ZYXEL
Your Networking Ally

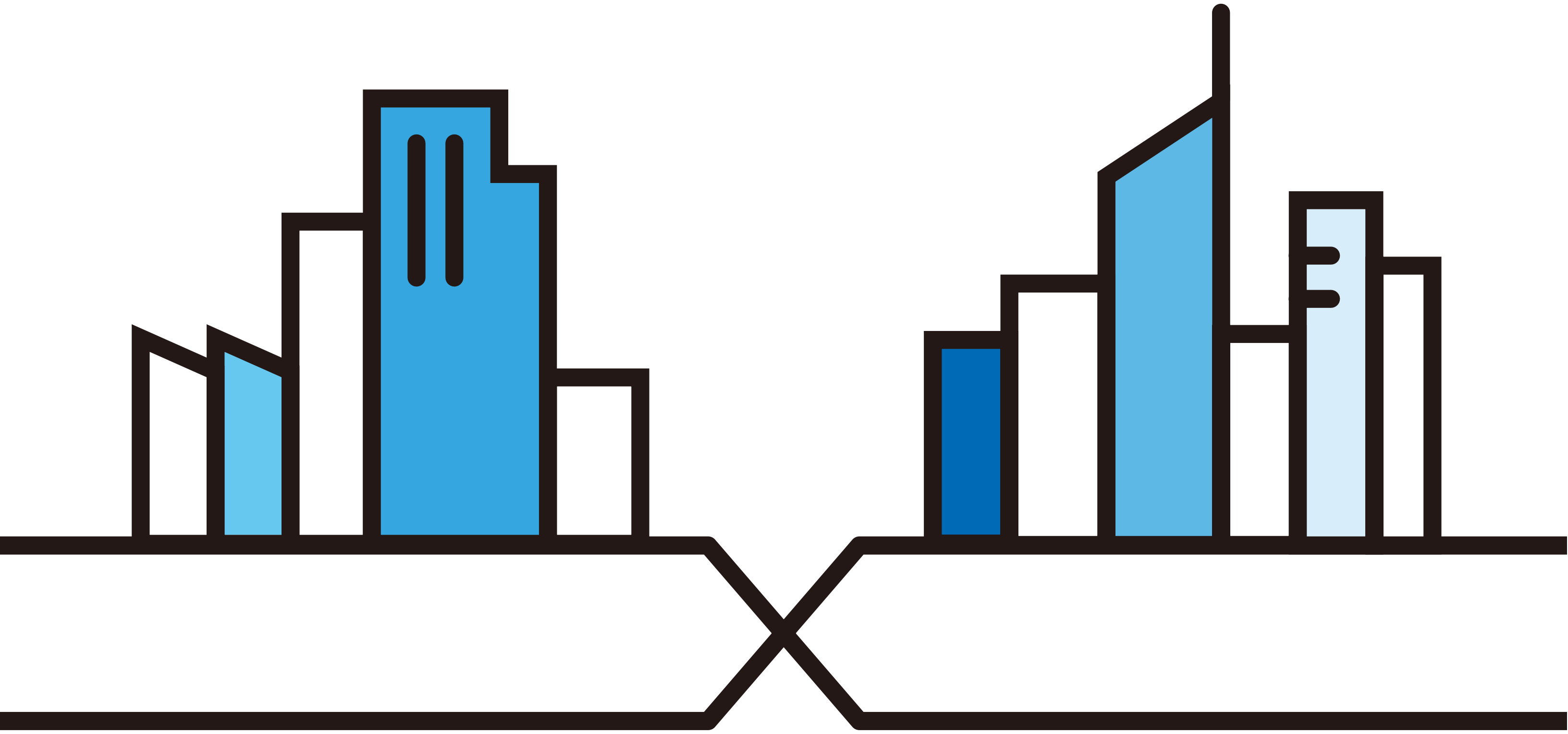
User's Guide

LTE3302-M432 & LTE3312-M432

4G LTE Indoor Router/4G LTE Indoor IAD

Version 1.00 Edition 1, 09/2017

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



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Screenshots and graphics in this book may differ slightly from your product due to differences in your product firmware or your computer operating system. Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect and log into the LTE Device. It contains information on WPS settings and installation of the SIM card, external antennas, and battery.

- More Information

  Go to **support.zyxel.com** to find other information on the LTE Device.

Document Conventions

Warnings and Notes

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

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

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

Syntax Conventions

- All models may be referred to as the “LTE Device” in this guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Configuration > Log / Report > Log Settings** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.

Icons Used in Figures

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

LTE Device 	Generic Router 	Switch
Firewall 	Cell Tower 	Printer
Server 		

Contents Overview

Table of Contents

PART I

User's Guide

CHAPTER 1 Introduction

1.1 Overview

The LTE3302-M432 is a wireless router and the LTE3312-M432 is a wireless IAD (Integrated Access Device) which is a router with a phone port for Internet phone calls.

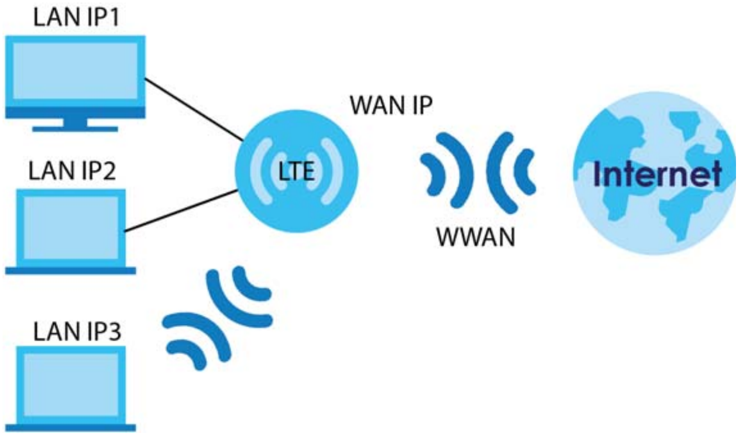
1.1.1 Operating Modes

The LTE Device supports **Bridge mode** and **Router mode.**

- **Router mode**: This is the default operating mode of the LTE Device. Use **Router mode** if you want to use routing functions, such as firewall, DHCP, NAT, and so on.

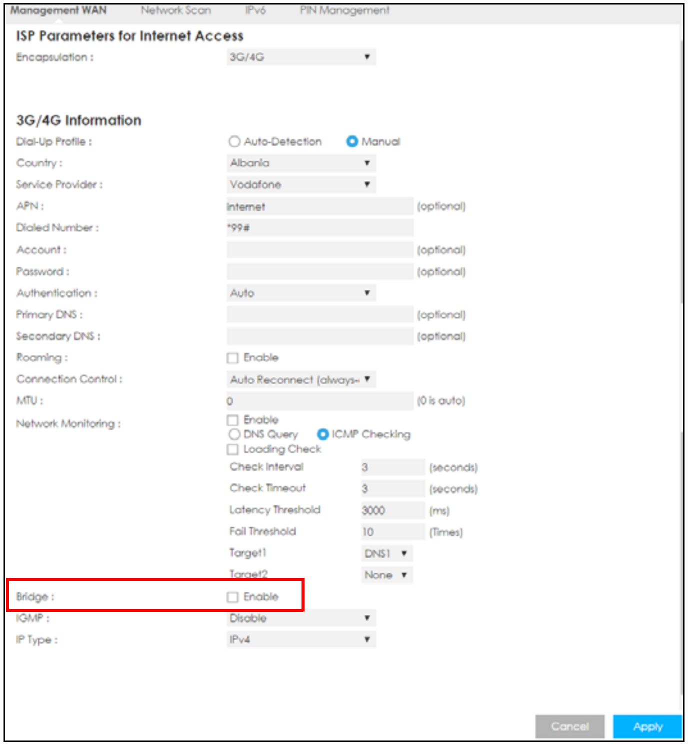
  The following figure shows an example of the LTE Device in **Router mode**.

Figure 1 The LTE Device in Router Mode



- **Bridge mode**: Select **Bridge 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.
  Click the **Edit** button in the **Configuration > Network > WAN > Management WAN** screen. Select the **Enable** check box in the **Bridge** field to use **Bridge** mode.

Figure 2 Choose a Mode



ISP Parameters for Internet Access

Encapsulation : 3G/4G ▾

3G/4G Information

Dial-Up Profile :	○ Auto-Detection ● Manual	
Country :	Albania ▾	
Service Provider :	Vodafone ▾	
APN :	Internet	(optional)
Dialed Number :	*99#	
Account :		(optional)
Password :		(optional)
Authentication :	Auto ▾	
Primary DNS :		(optional)
Secondary DNS :		(optional)
Roaming :	□ Enable	
Connection Control :	Auto Reconnect (always- ▾	
MTU :	0	(0 is auto)
Network Monitoring :	□ Enable ○ DNS Query ● ICMP Checking □ Loading Check	
	Check Interval 3	(seconds)
	Check Timeout 3	(seconds)
	Latency Threshold 3000	(ms)
	Fail Threshold 10	(Times)
	Target1 DNS1 ▾	
	Target2 None ▾	
Bridge :	□ Enable	
IGMP :	Disable ▾	
IP Type :	IPv4 ▾	

The following figures show examples of the LTE Device in **Bridge mode**.

