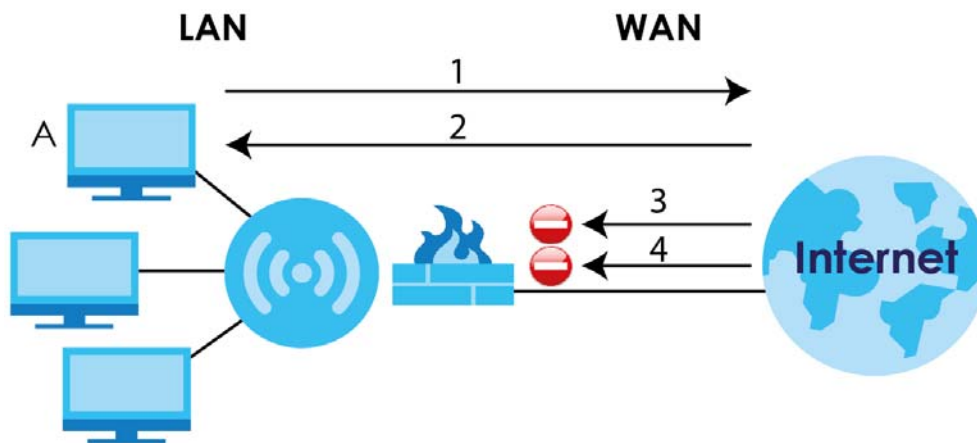
Use these screens to enable and configure the firewall that protects your LTE3202-M430 and your LAN from unwanted or malicious traffic.

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 42 Default Firewall Action



9.1.1 What You Can Do

- Use the **DoS Protection** screen to enable Denial of Service (DoS) protection in the LTE3202-M430 ([Section 9.2 on page 66](#)).
- Use the **ICMP Protection** screen to enable ICMP protection in the LTE3202-M430 ([Section 9.3 on page 67](#)).
- Use the **ARP Protection** screen to enable ARP protection in the LTE3202-M430 ([Section 9.4 on page 67](#)).
- Use the **URL Filter** screen to view and configure content filtering rules ([Section 9.5 on page 68](#)).
- Use the **IPv4 Port Filter** screen to view and configure IPv4/Port filtering rules ([Section 9.6 on page 69](#)).
- Use the **IPv6 Port Filter** screen to view and configure IPv6/Port filtering rules ([Section 9.7 on page 71](#)).

9.1.2 What You Need To Know

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

About the LTE3202-M430 Firewall

The LTE3202-M430'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 LTE3202-M430's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The LTE3202-M430 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 LTE3202-M430 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 LTE3202-M430 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 e-mail, FTP and the World Wide Web. However, "inbound access" is not allowed (by default) unless the remote host is authorized to use a specific service.

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.

9.2 The DoS Protection Screen

Use this screen to enable DoS (Denial of Service) protection on the LTE3202-M430.

Denial of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources.

SYN attack floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response, While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer (which is set a relatively long intervals) terminates the TCP three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

ICMP attack floods a targeted system with ICMP/PING echo requests.

Click **Configuration > Firewall > DoS Protection** to open the following screen.

Figure 43 Configuration > Firewall > DoS Protection

The screenshot shows the 'DoS protection' configuration screen. At the top, there is a checked checkbox labeled 'Enable DoS protection'. Below this, there are two unchecked checkboxes: 'SYN Flood' with a value of 128 and 'ICMP Flood' with a value of 100, both labeled 'packets per sec'. At the bottom of the screen, there are two buttons: 'Apply' and 'Cancel'.

The following table describes the labels on this screen.

Table 26 Configuration > Firewall > DoS Protection

LABEL	DESCRIPTION
DoS Protection	
Enable DoS protection	Select this check box to enable DoS protection.
SYN Flood	Select this to enable TCP SYN flood attack protection and specify the maximum number of packets allowed per second. If the TCP SYN packets exceed the threshold the LTE3202-M430 drops the over flooding packets.
ICMP Flood	Select this to enable ICMP flood attack protection and specify the maximum number of packets allowed per second. If the ICMP packets exceed the threshold the LTE3202-M430 drops the over flooding packets.
Apply	Click Apply to save your changes back to the LTE3202-M430.
Cancel	Click Cancel to reload the previous configuration for this screen.

9.3 The ICMP Protection Screen

If an outside user attempts to probe an unsupported port on your LTE3202-M430, an ICMP response packet is automatically returned. This allows the outside user to know the LTE3202-M430 exists. Use this screen to prevent the ICMP response packet from being sent. This keeps outsiders from discovering your LTE3202-M430 when unsupported ports are probed.

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

Click **Configuration > Firewall > ICMP Protection** to open the following screen.

Figure 44 Configuration > Firewall > ICMP Protection

The following table describes the labels on this screen.

Table 27 Configuration > Firewall > ICMP Protection

LABEL	DESCRIPTION
ICMP Protection	
Enable WAN Ping	The LTE3202-M430 will not respond to any incoming WAN Ping requests when this checkbox is not selected. Select Enable WAN Ping to reply to incoming WAN Ping requests.
Enable LAN Ping	The LTE3202-M430 will not respond to any incoming LAN Ping requests when this checkbox is not selected. Select Enable LAN Ping to reply to incoming LAN Ping requests.
Apply	Click Apply to save your changes back to the LTE3202-M430.
Cancel	Click Cancel to reload the previous configuration for this screen.

9.4 The ARP Protection Screen

Use this screen to enable (Address Resolution Protocol) ARP protection. This protects your LTE3202-M430 against ARP spoofing, by inspecting the ARP requests and replies comparing them against the information gathered through DHCP snooping to validate ARP packet and protect against ARP spoofing. Click **Configuration > Firewall > ARP Protection** to open the following screen.

Figure 45 Configuration > Firewall > ARP Protection

The following table describes the labels on this screen.

Table 28 Configuration > Firewall > ARP Protection

LABEL	DESCRIPTION
ARP Protection	
Enable ARP attack protecting	Select this to activate ARP protection.
LAN IP/MAC Binding List	Each ARP packet is intercepted and checked to verify if its IP/MAC binding is valid. The LTE3202-M430 only accepts packets sent by devices in this list, otherwise the packet will be dropped.
Add New	Click Add New to create a new rule.
Delete All	Click Delete All to remove all rules from the LAN IP/MAC Binding List.
	This field displays the rule index number.
IP address	Enter the IP address with which the LTE3202-M430 uses the IP/MAC binding to verify the ARP packets.
MAC address	Enter the MAC address with which the LTE3202-M430 uses the IP/MAC binding to verify the ARP packets.
Action	Click Edit to go to the screen where you can edit the filtering rule. Click Delete to remove the filtering rule.
Apply	Click Apply to save your changes back to the LTE3202-M430.
Cancel	Click Cancel to reload the previous configuration for this screen.

9.5 URL Filter Screen

Use this screen to block the users on your network from accessing certain web sites. To access this screen, click **Configuration > Firewall > URL Filter**.