Figure 3 The LTE Device in Bridge Mode with an Existing Router

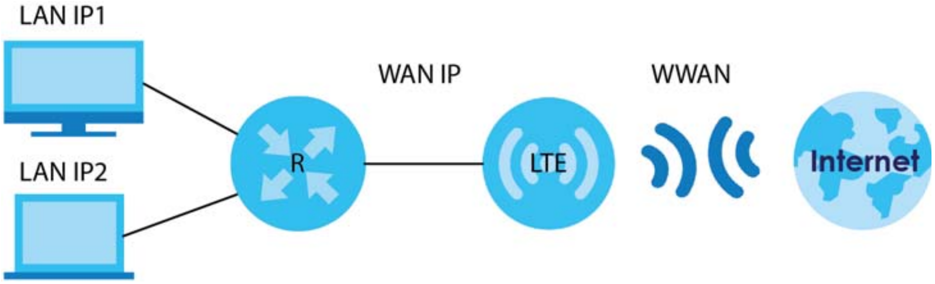
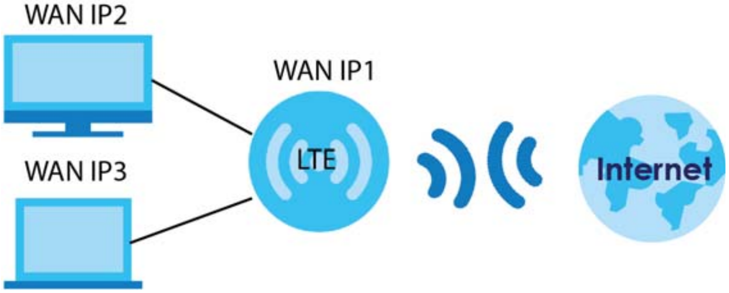


Figure 4 The LTE Device in Bridge Mode with Multiple Public IP Addresses



1.1.2 Wireless WAN (2G/3G/4G LTE)

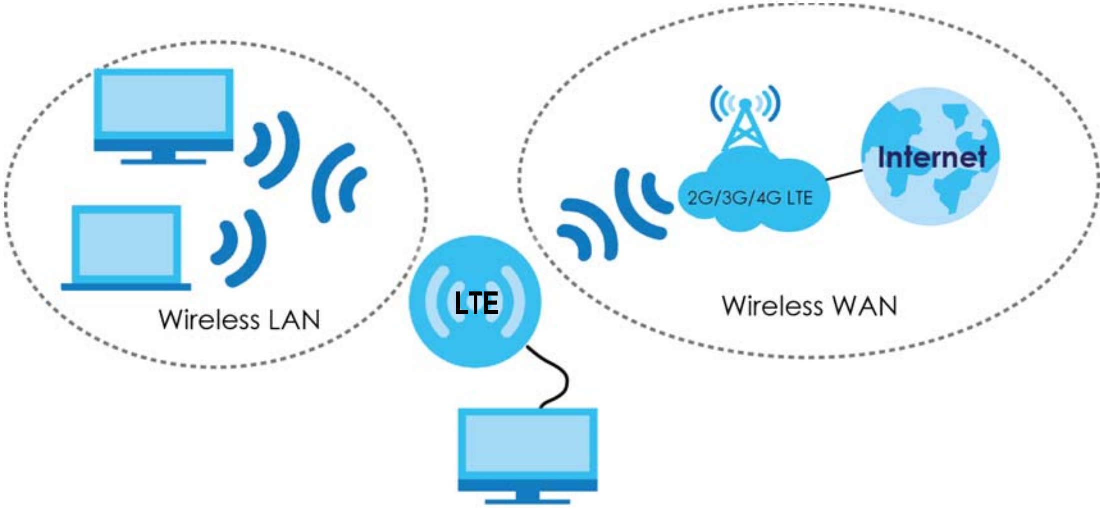
The LTE Device can connect to the Internet through a 2G/3G/4G LTE SIM card to access a wireless WAN connection. Just insert a SIM card into the SIM card slot at the back of the LTE Device.

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

You can install two external antennas to improve your wireless WAN signal strength. Note that external antennas are not provided. They are the default antennas for signal transmission when the LTE Device is starting up.

1.1.3 Wireless LAN (WiFi)

IEEE 802.11b/g/n wireless clients can connect to the LTE Device to access network resources and the Internet. Your LTE Device supports Wi-Fi Protected Setup (WPS), which allows you to quickly set up a wireless network with strong security.



1.1.4 Firmware

You can upgrade firmware on the LTE Device for feature enhancements and/or the LTE (2G/3G/4G) module for LTE enhancements. The latter needs to be implemented when a notice is released on the Zyxel website.

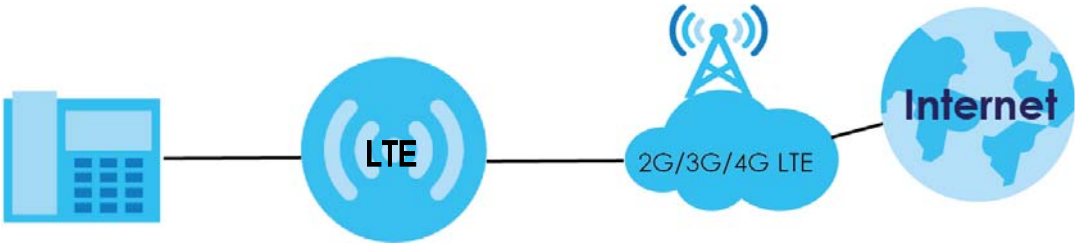
A range of services such as a firewall and content filtering are also available for secure Internet computing. See the Tutorials chapter for more information.

1.1.5 Power Supplies

Two types of power supplies are supported. You can connect the power adaptor to an appropriate power outlet or install a battery at the bottom of the LTE Device as an alternative way to supply power if you don’t have access to a power outlet. Note that a battery is not provided.

1.1.6 Internet Phone Calls (Vo3G) on the LTE3312-M432

You can connect an analog phone to the **PHONE** port to make phone calls over the Internet. See the Tutorials chapter for more information.



1.2 Good Habits for Managing the LTE Device

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

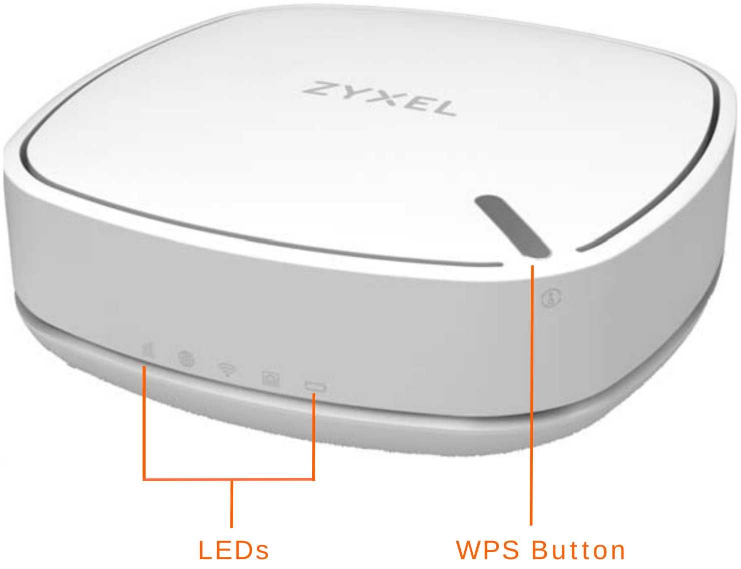
- Change the WiFi and Web Configurator passwords. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Go to **Maintenance > Backup/ Restore** to back up or restore a configuration file. Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the LTE Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the LTE Device. You could simply restore your last configuration. See the Troubleshooting chapter for more information.

1.3 Hardware

1.3.1 Front Panel

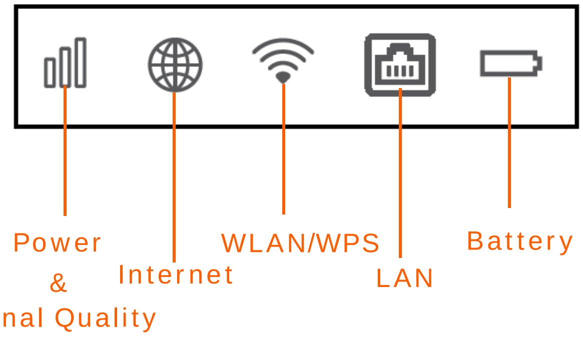
The following graphic displays the front panel of the LTE Device.

Figure 5 LTE Device Front Panel



1.3.2 LEDs

Figure 6 Front Panel LEDs



The following table describes the LEDs.

Table 1 Front Panel LEDs

LED	COLOR	STATUS	DESCRIPTION
📶 Power & Signal Quality	Green	On	The LTE Device is receiving power and having excellent signal strength.
	Amber	On	The LTE Device is receiving power and having fair signal strength.
	Red	On	The LTE Device is receiving power and having poor signal strength.
		Blinking	The LTE Device is receiving power but not having 4G/3G/2G signals.
	Off		The LTE Device is not receiving power.

Table 1 Front Panel LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
Internet	Green	On	The LTE Device’s 4G connection is ready but no new SMS text messages.
		Blinking (slow)	The LTE Device’s 4G connection is not ready and there is no new SMS text messages.
		Blinking (fast)	The LTE Device’s 4G connection is ready and there is a new SMS text message.
	Amber	On	The LTE Device’s 3G/2G connection is ready but no new SMS text messages.
		Blinking (slow)	The LTE Device’s 3G/2G connection is not ready and there is no new SMS text messages.
		Blinking (fast)	The LTE Device’s 3G/2G connection is ready and there is a new SMS text message.
	Off		The WAN connection is not ready, or has failed, and there is no new SMS text messages.
WLAN/WPS	Green	On	The LTE Device is ready and the 2.4GHz wireless LAN is on, but is not sending/receiving data through the wireless LAN.
		Blinking (slow)	The LTE Device is ready and WPS is on.
		Blinking (fast)	The LTE Device is sending/receiving data through the wireless LAN.
	Off		The wireless LAN is not ready or has failed or WPS is disabled.
LAN	Green	On	The LTE Device’s LAN connection is ready.
		Blinking	The LTE Device is sending/receiving data through the LAN.
	Off		The LAN connection is not ready, or has failed.
Battery	Green	On	A battery is installed in the LTE Device, and it’s fully charged. Note: Remove the battery or disconnect the power cable when the battery is fully charged.
	Amber	Blinking	A battery is installed in the LTE Device, and it’s charging.
	Green & Amber	Alternating	The **Battery** LED will alternate between green and amber in the following situations: • A wrong type of battery is being used, or the battery is damaged (correct type of battery: lithium-ion battery). • The battery was removed while charging. • The battery temperature is too high or too low. Note: The recommended ambient temperature range for an operating environment is 0°C to 40°C (32°F to 104°F).
	Off		No battery is installed in the LTE Device, or the power cable is not connected to the LTE3302-M432 to charge the battery installed in the LTE3302-M432.