Figure 46 Configuration > Firewall > URL Filter

The following table describes the labels in this screen.

Table 29 Configuration > Firewall > URL Filter

LABEL	DESCRIPTION
URL filter	
Enable URL Filter	Select the check box to enable the rule.
URL Filtering Policy	Select Whitelist to allow users to access the websites that match the filtering rules defined on this screen. Select Blacklist to block users to access the websites that match the filtering rules defined on this screen.
URL filter List	
Add New	Click Add New to create a new rule.
	This field displays the rule index number.
Keywords of URL or Domain	This field displays the keywords of URL or domain to which the LTE3202-M430 block or allow.
Action	Click Edit to go to the screen where you can edit the filtering rule. Click Delete to remove the filtering rule.
Apply	Click Apply to save your changes back to the LTE3202-M430.
Cancel	Click Cancel to reload the previous configuration for this screen.

9.6 IPv4/Port Filter Screen

The LTE3202-M430 firewall is a packet filtering firewall and restricts access based on the source/destination computer network address of a packet and the type of application. Use this screen to configure IP filtering rules. To access this screen, click **Configuration > Firewall > IPv4/Port Filter**.

Figure 47 Configuration > Firewall > IPv4/Port Filter

The following table describes the labels in this screen.

Table 30 Configuration > Firewall > IPv4/Port Filter

LABEL	DESCRIPTION
IPv4 Port Filter	
Enable IPv4 Port Filter	Select the check box to enable the rule.
IPv4 Port Filter Policy	Select IPv4 Whitelist description to allow packets that match the filtering rules defined on this screen to pass through. Select IPv4 Blacklist description to block packets that match the filtering rules defined on this screen.
Blacklist/Whitelist	This displays how many entries you have in the Whitelist/Blacklist summary tables.
Add New	Click Add New to create a new rule.
	This field displays the rule index number.
Source IP	This field displays the source IPv4 addresses to which this rule applies.
Port	This field displays a single port number of the source or a port range. Enter the port number/range of the source that define the traffic type, for example TCP port 80 defines web traffic.
Protocol	This field displays the protocol (TCP , UDP , TCP+UDP or any) used to transport the packets for which you want to apply the rule.
Dest. IP	This field displays the destination IPv4 addresses to which this rule applies.
Port	This field displays a single port number of the destination or a port range. Enter the port number/range of the destination that define the traffic type, for example TCP port 80 defines web traffic.
Comment	Enter descriptions of the rule in this field.
Action	Click Edit to go to the screen where you can edit the filtering rule. Click Delete to remove the filtering rule.
Apply	Click Apply to save your changes back to the LTE3202-M430.
Cancel	Click Cancel to reload the previous configuration for this screen.

9.7 IPv6/Port Filter Screen

The LTE3202-M430 firewall is a packet filtering firewall and restricts access based on the source/destination computer network address of a packet and the type of application. Use this screen to configure IP filtering rules. To access this screen, click **Configuration > Firewall > IPv6/Port Filter**.

Figure 48 Configuration > Firewall > IPv6/Port Filter

The following table describes the labels in this screen.

Table 31 Configuration > Firewall > IPv6/Port Filter

LABEL	DESCRIPTION
IPv6 Port Filter	
Enable IPv6 Port Filter	Select the check box to enable the rule.
IPv6 Port Filtering Policy	Select Whitelist: Allow only IPv6/Port in the list. to allow packets that match the filtering rules defined on this screen to pass through. Select Blacklist: Reject only IPv6/Port in the list. to block packets that match the filtering rules defined on this screen.
Blacklist/Whitelist	This displays how many entries you have in the Whitelist/Blacklist summary tables.
Add New	Click Add New to create a new rule.
	This field displays the rule index number.
Source IP	This field displays the source IPv6 addresses to which this rule applies.
Port	This field displays a single port number of the source or a port range. Enter the port number/range of the source that define the traffic type, for example TCP port 80 defines web traffic.
Protocol	This field displays the protocol (TCP , UDP , TCP+UDP or any) used to transport the packets for which you want to apply the rule.
Dest. IP	This field displays the destination IPv6 addresses to which this rule applies.
Port	This field displays a single port number of the destination or a port range. Enter the port number/range of the destination that define the traffic type, for example TCP port 80 defines web traffic.
Comment	Enter descriptions of the rule in this field.
Action	Click Edit to go to the screen where you can edit the filtering rule. Click Delete to remove the filtering rule.
Apply	Click Apply to save your changes back to the LTE3202-M430.
Cancel	Click Cancel to reload the previous configuration for this screen.

CHAPTER 10

NAT

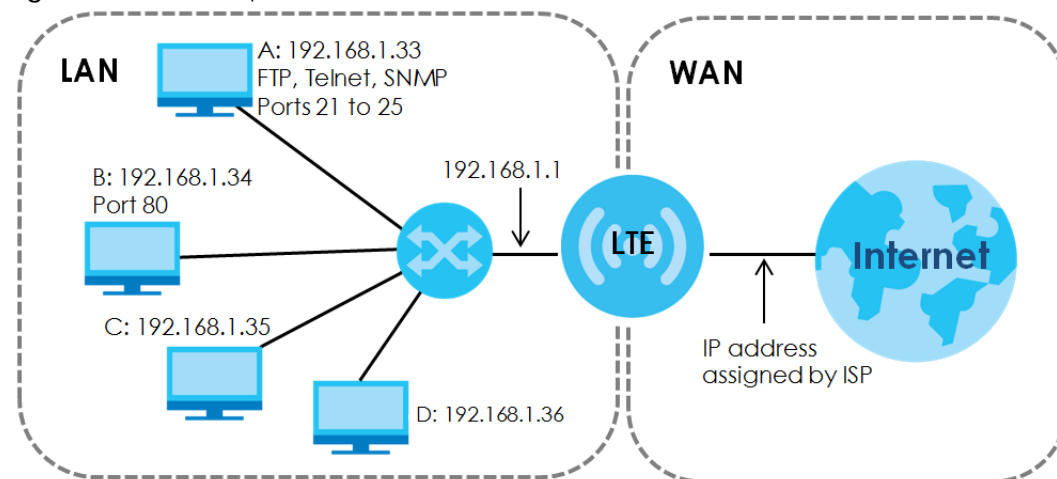
10.1 Overview

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 LTE3202-M430. 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 LTE3202-M430, which is 192.168.1.1.

Figure 49 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 LTE3202-M430.

10.1.1 What You Can Do in this Chapter

- Use the **IP/Port Forwarding** screen to view and configure port forwarding rules ([Section 10.2 on page 73](#)).
- Use the **DMZ** screen to configure a default server ([Section 10.3 on page 74](#)).
- Use the **ALG** screen to enable or disable SIP (VoIP) ALG (Application Layer Gateway) in the LTE3202-M430 ([Section 10.4 on page 74](#)).
- Use the **Pass through** screen to enable/disable ALGs in the LTE3202-M430 ([Section 10.5 on page 75](#)).