1.3.3 Rear Panel

The following graphics displays the rear panels of the LTE Device.

Figure 7 LTE3302-M432 Rear Panel

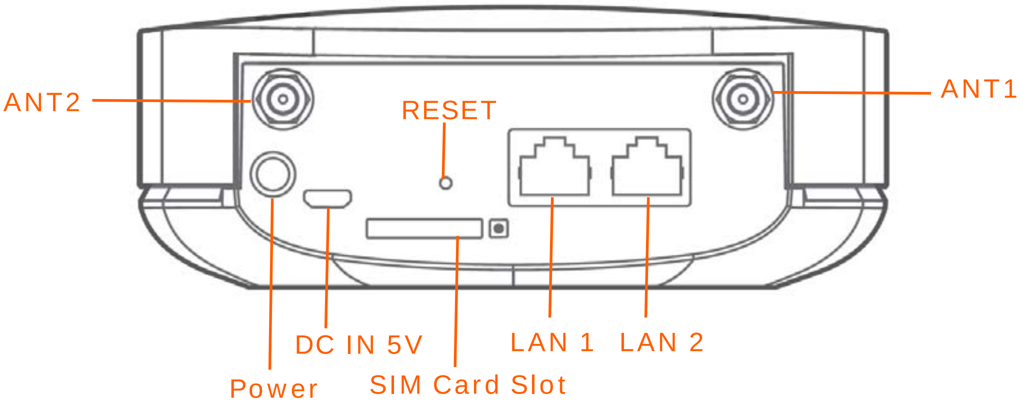
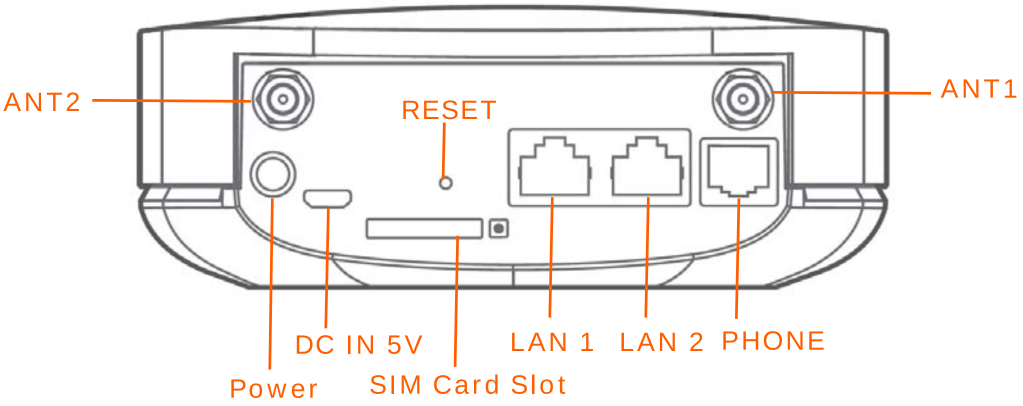


Figure 8 LTE3312-M432 Rear Panel



The following table describes the items on the rear panel.

Table 2 Rear Panel Ports

LABEL	DESCRIPTION
ANT1 & ANT2	Install two external antennas to improve your wireless WAN signals.
Power Button	Press the power button after the power cable is connected to start the device.
DC IN 5V	Connect the power cable to the micro USB port and press the power button to start the device.
SIM Card Slot	Press the button next to the SIM card slot to release the tray. Position a SIM card in the tray and slide it back into the LTE Device. Note: Correctly and securely insert your SIM card into a SIM card adapter to avoid possible damage to your device, if it's needed.
Reset	Press the button to return the LTE Device to the factory defaults, if you forget your password or cannot access the Web Configurator.
LAN1 ~ LAN2	Connect a device with an Ethernet port that requires high-speed Internet access. For example, connect a computer, NAS storage device, gaming console and so on.
PHONE (LTE3312-M432 only)	Connect an analog phone to the PHONE port to make phone calls over the Internet.

1.3.4 Wall Mounting

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

Table 3 Wall Mounting Information

Distance between holes	55 mm
M4 Screws	Two
Screw anchors (not provided)	Two

1 Select a position free of obstructions on a wall strong enough to hold the weight of the device.

2 Mark two holes on the wall at the appropriate distance apart for the screws.

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

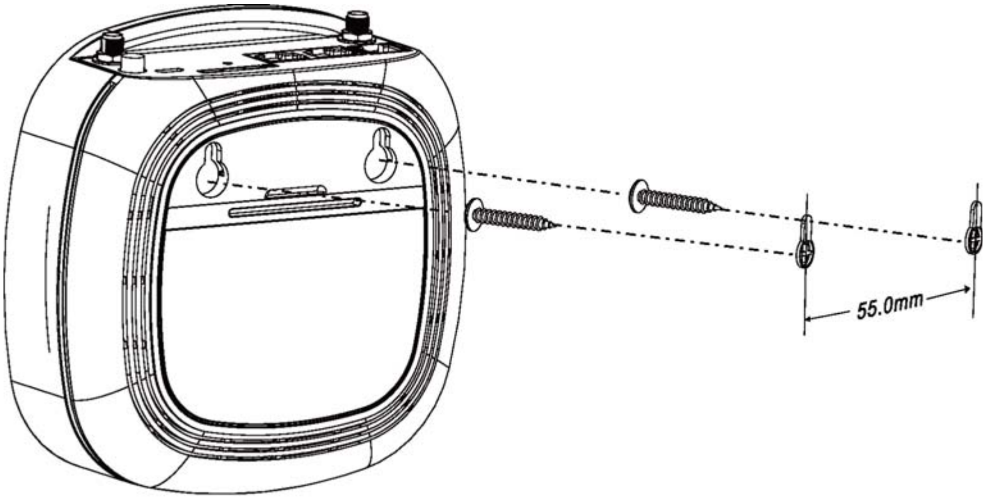
3 If using screw anchors, drill two holes for the screw anchors into the wall. Push the anchors into the full depth of the holes, then insert the screws into the anchors. Do not insert the screws all the way in - leave a small gap of about 0.5 cm.

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

4 Make sure the screws are fastened well enough to hold the weight of the LTE Device with the connection cables.

5 Align the holes on the back of the LTE Device with the screws on the wall. Hang the LTE Device on the screws.

Figure 9 Wall Mounting Example



Note: The mounting kit is not provided.

CHAPTER 2
Introducing the Web Configurator

2.1 Overview

This user's guide uses the LTE3312-M432 screens as examples. The screens may vary slightly for different models.

This chapter describes how to access the LTE Device 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 LTE Device via Internet browser. The recommended screen resolution is 1024 by 768 pixels. In order to use the Web Configurator successfully, use the supported browsers as shown below:

- Internet Explorer 9.0 and later versions
- Mozilla Firefox 21 and later versions
- Safari 6.0 and later versions
- Google Chrome 26.0 and later versions. 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 your browser help to see how to make sure these functions are allowed.

2.2 Accessing the Web Configurator

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

2 Launch your web browser.

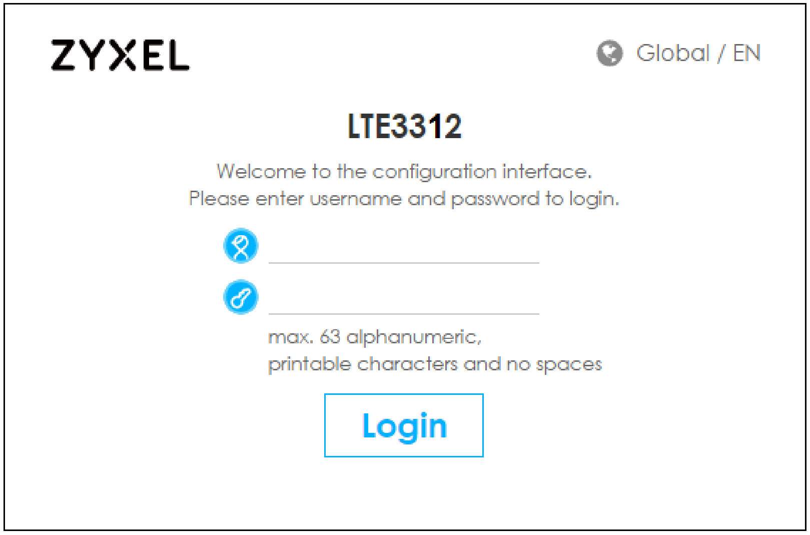
3 Type "http://192.168.1.1" as the website address.

Your computer must be in the same subnet in order to access this website address.

2.2.1 Login Screen

The Web Configurator initially displays the following login screen.

Figure 10 Login screen



LTE3312

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

max. 63 alphanumeric,
printable characters and no spaces

The following table describes the labels in this screen.

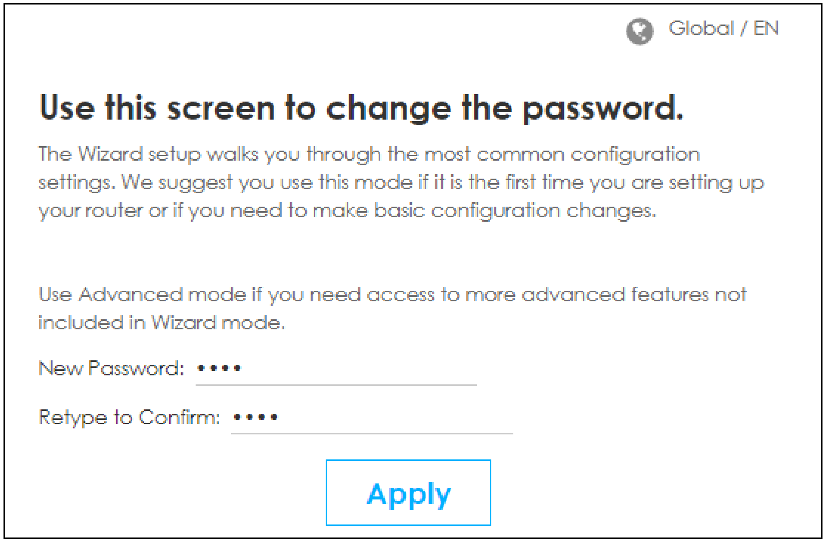
Table 4 Login screen

LABEL	DESCRIPTION
User	Type "admin" (default) as the user name.
Password	Type "1234" (default) as the password. Click **Login**.

2.2.2 Password Screen

You should see a screen asking you to change your password (highly recommended) as shown next.

Figure 11 Change Password screen



Use this screen to change the password.

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

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

New Password: ••••

Retype to Confirm: ••••

The following table describes the labels in this screen.

Table 5 Login screen

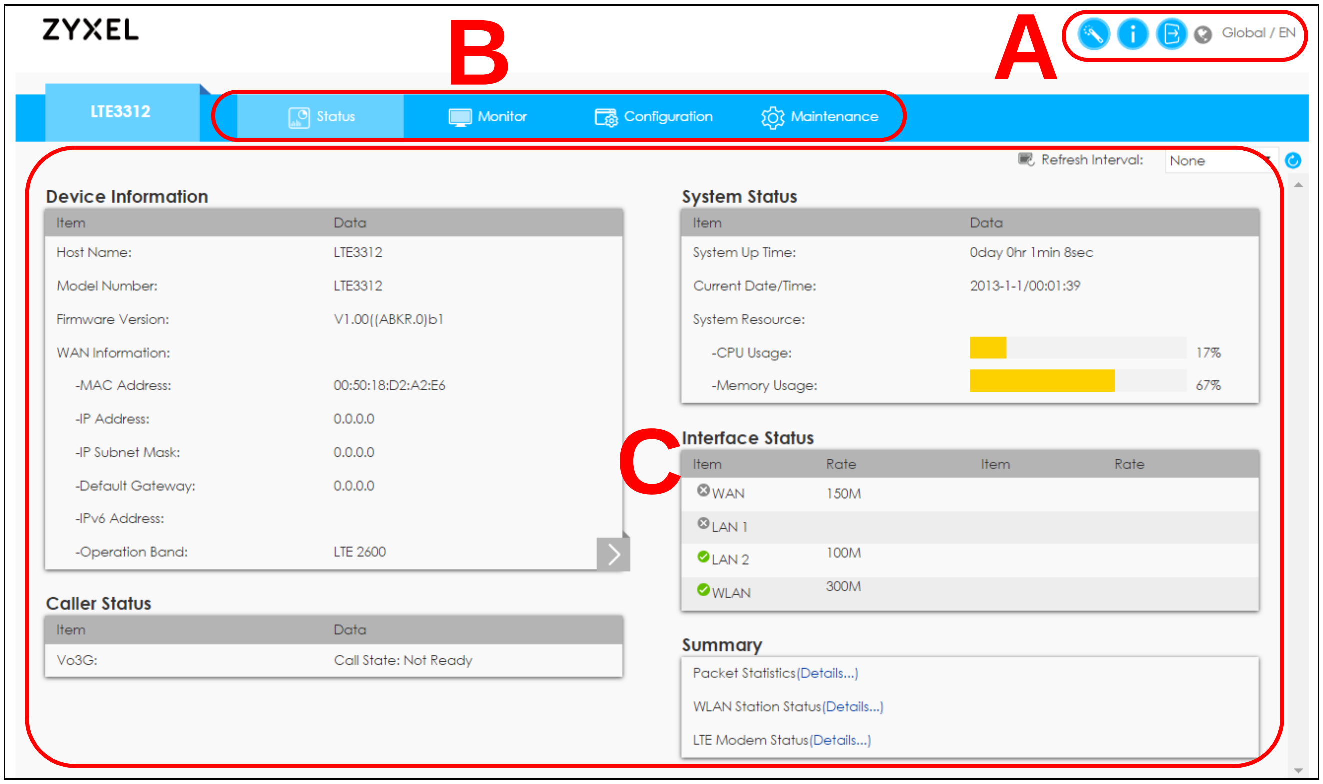
LABEL	DESCRIPTION
New Password	Type a new password.
Retype to Confirm	Retype the password for confirmation.
Apply	Click **Apply** to save your changes back to the LTE Device.

Note: The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes; go to Section 23.3 on page 145 to change this). Simply log back into the LTE Device if this happens.

2.3 The Main Screen

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

Figure 12 The Web Configurator's Main Screen



Device Information

Item	Data
Host Name:	LTE3312
Model Number:	LTE3312
Firmware Version:	V1.00((ABKR.0)b1
WAN Information:	
-MAC Address:	00:50:18:D2:A2:E6
-IP Address:	0.0.0.0
-IP Subnet Mask:	0.0.0.0
-Default Gateway:	0.0.0.0
-IPv6 Address:	
-Operation Band:	LTE 2600

Caller Status

Item	Data
Vo3G:	Call State: Not Ready

System Status

Item	Data
System Up Time:	0day 0hr 1min 8sec
Current Date/Time:	2013-1-1/00:01:39
System Resource:	
-CPU Usage:	17%
-Memory Usage:	67%

Interface Status

Item	Rate	Item	Rate
WAN	150M		
LAN 1			
LAN 2	100M		
WLAN	300M		

Summary

Packet Statistics(Details...)

WLAN Station Status(Details...)

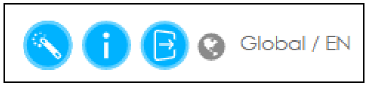
LTE Modem Status(Details...)

- **A** - Title Bar
- **B** - Navigation Panel
- **C** - Main Window

2.3.1 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 13 Title Bar



The icons provide the following functions.

Table 6 Title Bar: Web Configurator Icons

LABEL	DESCRIPTION
Wizard	Click this icon to open the setup wizard for the LTE Device.
About	Click this icon to open a screen where you can click a link to visit the Zyxel web site to see detailed product information.
Logout	Click this icon to log out of the Web Configurator.
Language Global / EN	Select the language you prefer for the Web Configurator.

2.3.2 Navigation Panel

The following table describes the screens that you can access using the navigation panel.

Table 7 Navigation Panel

LINK	TAB	FUNCTION
Status		This screen shows the LTE Device'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 LTE Device.
DHCP Table		Use this screen to view current DHCP client information.
ARP Table		Use this screen to view the ARP table. It displays the mappings of IP addresses to MAC addresses.
Packet Statistics		Use this screen to view port status and packet specific statistics.
WLAN Station Status		Use this screen to view the wireless stations that are currently associated to the LTE Device's 2.4GHz wireless LAN.
LTE Modem Status		Use this screen to view the detailed information about the modem, SIM card status, and SIM card details. You can also view the LTE connection status.
Configuration		
Network		
WAN	Management WAN	This screen allows you to configure ISP parameters, WAN IP address assignment, and DNS servers.
	Network Scan	Use this screen to specify the type of the mobile network to which the LTE Device is connected and how you want the LTE Device to connect to an available mobile network.
	IPv6	Use this screen to configure the LTE Device's IPv6 settings.
	PIN Management	Use this screen to enable the SIM card PIN code authentication and enter the PIN code.

Table 7 Navigation Panel (continued)

LINK	TAB	FUNCTION
Wireless LAN	General	Use this screen to enable the wireless LAN and configure wireless LAN and wireless security settings.
	More AP	Use this screen to configure multiple BSSs on the LTE Device.
	MAC Filter	Use the MAC filter screen to allow or deny wireless stations based on their MAC addresses from connecting to the LTE Device.
	Advanced	This screen allows you to configure advanced wireless LAN settings.
	QoS	Use this screen to configure Wi-Fi Multimedia Quality of Service (WMM QoS). WMM QoS allows you to prioritize wireless traffic according to the delivery requirements of individual services.
	WPS	Use this screen to configure the WPS settings.
	WPS Station	Use this screen to add a wireless station using WPS.
	Scheduling	Use this screen to schedule the times the Wireless LAN is enabled.
	WDS	Use this screen to enable and configure the WDS settings.
LAN	IP	Use this screen to configure LAN IP address and subnet mask.
DHCP Server	General	Use this screen to enable the LTE Device's DHCP server.
	Advanced	Use this screen to assign IP addresses to specific individual computers based on their MAC addresses and to have DNS servers assigned by the DHCP server.
	Client List	Use this screen to view information related to your DHCP status.
NAT	General	Use this screen to enable NAT.
	Port Forwarding	Use this screen to configure servers behind the LTE Device and forward incoming service requests to the server(s) on your local network.
	Port Trigger	Use this screen to change your LTE Device's port triggering settings.
	ALG	Use this screen to enable or disable SIP (VoIP) ALG (Application Layer Gateway) in the LTE Device.
Dynamic DNS	Dynamic DNS	Use this screen to set up dynamic DNS.
Routing	Static Route	Use this screen to configure IP static routes.
	Dynamic Routing	Use this screen to enable and configure RIP on the LTE Device.
Interface Group	Interface Group	Use this screen to create a new interface group.
Security		
Firewall	General	Use this screen to activate/deactivate the firewall.
	Services	This screen shows a summary of the firewall rules, and allows you to edit/add a firewall rule.
Content Filter	Content Filter	Use this screen to restrict web features and designate a trusted computer. You can also block certain web sites containing certain keywords in the URL.
IPv6 firewall	Services	Use this screen to configure IPv6 firewall rules.
Application		
SMS		Use this screen to send SMS text messages and view messages received on the LTE Device.
Voice over 3G (LTE3312-M432 only)	General	Use this screen to enable Internet phone calls through the LTE Device.
	Call Conf.	Use this screen to create rules for handling incoming calls.
Management		