10.2 The IP/Port Forwarding Screen

Use this screen to configure port forwarding rules. To access this screen, click **Configuration > NAT > IP/Port Forwarding**.

Figure 50 Configuration > NAT > IP/Port Forwarding

IP/Port Forwarding

Enable Port forwarding

IP/Port Forwarding List: 1/30 [Add New](#) [Delete All](#)

	LAN IP address	LAN port	WAN port	Protocol	Action
1	192.168.1.15	80	90	TCPUDP	Edit Delete

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

The following table describes the labels in this screen.

Table 32 Configuration > NAT > IP/Port Forwarding

LABEL	DESCRIPTION
IP/Port Forwarding	
Enable Port Forwarding	Select the check box to enable port forwarding rules.
IP/Port Forwarding List	This displays how many of the allowed rules you have configured in the IP/Port Forwarding summary table.
Add New	Click Add New to create a new rule.
Delete all	Click Delete All to remove all port forwarding rules.
	This field displays the rule index number.
LAN IP address	This field displays the inside IP address of the server. Enter the inside IP address of the virtual server here.
LAN Port	A private port is a port that causes (or triggers) the LTE3202-M430 to record the IP address of the LAN computer that sent the traffic to a server on the WAN. Enter the port number/range of the private in this field.
WAN Port	A global port is a port that a server on the WAN uses when it sends out a particular service. The LTE3202-M430 forwards the traffic with this port to the client computer on the LAN that requested the service. Enter the port number/range of the global in this field.
Protocol	This field displays the protocol (TCP , UDP , TCPUDP) used to transport the packets for which you want to apply the rule.
Action	Click Edit to go to the screen where you can edit the port forwarding rule. Click Delete to remove the port forwarding rule.
Apply	Click Apply to save your changes back to the LTE3202-M430.
Cancel	Click Cancel to reload the previous configuration for this screen.

10.3 The DMZ Screen

The DeMilitarized Zone (DMZ) auto-negotiating 10/100 Mbps Ethernet port provides a way for public servers (Web, e-mail, FTP, etc.) to be visible to the outside world (while still being protected from DoS (Denial of Service) attacks such as SYN flooding and Ping of Death). These public servers can also still be accessed from the secure LAN.

By default the firewall allows traffic between the WAN and the DMZ, traffic from the DMZ to the LAN is denied, and traffic from the LAN to the DMZ is allowed. Internet users can have access to host servers on the DMZ but no access to the LAN, unless special filter rules allowing access were configured by the administrator or the user is an authorized remote user.

Click **Configuration > NAT > DMZ** to open the following screen.

Figure 51 Configuration > NAT > DMZ

The following table describes the labels in this screen.

Table 33 Configuration > NAT > DMZ

LABEL	DESCRIPTION
DMZ	
Enable DMZ	Select this to enable DMZ on the LTE3202-M430.
DMZ IP address	Type the IP address of your LTE3202-M430's DMZ port in dotted decimal notation. Note: Make sure the IP addresses of the LAN, WAN and DMZ are on separate subnets.
Apply	Click Apply to save your changes back to the LTE3202-M430.
Cancel	Click Cancel to reload the previous configuration for this screen.

10.4 The ALG Screen

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 Device registers with the SIP register server, the SIP ALG translates the LTE Device's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if your LTE Device is behind a SIP ALG.

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

Figure 52 Configuration > NAT > ALG

The following table describes the labels in this screen.

Table 34 Configuration > NAT > ALG

LABEL	DESCRIPTION
ALG	
FTP ALG	Select this check box to allow FTP sessions to pass through the LTE3202-M430. FTP (File Transfer Protocol) is a protocol that enables fast transfer of files, including large files that may not be possible by e-mail.
TFTP ALG	Select this check box to allow TFTP sessions to pass through the LTE3202-M430. TFTP (Trivial File Transfer Protocol) is an Internet File Transfer Protocol similar to FTP, but uses UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
PPTP ALG	Select this check box to enable PPTP ALG on the LTE3202-M430 to detect PPTP traffic and help build PPTP sessions through the LTE3202-M430's NAT.
RSTP ALG	Select this check box to have the LTE3202-M430 detect RSTP traffic and help build RTSP sessions through its NAT. The Real Time Streaming (media control) Protocol (RSTP) is a remote control for multimedia on the Internet.
SIP ALG	Select this check box to allow SIP sessions to pass through the LTE3202-M430. SIP is a signaling protocol used in VoIP (Voice over IP), the sending of voice signals over Internet Protocol.
Apply	Click Apply to save your changes back to the LTE3202-M430.
Cancel	Click Cancel to reload the previous configuration for this screen.

10.5 The Pass Through Screen

Use this screen to enable NAT and enable/disable the ALGs (Application Layer Gateways) in the LTE3202-M430. Click **Configuration > NAT > Pass through** to open the following screen.

Figure 53 Configuration > NAT > Pass through

Pass through

- Enable IPsec
- Enable PPTP
- Enable L2TP

Apply **Cancel**

The following table describes the labels in this screen.

Table 35 Configuration > NAT > Pass through

LABEL	DESCRIPTION
Pass through	
Enable IPsec	Select this check box to turn on the IPsec ALG (Application Layer Gateway) on the LTE3202-M430 to detect IPsec traffic and help build IPsec sessions through the LTE3202-M430's NAT.
Enable PPTP	Enable this to turn on the PPTP ALG on the LTE3202-M430 to detect PPTP traffic and help build PPTP sessions through the LTE3202-M430's NAT.
Enable L2TP	Enable this to turn on the L2TP ALG on the LTE3202-M430 to detect L2TP traffic and help build L2TP sessions through the LTE3202-M430's NAT.
Apply	Click Apply to save your changes back to the LTE3202-M430.
Cancel	Click Cancel to reload the previous configuration for this screen.

CHAPTER 11

DDNS

11.1 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 LTE3202-M430 or a server in your network.

The LTE3202-M430 must have a public global IP address and you should have your registered DDNS account information on hand.

11.2 The DDNS Screen

To change your LTE3202-M430's DDNS, click **Configuration > DDNS**. The screen appears as shown.

Figure 54 Configuration > DDNS

The following table describes the labels on this screen.

Table 36 Configuration > DDNS

LABEL	DESCRIPTION
DDNS	
Enable DDNS	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.

Table 36 Configuration > DDNS

LABEL	DESCRIPTION
Domain Name	The domain name is the host name that the DDNS service will map to your dynamic global IP address. Type the domain name fully qualified, for example, "yourhost.mydomain.net". You can specify up to two host names in the field separated by a comma (",").
User name	Enter your user name.
Password	Enter the password assigned to you.
Apply	Click Apply to save your changes back to the LTE3202-M430.
Cancel	Click Cancel to reload the previous configuration for this screen.