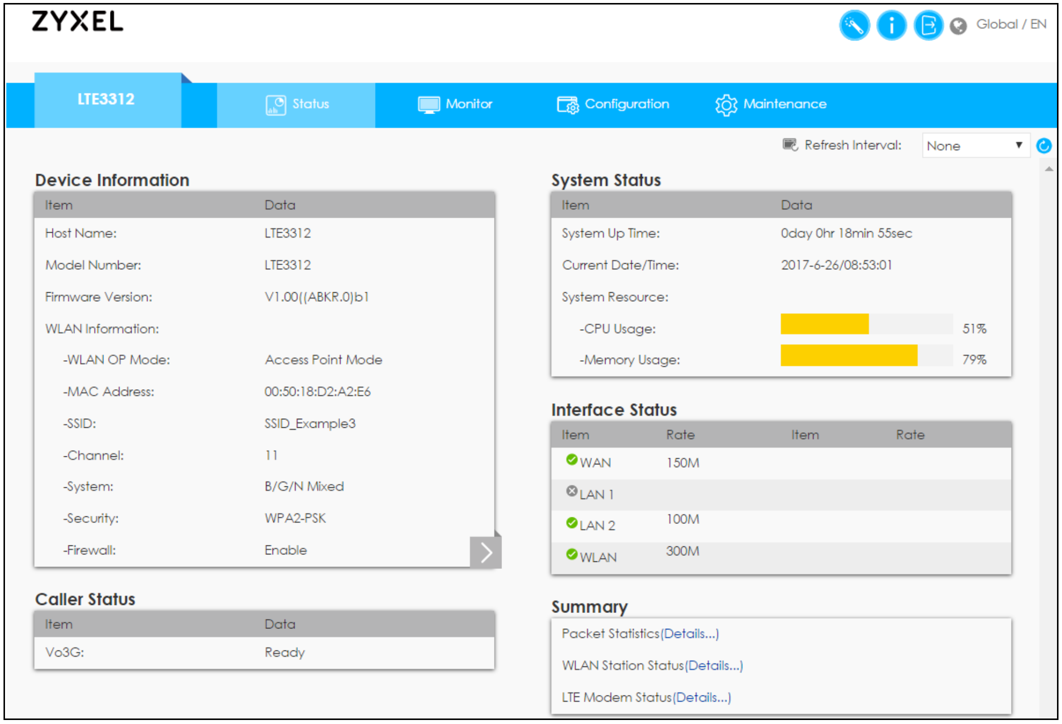
Table 7 Navigation Panel (continued)

LINK	TAB	FUNCTION
Remote MGMT	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the LTE Device.
	Remote Management	Use this screen to configure from which IP address(es) users can access the LTE Device.
Bandwidth Management	General	Use this screen to enable bandwidth management.
	Advanced	Use this screen to set the upstream bandwidth and edit a bandwidth management rule.
UPnP	UPnP	Use this screen to enable UPnP on the LTE Device.
TR069	TR069	Use this screen to configure your LTE Device to be managed by an ACS.
Maintenance		
General	General	Use this screen to view and change administrative settings such as system and domain names.
Account	User Account	Use this screen to change the user name and password of your LTE Device.
Time	Time Setting	Use this screen to change your LTE Device's time and date.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload router firmware to your LTE Device.
Module Upgrade	Module Upgrade	Use this screen to upload LTE module firmware to your LTE Device.
Backup/ Restore	Backup/ Restore	Use this screen to backup and restore the configuration or reset the factory defaults to your LTE Device.
Restart	System Restart	This screen allows you to reboot the LTE Device without turning the power off.

2.4 Status Screen

Click Status to open the **Status** screen.

Figure 14 Status Screen



ZYXEL

Global / EN

LTE3312 | Status | Monitor | Configuration | Maintenance

Refresh Interval: None ▾

Device Information

Item	Data
Host Name:	LTE3312
Model Number:	LTE3312
Firmware Version:	V1.00((ABKR.0)b1
WLAN Information:	
-WLAN OP Mode:	Access Point Mode
-MAC Address:	00:50:18:D2:A2:E6
-SSID:	SSID_Example3
-Channel:	11
-System:	B/G/N Mixed
-Security:	WPA2-PSK
-Firewall:	Enable

Caller Status

Item	Data
Vo3G:	Ready

System Status

Item	Data
System Up Time:	0day 0hr 18min 55sec
Current Date/Time:	2017-6-26/08:53:01
System Resource:	
-CPU Usage:	51%
-Memory Usage:	79%

Interface Status

Item	Rate	Item	Rate
✓ WAN	150M		
⊗ LAN 1			
✓ LAN 2	100M		
✓ WLAN	300M		

Summary

Packet Statistics(Details...)

WLAN Station Status(Details...)

LTE Modem Status(Details...)

The following table describes the icons shown in the **Status** screen.

Table 8 Status Screen Icon Key

ICON	DESCRIPTION
Refresh Interval: None ▾	Select a number of seconds or **None** from the drop-down list box to refresh all screen statistics automatically at the end of every time interval or to not refresh the screen statistics.
↻	Click this button to refresh the status screen statistics.
Status	Click this icon to see the **Status** page. The information in this screen depends on the device mode you select.
Monitor	Click this icon to see the **Monitor** navigation menu.
Configuration	Click this icon to see the **Configuration** navigation menu.
Maintenance	Click this icon to see the **Maintenance** navigation menu.

The following table describes the labels shown in the **Status** screen.

Table 9 Status Screen

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	
MAC Address	This shows the WAN Ethernet adapter MAC Address of your LTE Device.

Table 9 Status Screen (continued)

LABEL	DESCRIPTION
IP Address	This shows the WAN port's IP address.
IP Subnet Mask	This shows the WAN port's subnet mask.
Default Gateway	This shows the WAN port's gateway IP address.
IPv6 Address	This shows the IPv6 address of the LTE Device on the WAN.
Operation Band	This shows the network type and the frequency band used by the mobile network to which the LTE Device is connecting.
LAN Information	
MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
IP Address	This shows the LAN port's IP address.
IP Subnet Mask	This shows the LAN port's subnet mask.
DHCP	This shows the LAN port's DHCP role - **Server** or **Disable**.
IPv6 Address	This shows the IPv6 address of the LTE Device on the LAN.
WLAN Information	
WLAN OP Mode	This is the device mode to which the LTE Device's wireless LAN is set - **Access Point Mode**.
MAC Address	This shows the 2.4GHz wireless adapter MAC Address of your device.
SSID	This shows a descriptive name used to identify the LTE Device in the 2.4GHz wireless LAN.
Channel	This shows the channel number which you select manually.
System	This shows the wireless standards the LTE Device supports.
Security	This shows the level of wireless security the LTE Device is using.
Firewall	This shows whether the firewall is enabled or not.
Caller Status (LTE3312-M432 only)	
Item	This column shows the caller ID when you make phone calls through the LTE3312-M432.
Data	This column shows the current state of the phone call.
System Status	
Item	This column shows the type of data the LTE Device is recording.
Data	This column shows the actual data recorded by the LTE Device.
System Up Time	This is the total time the LTE Device has been on.
Current Date/Time	This field displays your LTE Device's present date and time.
System Resource	
- CPU Usage	This displays what percentage of the LTE Device's processing ability is currently used. When this percentage is close to 100%, the LTE Device is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management.)
- Memory Usage	This shows what percentage of the heap memory the LTE Device is using.
Interface Status	
Item	This displays the LTE Device port types. The port types are: **WAN**, **LAN** and **WLAN**.

Table 9 Status Screen (continued)

LABEL	DESCRIPTION
Rate	For the LAN ports, this 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 the maximum transmission rate when the WLAN is enabled and is left blank when the WLAN is disabled.
Summary	
Packet Statistics	Click **Details...** to go to the **Monitor > Packet Statistics** screen (Section 5.6 on page 53). Use this screen to view port status and packet specific statistics.
WLAN Station Status	Click **Details...** to go to the **Monitor > WLAN Station Status** screen (Section 5.7 on page 54). Use this screen to view the wireless stations that are currently associated to the LTE Device's 2.4GHz wireless LAN.
LTE Modem Status	Click **Details...** to go to the **Monitor > LTE Modem Status** screen (Section 5.7 on page 54). 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 3
Setup Wizard

3.1 Overview

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

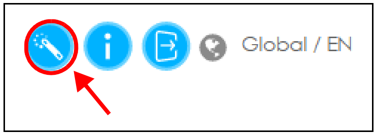
The Web Configurator's wizard helps you configure your device to access the Internet and change the wireless LAN settings. Refer to your ISP for your Internet account information. Leave a field blank if you don't have that information.

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 top right corner of the web configurator to open the Wizard screen.