CHAPTER 12

Remote Management

12.1 Overview

Use the **Remote Management** screens to configure the LTE3202-M430's web interface port, TR-069 auto-configuration settings and activate UPnP. Additionally you can set up different bandwidth management profiles that provide a convenient way to manage the LTE3202-M430's network.

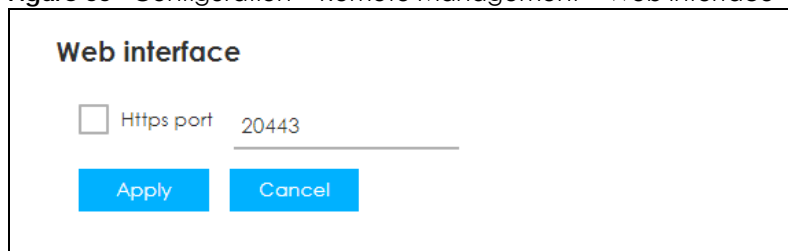
12.1.1 What You Can Do in this Chapter

- Use the **Web interface** screen to modify the server port for the HTTPS service ([Section 12.2 on page 79](#)).
- Use the **TR069** screen to configure the LTE3202-M430 to be managed by an ACS ([Section 12.3 on page 80](#)).
- Use the **Telnet** screen to enable Telnet in the LTE3202-M430 LAN/WAN interfaces ([Section 12.4 on page 81](#)).
- Use the **UPnP** screen to enable UPnP on the LTE3202-M430 ([Section 12.5 on page 82](#)).
- Use the **Bandwidth Management** screen to configure bandwidth management profiles ([Section 12.6 on page 83](#)).

12.2 The Web Interface Screen

Use the **Web interface** screen to change the LTE3202-M430's WAN interface remote management settings. Click **Configuration > Remote Management > Web interface** to open the following screen.

Figure 55 Configuration > Remote Management > Web interface



The screenshot shows a configuration screen titled "Web interface". It features a checkbox labeled "Https port" which is currently unchecked. To the right of the checkbox is a text input field containing the number "20443". Below the input field are two blue buttons: "Apply" and "Cancel".

The following table describes the labels on this screen.

Table 37 Configuration > Remote Management >

LABEL	DESCRIPTION
Web interface	
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.

Table 37 Configuration > Remote Management >

LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the LTE3202-M430.
Cancel	Click Cancel to reload the previous configuration for this screen.

12.3 The TR069 Screen

TR-069 defines how Customer Premise Equipment (CPE), for example your LTE3202-M430, 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 LTE3202-M430, modify settings, perform firmware upgrades as well as monitor and diagnose the LTE3202-M430. 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 > Remote Management > TR069** to open the following screen. Use this screen to configure your LTE3202-M430 to be managed by an ACS.

Figure 56 Configuration > Remote Management > TR069

The screenshot shows the TR069 configuration screen with the following elements:

- TR069** (Section Header)
- Enable TR069
- ACS URL (Text input field)
- ACS Username (Text input field)
- ACS Password (Text input field)
- Enable Periodic Inform
- Periodic Inform Interval (Text input field)
- Connection Request Port (Text input field)
- Connection Request Username (Text input field)
- Connection Request Password (Text input field)
- Apply (Blue button)
- Cancel (Blue button)

The following table describes the labels on this screen.

Table 38 Configuration > Remote Management > TR069

LABEL	DESCRIPTION
TR069	
Enable TR069	Select the check box to enable TR069 on the LTE3202-M430.
ACS URL	Enter the URL or IP address of the auto-configuration server.

Table 38 Configuration > Remote Management > TR069

LABEL	DESCRIPTION
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.
Enable Periodic Inform	Select the check box for the LTE3202-M430 to send periodic inform via TR-069 on the WAN.
Periodic Inform Interval	Enter the time interval (in seconds) at which the LTE3202-M430 sends information to 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 LTE3202-M430, 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 LTE3202-M430, this password is used to authenticate the ACS.
Apply	Click Apply to save your changes back to the LTE3202-M430.
Cancel	Click Cancel to reload the previous configuration for this screen.

12.4 The Telnet Screen

You can use Telnet to access the LTE3202-M430's command line interface. Specify which interfaces allow Telnet access.

Click **Configuration > Remote Management > Telnet** to open the following screen.

Figure 57 Configuration > Remote Management > Telnet

The following table describes the labels on this screen.

Table 39 Configuration > Remote Management > Telnet

LABEL	DESCRIPTION
Telnet	
LAN	Select this check box to enable devices in the LTE3202-M430's LAN network to access the LTE3202-M430 using Telnet.
WAN port	Select this check box to enable devices in the LTE3202-M430's WAN network to access the LTE3202-M430 using Telnet. Specify the service port number for accessing the LTE3202-M430.

Table 39 Configuration > Remote Management > Telnet

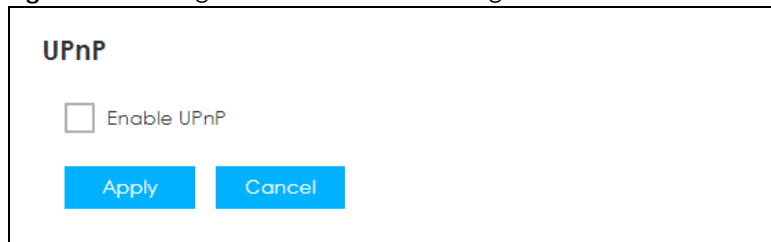
LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the LTE3202-M430.
Cancel	Click Cancel to reload the previous configuration for this screen.

12.5 The UPnP Screen

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

Use this screen to enable UPnP on the LTE3202-M430. Click **Configuration > Remote Management > UPnP** to open the following screen.

Figure 58 Configuration > Remote Management > UPnP



The following table describes the labels on this screen.

Table 40 Configuration > Remote Management > UPnP

LABEL	DESCRIPTION
UPnP	
Enable UPnP	Select the check box to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the LTE3202-M430's IP address (although you must still enter the password to access the web configurator).
Apply	Click Apply to save your changes back to the LTE3202-M430.
Cancel	Click Cancel to reload the previous configuration for this screen.

12.5.1 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 LTE3202-M430 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.

12.6 The Bandwidth Management Screen

Click **Configuration > Remote Management > Bandwidth Management** to open the following screen.

Figure 59 Configuration > Remote Management > Bandwidth Management

The following table describes the labels on this screen.

Table 41 Configuration > Remote Management > Bandwidth Management

LABEL	DESCRIPTION
Bandwidth Management	
Enable Bandwidth Management	Select the check box to use the Bandwidth Management.
Default	Select a profile from the drop-down list to be the LTE3202-M430's default bandwidth management profile.
Profile of Bandwidth Management	
Best effort	Best Effort is the bandwidth management profile with the highest priority. Enter the data rate for both Uplink (UL) and Downlink (DL) in MB/s for the Best Effort profile.
High	Enter the data rate for both Uplink (UL) and Downlink (DL) in MB/s for the High bandwidth management profile.
Medium	Enter the data rate for both Uplink (UL) and Downlink (DL) in MB/s for the Medium bandwidth management profile.
Normal	Enter the data rate for both Uplink (UL) and Downlink (DL) in MB/s for the Normal bandwidth management profile.

Table 41 Configuration > Remote Management > Bandwidth Management

LABEL	DESCRIPTION
Add New	Click Add new to add a new device to one of the LTE3202-M430's bandwidth management profiles.
Delete All	Click Delete All to remove all entries.
	This displays the number of bandwidth management profiles created in the LTE3202-M430.
MAC address	This field displays the device's MAC address.
Profile	This field displays the type of bandwidth profile for the device.
Action	Click Edit to go to the screen where you can edit the MAC address and/or the bandwidth management profile. Click Delete to remove the device from the list.
Apply	Click Apply to save your changes back to the LTE3202-M430.
Cancel	Click Cancel to reload the previous configuration for this screen.

CHAPTER 13

Short Message

13.1 Overview

This chapter shows you how to send and view the text messages. SMS (Short Message Service) allows you to send and view the text messages that the LTE3202-M430 received from mobile devices or the service provider.

When the SMS box is full the LTE3202-M430 will begin to delete older entries as it adds new ones.

13.1.1 What You Can Do in this Chapter

- Use the **New SMS** screen to send new messages ([Section 13.2 on page 85](#)).
- Use the **Inbox** screen to view messages received on the LTE3202-M430 ([Section 13.3 on page 86](#)).
- Use the **Outbox** screen to view messages sent from the LTE3202-M430 ([Section 13.4 on page 86](#)).
- Use the **Draftbox** screen to view messages not yet sent from the LTE3202-M430 ([Section 13.5 on page 87](#)).
- Use the **SIM SMS** screen to view messages received on the SIM card ([Section 13.6 on page 88](#)).

13.2 New SMS Screen

Use this screen to send messages using the LTE3202-M430. To access this screen, click **Configuration > Short Message > New SMS**.

Type a phone number and message content. You can type up to 140 English characters (70 Chinese characters) in one message. If the message exceeds 160 English characters, more than one message will be sent. The maximum number of SMS that can be sent is 8. Click **Send** to send the message. Click **Save to drafts** to store the message as a draft. Click **Reset** to reload the previous configuration for this screen.

Figure 60 Configuration > Short Message > New SMS



13.3 Inbox Screen

Use this screen to view messages received on the LTE3202-M430. To access this screen, click **Configuration > Short Message > Inbox**.

Figure 61 Configuration > Short Message > Inbox: Unread Message



From	Content	Date	Action
09 [redacted]	Test message for LTE	2018/07/24,11:32:10	Delete

The following table describes the labels in this screen.

Table 42 Configuration > Short Message > Inbox

LABEL	DESCRIPTION
Delete All	Click Delete All to remove all messages.
	This field displays the index number of the message.
From	This field displays the name from which the message is sent.
Content	This field displays the content of the message.
Date	This field displays the date and time the message was received.
Action	Click Delete to remove the message record.

Click a message to open its content. Click **Reply** to respond to the message. Click **Forward** to send this message to a new number.

Figure 62 Configuration > Short Message > Inbox: Open Message



13.4 Outbox Screen

Use this screen to view messages sent from the LTE3202-M430. To access this screen, click **Configuration > Short Message > Outbox**.

Figure 63 Configuration > Short Message > Outbox


Recipients	Content	Date	Action
09 [redacted]	sent by LTE3202	2018/07/16,09:02:09	Delete

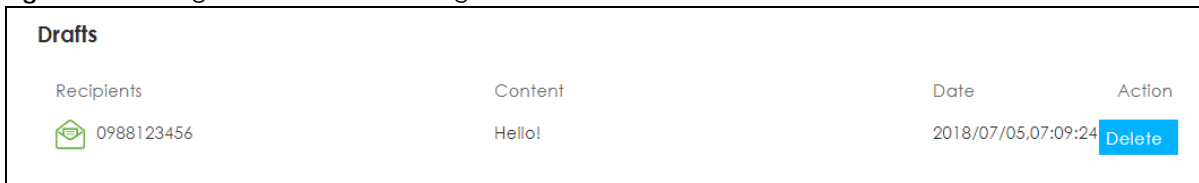
The following table describes the labels in this screen.

Table 43 Configuration > Short Message > Outbox

LABEL	DESCRIPTION
Delete All	Click Delete All to remove all messages.
	This field displays the index number of the message.
To	This field displays the name the message is sent to.
Content	This field displays the content of the message.
Date	This field displays the date and time the message was sent.
Action	Click Delete to remove the message record.

13.5 Draft Screen

Use this screen to view messages not yet sent from the LTE3202-M430. To access this screen, click **Configuration > Short Message > Draft**.

Figure 64 Configuration > Short Message > Draft


Recipients	Content	Date	Action
0988123456	Hello!	2018/07/05,07:09:24	Delete

The following table describes the labels in this screen.

Table 44 Application > Short Message > Draft

LABEL	DESCRIPTION
Delete All	Click Delete All to remove all messages.
	This field displays the index number of the message.
Recipients	This field displays the name the message is sent to.
Content	This field displays the content of the message.
Time	This field displays the date and time the message was sent.
Action	Click Delete to remove the message record. Click Send to deliver the message.

13.6 SIM SMS Screen

Use this screen to view messages received on the SIM card. To access this screen, click **Configuration > Short Message > SIM SMS**.

Figure 65 Configuration > Short Message > SIM SMS



The following table describes the labels in this screen.

Table 45 Configuration > Short Message > SIM SMS

LABEL	DESCRIPTION
Delete All	Click Delete All to remove all messages.
	This field displays the index number of the message.
From	This field displays the mobile phone number from which the message is sent.
Time	This field displays the date and time the message was received.
Content	This field displays the content of the message.
Action	Click Delete to remove the message record.

CHAPTER 14

System

14.1 Overview

Use the system screens to configure general LTE3202-M430 settings.