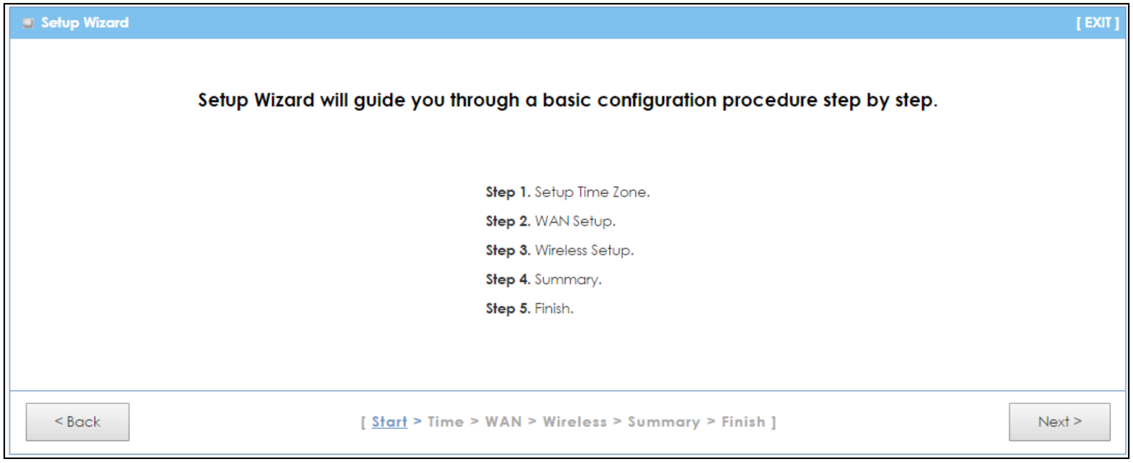
Figure 15 Title Bar: Wizard icon



3.3 Wizard Setup

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

Figure 16 Wizard: Start

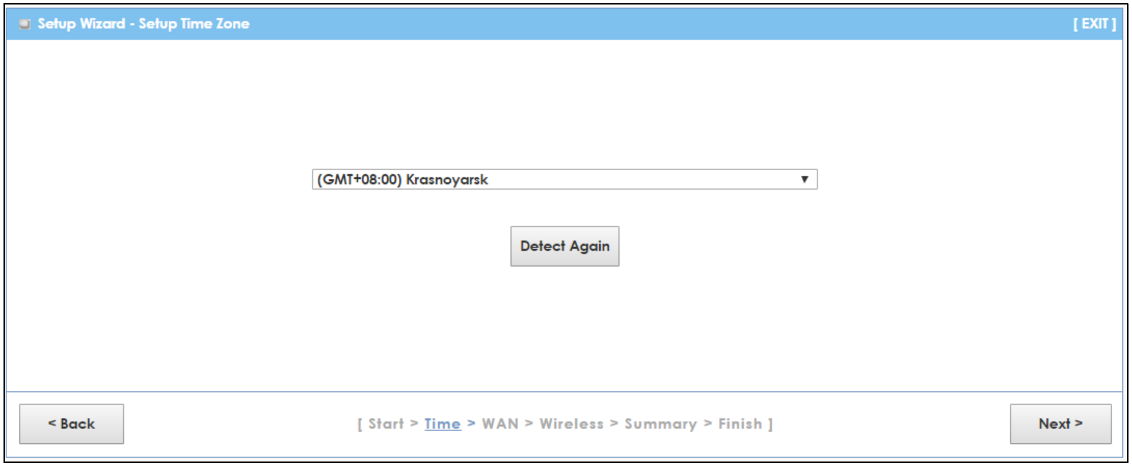


Setup Wizard will guide you through a basic configuration procedure step by step.

Step 1. Setup Time Zone.
Step 2. WAN Setup.
Step 3. Wireless Setup.
Step 4. Summary.
Step 5. Finish.

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

Figure 17 Wizard: Time



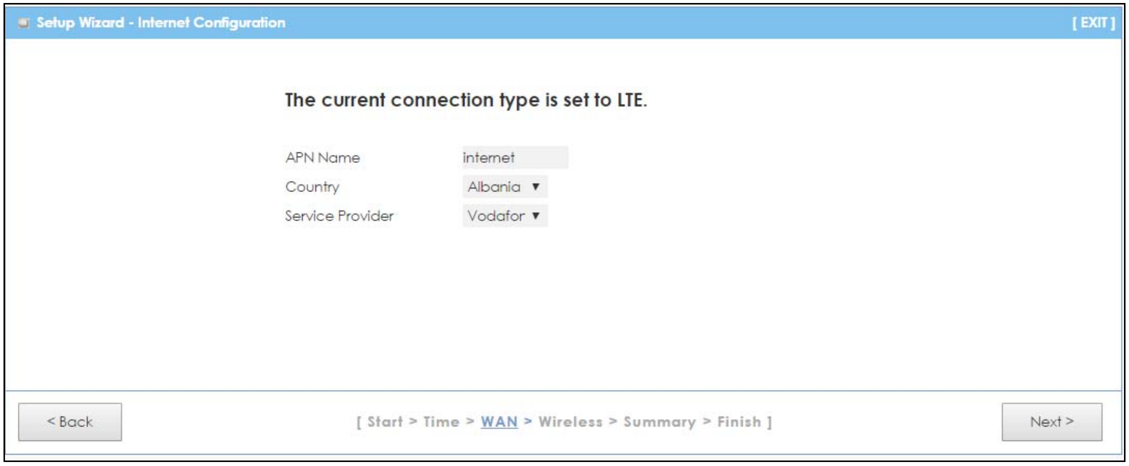
Setup Wizard - Setup Time Zone
[EXIT]

(GMT+08:00) Krasnoyarsk

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

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

Figure 18 Wizard: WAN



Setup Wizard - Internet Configuration
[EXIT]

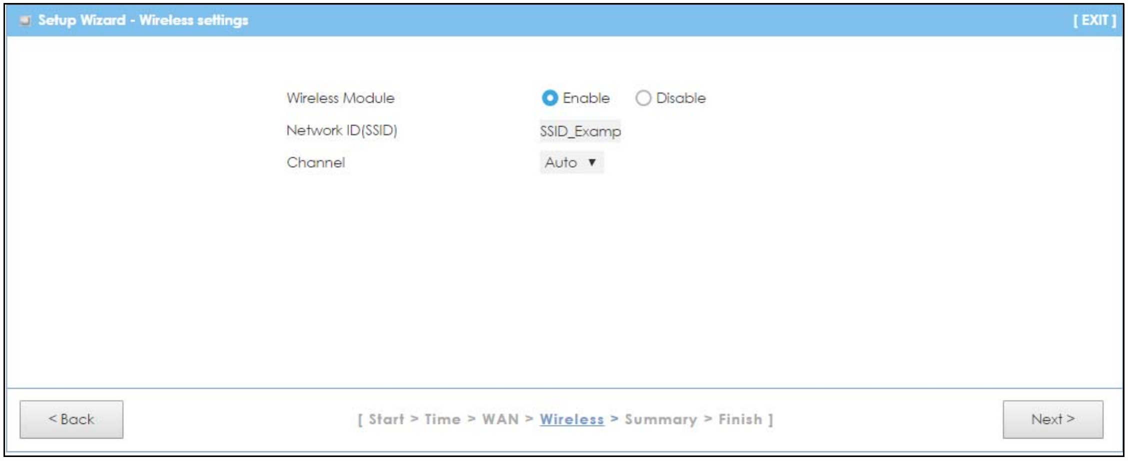
The current connection type is set to LTE.

APN Name internet
Country Albania
Service Provider Vodafor

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

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

Figure 19 Wizard: Wireless Settings


Setup Wizard - Wireless settings
[EXIT]
< Back
[Start > Time > WAN > Wireless > Summary > Finish]
Next >

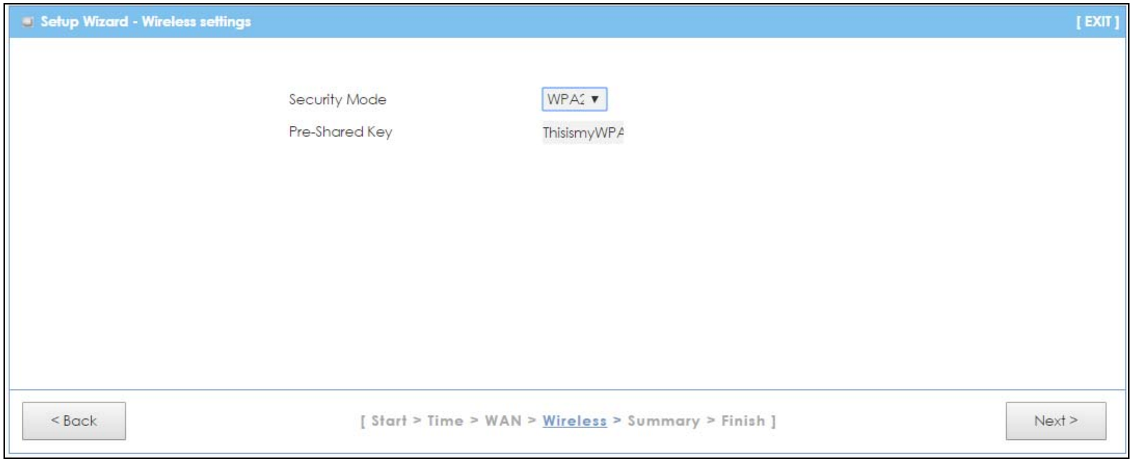
Wireless Module ● Enable ○ Disable

Network ID(SSID) SSID_Examp

Channel Auto ▼

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

Figure 20 Wizard: Wireless Security

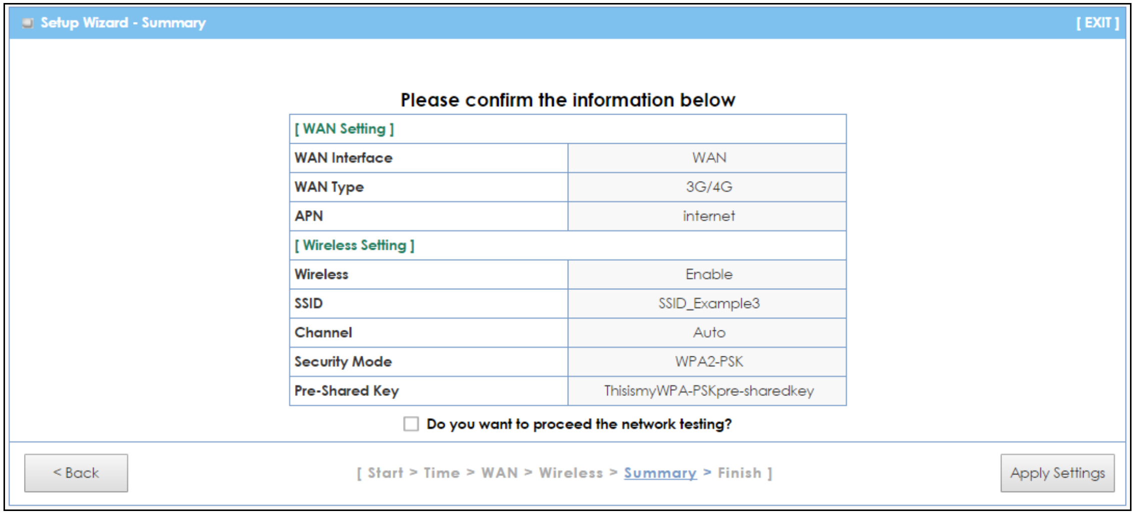

Setup Wizard - Wireless settings
[EXIT]
< Back
[Start > Time > WAN > Wireless > Summary > Finish]
Next >