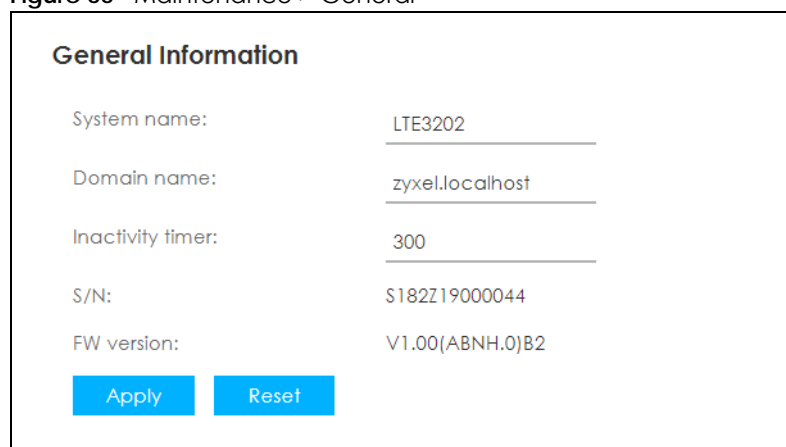
14.1.1 What You Can Do in this Chapter

- Use the **General** screen to view basic information about the LTE3202-M430 and restart the LTE3202-M430 ([Section 14.2 on page 89](#)).
- Use the **User Account** screen to set the domain name and change the LTE3202-M430's system password ([Section 14.3 on page 90](#)).
- Use the **Time Settings** screen to change the LTE3202-M430's time and date and configure daylight saving time ([Section 14.4 on page 91](#)).
- Use the **Firmware Upgrade** screen to upload new firmware to your LTE3202-M430 ([Section 14.5 on page 92](#)).
- Use the **Settings Profile** screen to reset your device settings back to the factory default, backup configuration, and restoring configuration ([Section 14.6 on page 93](#)).
- Use the **Reboot** screen to restart your LTE3202-M430 ([Section 14.7 on page 94](#)).

14.2 The General Screen

Use this screen to view basic information about the LTE3202-M430 and restart the LTE3202-M430. To access this screen, click **Maintenance > General**.

Figure 66 Maintenance > General



The screenshot shows a web interface titled "General Information". It contains several fields with labels on the left and values on the right, each with a horizontal line underneath for editing. At the bottom, there are two blue buttons: "Apply" and "Reset".

System name:	LTE3202
Domain name:	zyxel.localhost
Inactivity timer:	300
S/N:	S182Z19000044
FW version:	V1.00(ABNH.0)B2

The following table describes the labels in this screen.

Table 46 System > System Information

LABEL	DESCRIPTION
General Information	
System name	System name is a unique name to identify the LTE3202-M430 in an Ethernet network.
Domain name	Enter the domain name you want to give to the LTE3202-M430.
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).
S/N	This displays the serial number of the LTE3202-M430.
FW Version	This displays the current firmware version of the LTE3202-M430.
Apply	Click this button to save your changes back to the LTE3202-M430.
Reset	Click Reset to reload the previous configuration for this screen.

14.3 The User Account Screen

This screen allows you to set the domain name and change the LTE3202-M430's system password. It is strongly recommended that you change your LTE3202-M430's system password. To access this screen, click **Maintenance > User Account**.

See [Section 2.2 on page 14](#) for more information about login accounts.

Figure 67 Maintenance > User Account

The screenshot shows a web interface for configuring the user account. The title is "User Account". Below the title, there are three input fields: "User Name" (containing "admin"), "Password", and "Confirm Password". At the bottom of the form, there are two buttons: "Apply" and "Reset".

The following table describes the labels in this screen.

Table 47 System > User Account

LABEL	DESCRIPTION
User Settings	
Username	Enter your username of the system account.
Password	Type your new system password. Note that as you type a password, the screen displays as dot (.) for each character you type.
Confirm Password	Type the new password again in this field.
Apply	Click Apply to save your changes back to the LTE3202-M430.
Reset	Click Reset to reload the previous configuration for this screen.

14.4 The Time Settings Screen

For effective scheduling and logging, the LTE3202-M430 system time must be accurate. The LTE3202-M430 has a software mechanism to get the current time and date from an external server. To change your LTE3202-M430's time zone, click **Maintenance > Time Settings**. The screen displays as shown. You can have the LTE3202-M430 get the date and time from a time server or change the IP address or URL of your time server.

Figure 68 Maintenance > Time Settings

Time Settings

Current date and time 07:30:43, 05/07/2018

NTP Mode set manually
 sync from network

Primary NTP server hora.ngn.rima-tde.net ▼

Secondary NTP server hora.ngn.rima-tde.net ▼

Time zone GMT+01:00 ▼

Daylight saving time Enable

From 01:00 AM ▼ March ▼
Last ▼ Sunday ▼

Start date 01:00 AM, 25/3/2018

To 01:00 AM ▼ October ▼
Last ▼ Sunday ▼

End date 01:00 AM, 28/10/2018

Offset time 60 minutes (1-1440)

The following table describes the labels in this screen.

Table 48 Maintenance > Time Settings

LABEL	DESCRIPTION
Time Settings	
Current date and time	This field displays the present time and date of your LTE3202-M430.
NTP Mode	Select set manually 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. Select sync from network to have the LTE3202-M430 get the time and date from the time server you specified below.
Primary/Secondary NTP server	Enter the IP address or URL of your time server. Check with your ISP/network administrator if you are unsure of this information.

Table 48 Maintenance > Time Settings

LABEL	DESCRIPTION
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight saving time	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, here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select Second, Sunday, March and select 02:00AM in the time field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, March . The time you select in the time field depends on your time zone. In Germany for instance, you would select 02:00AM 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, here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select First, Sunday, November and select 02:00AM in the time field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, October . The time you select in the time field depends on your time zone. In Germany for instance, you would select 02:00AM because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Offset Time	Specify the offset time, which is the difference in minutes from Coordinated Universal Time (UTC) to obtain the LTE3202-M430's current time.
Apply	Click Apply to save your changes back to the LTE3202-M430.
Reset	Click Reset to reload the previous configuration for this screen.

14.5 The Firmware Upgrade Screen

This screen allows you to upload new firmware to your LTE3202-M430. You can download new firmware releases from your nearest ZyXEL FTP site (or www.zyxel.com) to use to upgrade your device's performance.

Only use firmware for your device's specific model.

To access this screen, click **Maintenance > Firmware Upgrade**. This screen displays the current firmware version and status of the LTE3202-M430. Type in the location of the file you want to upload in the **Select File** field or click **Choose File** to find it. Remember that you must decompress compressed (.ZIP) files before you can upload them. You can select the check box to return the LTE3202-M430 to its factory defaults after upgrading the new firmware. Click **Update** to begin the upload process.

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 LTE3202-M430 while firmware upload is in progress!

Figure 69 Maintenance > Firmware Upgrade

The screenshot shows the 'Firmware Upgrade' screen. At the top, it says 'Local_Update_Info'. Below that, 'Current Version' is listed as 'V1.00(ABNH.0)B2'. There is a 'Select File' section with a 'Choose File' button and the text 'No file chosen'. A checkbox is present with the text 'After upgrading the new firmware, restore the configuration to the factory default.' At the bottom, there is a blue 'Update' button.

14.6 The Settings Profile Screen

The **Settings Profile** screen allows you to backup and restore device configurations. You can also reset your device settings back to the factory defaults. To access this screen, click **Maintenance > Settings Profile**.

Figure 70 Maintenance > Settings Profile

The screenshot shows the 'Reset Settings' screen. It has a 'Restore Defaults description' section with a blue 'Restore' button. Below that is the 'Import & Export Profile' section. Under 'Apply Profile from File', there is a 'Choose File' button, the text 'No file chosen', and a blue 'Apply' button. Under 'Export Profile to File', there is a blue 'Apply' button.