Security Mode WPA2 ▼

Pre-Shared Key ThisismyWPA

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

Figure 21 Wizard: Summary



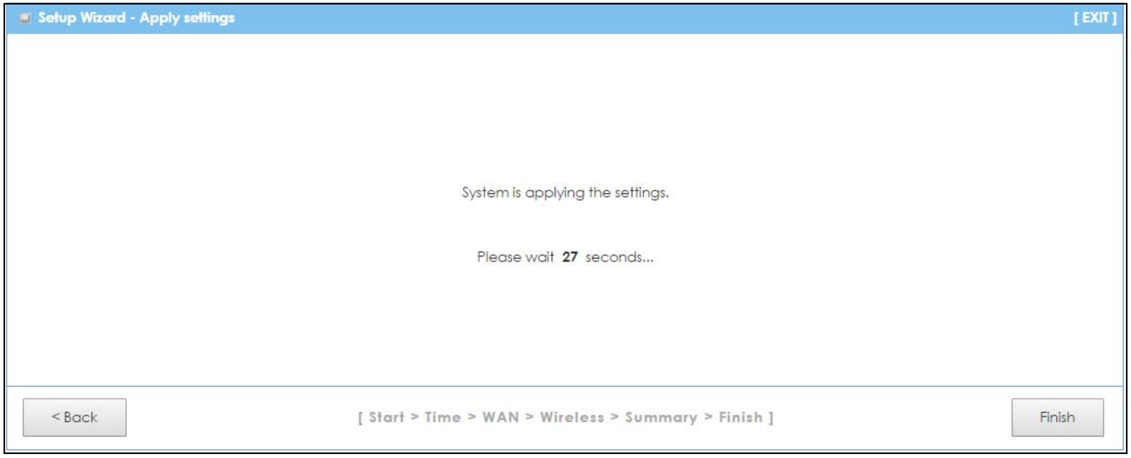
Please confirm the information below

[WAN Setting]	
WAN Interface	WAN
WAN Type	3G/4G
APN	internet
[Wireless Setting]	
Wireless	Enable
SSID	SSID_Example3
Channel	Auto
Security Mode	WPA2-PSK
Pre-Shared Key	ThisismyWPA-PSKpre-sharedkey

□ Do you want to proceed the network testing?

7 Wait while the system applies settings.

Figure 22 Wizard: Apply Settings



Setup Wizard - Apply settings
[EXIT]

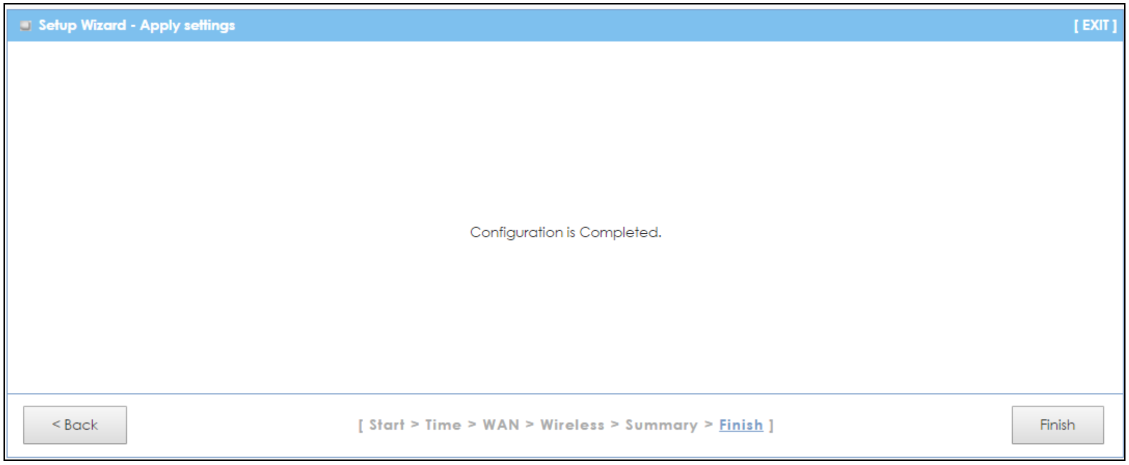
System is applying the settings.

Please wait 27 seconds...

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

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

Figure 23 Wizard: Finish



Setup Wizard - Apply settings
[EXIT]

Configuration is Completed.

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

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

CHAPTER 4
Tutorials

4.1 Overview

This chapter provides tutorials for setting up your LTE Device.

- Set Up a Wireless Network Using WPS
- Connect to the LTE Device's Wi-Fi Network
- Use Multiple SSIDs on the LTE Device
- Make an Internet Phone (Vo3G) Call on the LTE3312-M432
- Configure a Firewall Rule
- Configure Content Filtering
- Upgrade Firmware on the LTE Device
- Back up a Configuration File
- Restore Previous Configuration
- Send a New SMS Text Message

4.2 Set Up a Wireless Network Using WPS

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

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

- **Push Button Configuration (PBC)** - create a secure wireless network simply by pressing a button. See Section 4.2.1 on page 34. This is the easier method.
- **PIN Configuration** - create a secure wireless network simply by entering a wireless client's PIN (Personal Identification Number) in the LTE Device's interface. See Section 4.2.2 on page 35. This is the more secure method, since one device can authenticate the other.

4.2.1 Push Button Configuration (PBC)

1 Make sure that your LTE Device is turned on. Make sure the wireless LAN is turned on by pressing the **WLAN/WPS** button for less than five seconds, and that the device is placed within range of your notebook.

2 WPS is enabled by default on the LTE Device. If not, log into LTE Device's Web Configurator and press the **Push Button** in the **Configuration > Network > Wireless LAN 2.4G > WPS Station** screen. You can either press the WPS button on the LTE Device's top panel or press **Push Button** in the screen.

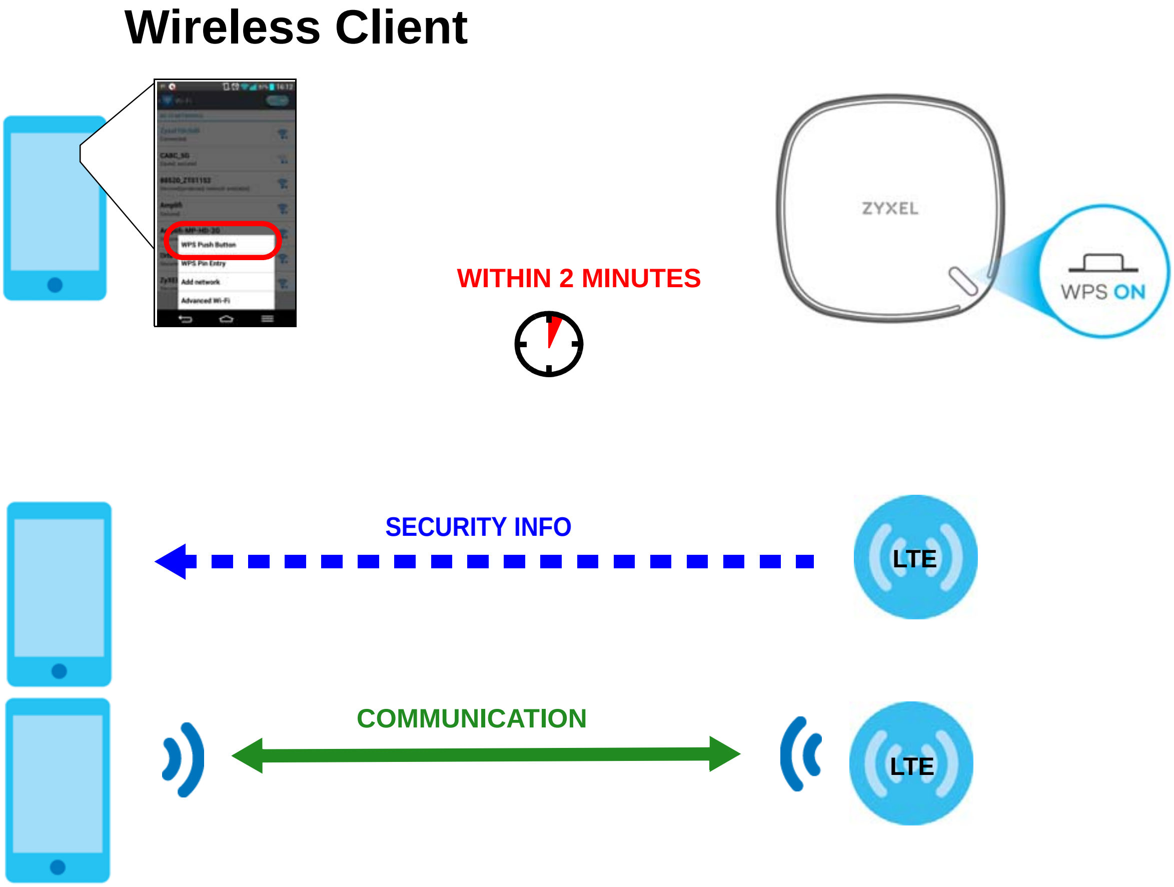
3 Go to your phone settings and turn on Wi-Fi. Open the Wi-Fi networks list and tap WPS Push Button or the WPS icon ( ).