14.6.1 Reset Settings

Click the **Restore** button to clear all user-entered configuration information and return the LTE3202-M430 to its factory defaults. The LTE3202-M430 automatically restarts.

You can also press the **Reset** button on the rear panel to reset the factory defaults of your LTE3202-M430. Refer to [Section 1.5.2.3 on page 13](#) for more information on the **Reset** button.

14.6.2 Import & Export Profile

This screen allows you to upload a new or previously saved configuration file from your computer to your LTE3202-M430.

Type in the location of the file you want to upload in the **Apply Profile from File** field or click **Choose File** to find it. Remember that you must decompress compressed (.ZIP) files before you can upload them. Click **Apply** to begin the upload process. The LTE3202-M430 automatically restarts.

Do not turn off the LTE3202-M430 while configuration file upload is in progress.

Backup Configuration allows you to back up (save) the LTE3202-M430's current configuration to a file on your computer. The configuration file should be saved and edited in UTF-8 (without BOM) format, if you're using Windows Notepad, make sure you choose **File > Save as UTF-8** in the text editor. Once your LTE3202-M430 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.

Select one profile from the drop-down list box in the **Export Profile to File** field, and click **Export** to save the LTE3202-M430's current configuration to your computer.

After the LTE3202-M430 configuration has been restored successfully, the login screen appears. 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 device IP address (192.168.1.1).

14.7 The Reboot Screen

System restart allows you to reboot the LTE3202-M430 without turning the power off.

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

Figure 71 Maintenance > Reboot



CHAPTER 15

Troubleshooting

15.1 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](#)
- [LTE3202-M430 Access and Login](#)
- [Internet Access](#)
- [Wireless Connections](#)

15.2 Power, and Hardware Installation

[The LTE3202-M430 does not turn on. None of the LEDs turn on.](#)

- 1 Make sure the LTE3202-M430 is correctly installed (refer to your Quick Start Guide).
- 2 Press the power button to turn the LTE3202-M430 on. See [Section 1.5.2 on page 12](#) and [Section 1.5.1 on page 11](#).
- 3 If the problem continues, contact the vendor.

15.3 LTE3202-M430 Access and Login

[I forgot the password for the LTE4506.](#)

- 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 13](#).

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 [LTE3202-M430 Access and Login](#)
- 2 Make sure the LTE3202-M430 is correctly installed and turned on. See the Quick Start Guide and [Section 1.5.2 on page 12](#).
- 3 Make sure your Internet browser does not block pop-up windows and has JavaScripts.
- 4 Make sure your computer is connected to the LTE3202-M430 and is in the same subnet as the LTE3202-M430.
- 5 Reset the device to its factory defaults, and try to access the LTE3202-M430 with the default IP address. See [Section 1.5.2.3 on page 13](#).
- 6 Disconnect your computer from the Internet (Wireless and/or Ethernet) and then insert the LTE3202-M430 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 13](#).

I can see the **Login** screen, but I cannot log in to the LTE3202-M430.

- 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 LTE3202-M430 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 13](#).

15.4 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 LTE3202-M430.
- 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 LTE3202-M430), but my Internet connection is not available anymore.

- 1 Reboot the LTE3202-M430.
- 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 LTE3202-M430 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 LTE3202-M430 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 LTE3202-M430.
- 4 If the problem continues, contact the network administrator or vendor.

15.5 Wireless Connections

I cannot access the LTE3202-M430 or ping any computer from the WLAN.

- 1 Make sure the wireless LAN is enabled on the LTE3202-M430.
- 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 LTE3202-M430's active radio.
- 4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the LTE3202-M430.
- 5 Check that both the LTE3202-M430 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.

15.6 Getting More Troubleshooting Help

Search for support information for your model at 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 <http://www.zyxel.com/homepage.shtml> and also http://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
- <http://www.zyxel.com>

Asia

China

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

India

- Zyxel Technology India Pvt Ltd
- <http://www.zyxel.in>

Kazakhstan

- Zyxel Kazakhstan
- <http://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
- <http://www.zyxel.com/tw/zh/>

Thailand

- Zyxel Thailand Co., Ltd
- <http://www.zyxel.co.th>

Vietnam

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

Europe

Austria

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

Belarus

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

Belgium

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

Bulgaria

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

Czech Republic

- Zyxel Communications Czech s.r.o
- <http://www.zyxel.cz>

Denmark

- Zyxel Communications A/S
- <http://www.zyxel.dk>

Estonia

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

Finland

- Zyxel Communications
- <http://www.zyxel.fi>

France

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

Germany

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

Hungary

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

Italy

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

Latvia

- Zyxel Latvia
- <http://www.zyxel.com/lv/lv/homepage.shtml>

Lithuania

- Zyxel Lithuania
- <http://www.zyxel.com/lt/lt/homepage.shtml>

Netherlands

- Zyxel Benelux
- <http://www.zyxel.nl>

Norway

- Zyxel Communications
- <http://www.zyxel.no>

Poland

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

Romania

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

Russia

- Zyxel Russia
- <http://www.zyxel.ru>

Slovakia

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

Spain

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

Sweden

- Zyxel Communications
- <http://www.zyxel.se>

Switzerland

- Studerus AG

- <http://www.zyxel.ch/>

Turkey

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

UK

- Zyxel Communications UK Ltd.
- <http://www.zyxel.co.uk>

Ukraine

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

Latin America

Argentina

- Zyxel Communication Corporation
- <http://www.zyxel.com/ec/es/>

Brazil

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

Ecuador

- Zyxel Communication Corporation
- <http://www.zyxel.com/ec/es/>

Middle East

Israel

- Zyxel Communication Corporation
- <http://il.zyxel.com/homepage.shtml>

Middle East

- Zyxel Communication Corporation
- <http://www.zyxel.com/me/en/>

North America

USA

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

Oceania

Australia

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

Africa

South Africa

- Nology (Pty) Ltd.
- <http://www.zyxel.co.za>

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 49 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 www.zyxel.com) 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 e-mail.
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 49 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 e-mail 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 e-mail 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 49 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 © 2018 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.
- Operation of this device is restricted to indoor use only, except for relevant user's manual mention that this device can be installed into the external environment.

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 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 catégorie I 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 26cm between the radio equipment and your body.
- The maximum RF power operating for each band as follows:
- **GSM 900**
The maximum RF power operating for each band as follows:
the band 880.2 to 914.8 MHz is 1584.89 mW.
- **GSM 1800**
The maximum RF power operating for each band as follows:
the band 1710.2 – 1784.8 MHz is 870.96 mW.
- **WCDMA Band I**
The maximum RF power operating for each band as follows:
the band 1922.6 to 1977.4 MHz is 194.98 mW.

- **WCDMA Band VIII**
The maximum RF power operating for each band as follows:
the band 882.6 to 912.4 MHz is 229.09 mW.
- **LTE Band 1**
The maximum RF power operating for each band as follows:
the band 1922.5 to 1977.5 MHz is 167.88 mW.
- **LTE Band 3**
The maximum RF power operating for each band as follows:
the band 1710.7 to 1784.3 MHz is 174.58 mW.
- **LTE Band 7**
The maximum RF power operating for each band as follows:
the band 2502.5 to 2567.5 MHz is 169.43 mW.
- **LTE Band 8**
The maximum RF power operating for each band as follows:
the band 880.7 to 914.3 MHz is 182.39 mW.
- **LTE Band 20**
The maximum RF power operating for each band as follows:
the band 834.5 to 859.5 MHz is 190.99 mW.
- **LTE Band 28**
The maximum RF power operating for each band as follows:
the band 704.5 to 746.5 MHz is 199.99 mW.
- **LTE Band 38**
The maximum RF power operating for each band as follows:
the band 2572.5 to 2617.5 MHz is 171.79 mW.
- **LTE Band 40**
The maximum RF power operating for each band as follows:
the band 2302.5 to 2397.5 MHz is 160.32 mW.
- **802.11 b**
The maximum RF power operating for each band as follows:
the band 2,400 to 2,483.5 MHz is 68.71 mW.
- **802.11 g**
The maximum RF power operating for each band as follows:
the band 2,400 to 2,483.5 MHz is 85.9 mW.
- **802.11 n**
The maximum RF power operating for each band as follows:
the band 2,400 to 2,483.5 MHz is 88.92 mW.

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>National Restrictions</p> <ul style="list-style-type: none"> • 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 http://www.bipt.be for more details. • 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 http://www.bipt.be voor meer gegevens. • 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 http://www.ibpt.be pour de plus amples détails.
Español (Spanish)	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..
Čeština (Czech)	Zyxel tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU.
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>National Restrictions</p> <ul style="list-style-type: none"> • In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage. • I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.
Deutsch (German)	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.
Eesti keel (Estonian)	Käesolevaga kinnitab Zyxel seadme seadmed vastavust direktiivi 2014/53/EL põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Ζyxel ΔΗΛΩΝΕΙ ΟΤΙ ΕΞΟΠΛΙΣΜΟΣ ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/ΕΕ.
English	Hereby, Zyxel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.
Français (French)	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.
Hrvatski (Croatian)	Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 2014/53/UE.
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)	<p>Con la presente Zyxel dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/UE.</p> <p>National Restrictions</p> <ul style="list-style-type: none"> 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 http://www.sviluppoeconomico.gov.it/ for more details. Questo prodotto è conforme alla 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 http://www.sviluppoeconomico.gov.it/ per maggiori dettagli.
Latviešu valoda (Latvian)	<p>Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 2014/53/ES būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.</p> <p>National Restrictions</p> <ul style="list-style-type: none"> The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details. 2.4 GHz frekvenču joslas izmantošanai ārpus telpām nepieciešama atļauja no Elektronisko sakaru direkcijas. Vairāk informācijas: http://www.esd.lv.
Lietuvių kalba (Lithuanian)	Šiuo Zyxel deklaruoją, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/ES Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, Zyxel nyilatkozom, 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-htigijiet 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:

1. Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 2014/53/EU has also been implemented in those countries.

2. 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 adapter 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。
- 無線資訊傳輸設備須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。

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、食物或其他不合適的材料。
- 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.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Open Source Licenses

This product contains 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. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.

Index

A

access [14](#)
ACS [80](#)
ARP Protection [67](#)
authentication [54, 55](#)
 RADIUS server [55](#)
Auto Configuration Server, see ACS [80](#)

B

Broadband [34](#)

C

certifications [112](#)
 viewing [114](#)
channel, wireless LAN [53](#)
configuration [9](#)
contact information [99](#)
cookies [14](#)
copyright [108](#)
CTS threshold [54](#)
current date/time [91](#)
customer support [99](#)

D

data fragment threshold [54](#)
date [91](#)
DHCP server [42](#)
disclaimer [108](#)

E

encryption [56](#)
ESSID [98](#)
Extended Service Set IDentification [49](#)

F

filters
 MAC address [50, 55](#)
Firefox [14](#)
Firewall
 guidelines [65](#)
firewall
 stateful inspection [64](#)
fragmentation threshold [54](#)

G

General wireless LAN screen [47](#)

H

hardware connections [10](#)

I

installation [9](#)
Internet Explorer [14](#)

J

Java

permissions [14](#)
JavaScripts [14](#)

L

LAN [41](#)
LAN overview [41](#)
LAN setup [41](#)
LEDs [11](#)
limitations
 wireless LAN [56](#)
 WPS [62](#)
Local Area Network [41](#)

M

MAC address
 filter [50, 55](#)
MAC authentication [50](#)
maintenance [9](#)
management [9](#)
managing the device
 good habits [10](#)

N

NAT [72](#)
 overview [72](#)
 see also Network Address Translation
Netscape Navigator [14](#)
Network Address Translation [72](#)

O

overview [9](#)

P

PBC [57](#)

PIN, WPS [57](#)
 example [59](#)
pop-up windows [14](#)
preamble [54](#)
Push Button Configuration, see PBC
push button, WPS [57](#)

R

RADIUS server [55](#)
remote management
 TR-069 [80](#)
Remote Procedure Calls, see RPCs [80](#)
RPPCs [80](#)
RTS threshold [54](#)

S

screen resolution [14](#)
security
 wireless LAN [54](#)
Service Set [49](#)
SIM card [10](#)
SSID [55](#)
stateful inspection firewall [64](#)
status [24](#)
supported browsers [14](#)

T

thresholds
 data fragment [54](#)
 RTS/CTS [54](#)
time [91](#)
TR-069 [80](#)
 ACS setup [80](#)

U

Universal Plug and Play

Security issues [82](#)
use [9](#)

push button [57](#)

W

WAN

Wide Area Network, see WAN [34](#)

warranty [114](#)

note [114](#)

Web Configurator [14](#)

access [14](#)

requirements [14](#)

supported browsers [14](#)

web configurator [9](#)

WEP [56](#)

Wi-Fi [46](#)

wireless channel [98](#)

wireless LAN [46, 52, 98](#)

authentication [54, 55](#)

channel [53](#)

encryption [56](#)

example [53](#)

fragmentation threshold [54](#)

limitations [56](#)

MAC address filter [50, 55](#)

preamble [54](#)

RADIUS server [55](#)

RTS/CTS threshold [54](#)

security [54](#)

SSID [55](#)

WEP [56](#)

WPA [56](#)

WPA-PSK [56](#)

WPS [57, 59](#)

example [60](#)

limitations [62](#)

PIN [57](#)

push button [57](#)

wireless security [98](#)

WPA [56](#)

WPA-PSK [56](#)

WPS [57, 59](#)

example [60](#)

limitations [62](#)

PIN [57](#)

example [59](#)