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

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

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

Figure 24 Example WPS Process: PBC Method



4.2.2 PIN Configuration

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

1 Go to your phone settings and turn on Wi-Fi. Open the Wi-Fi networks list and tap WPS PIN Entry get a PIN number.

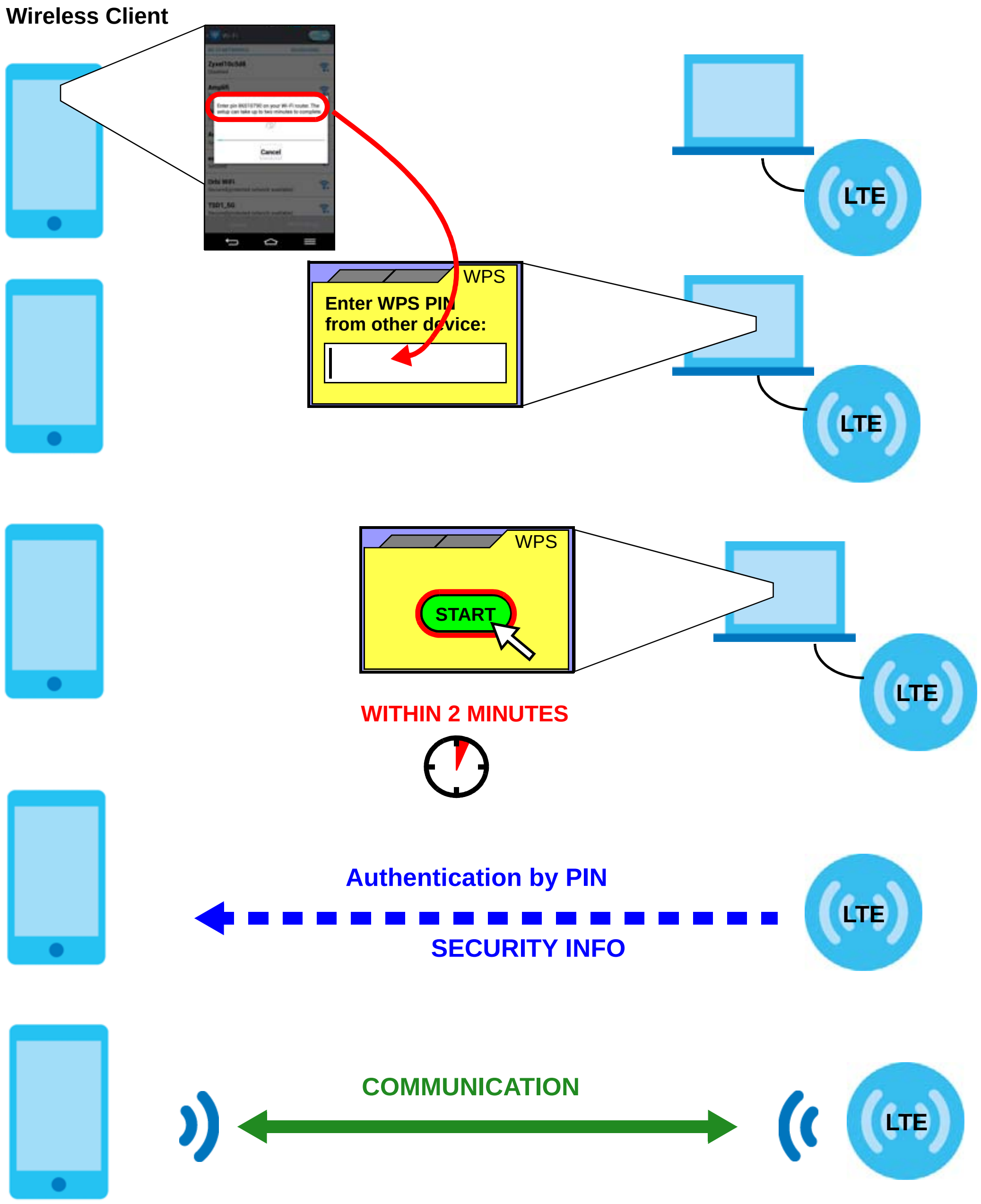
2 Enter the client's PIN number to the **PIN** field in the **Configuration > Network > Wireless LAN > WPS Station** screen on the LTE Device.

3 Click **Start** button (or button next to the PIN field) on the LTE Device's **WPS Station** screen within two minutes.

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

The following figure shows you the example to set up wireless network and security on LTE Device and wireless client (ex. the Android smartphone in this example) by using PIN method.

Figure 25 Example WPS Process: PIN Method



4.3 Connect to the LTE Device’s Wi-Fi Network

In this example, you’ve changed the LTE Device’s wireless settings in the wizard to the following settings.

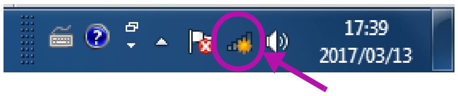
SSID	SSID_Example3

Channel	6
Security	WPA2-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)

Note: In this example, we use a Windows 7 laptop that has a built-in wireless adapter as the wireless client.

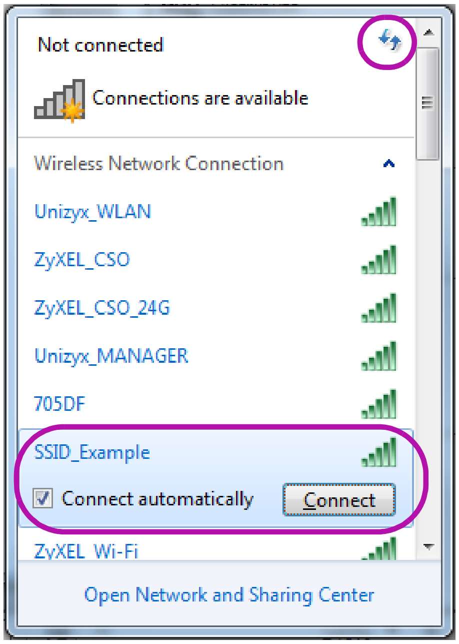
1 The LTE Device supports IEEE 802.11b, IEEE 802.11g, and IEEE 802.11n wireless clients. Make sure that your notebook or computer's wireless adapter supports one of these standards.

2 Click the Wi-Fi icon in your computer's system tray.

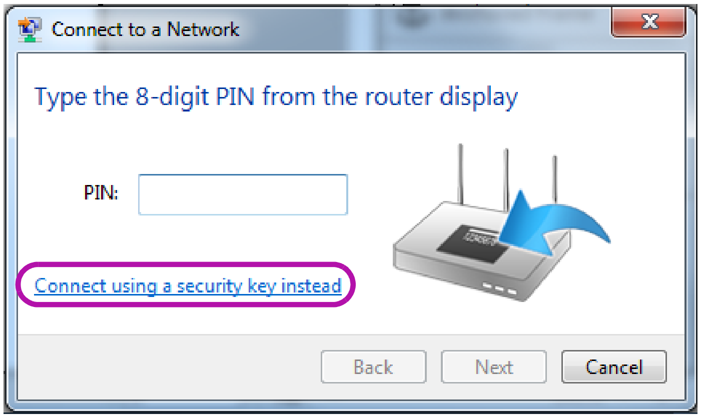


3 The **Wireless Network Connection** screen displays. Click the refresh button to update the list of the available wireless APs within range.

4 Select **SSID_Example3** and click **Connect**.



5 The following screen displays if WPS is enabled on the LTE Device but you didn't press the WPS button. Click **Connect using a security key instead**.



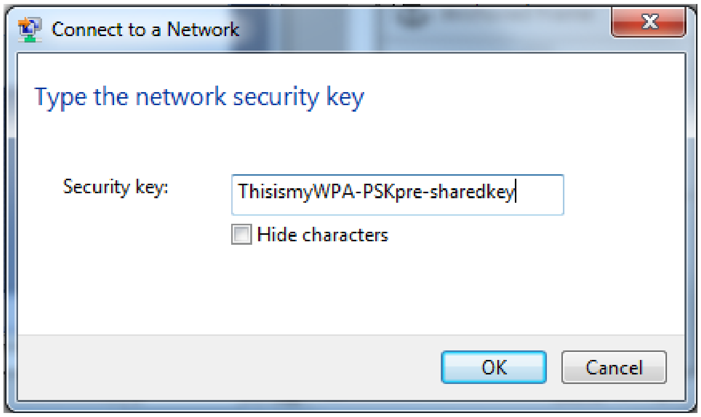
Connect to a Network

Type the 8-digit PIN from the router display

PIN:

Connect using a security key instead

6 Type the security key in the following screen. Click **OK**.



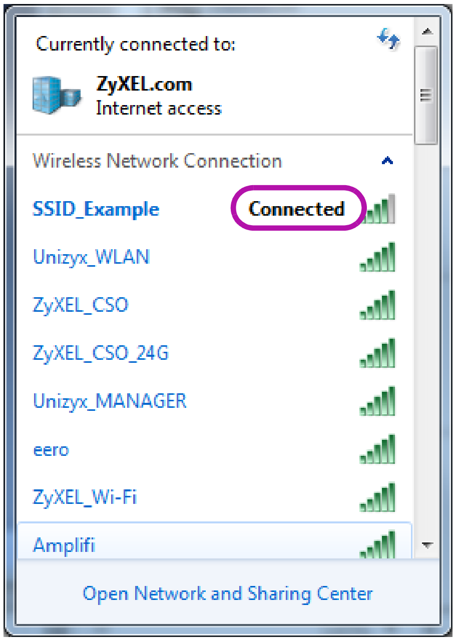
Connect to a Network

Type the network security key

Security key: ThisismyWPA-PSKpre-sharedkey

□ Hide characters

7 Check the status of your wireless connection in the screen below.



Currently connected to:

ZyXEL.com
Internet access

Wireless Network Connection

SSID_Example **Connected**

Unizyx_WLAN

ZyXEL_CSO

ZyXEL_CSO_24G

Unizyx_MANAGER

eero

ZyXEL_Wi-Fi

Amplifi

Open Network and Sharing Center

8 If the wireless client keeps trying to connect to or acquiring an IP address from the LTE Device, make sure you entered the correct security key.

If the connection has limited or no connectivity, make sure the DHCP server is enabled on the LTE Device.

If your connection is successful, open your Internet browser and enter http://www.zyxel.com or the URL of any other web site in the address bar. If you are able to access the web site, your wireless connection is successfully configured.

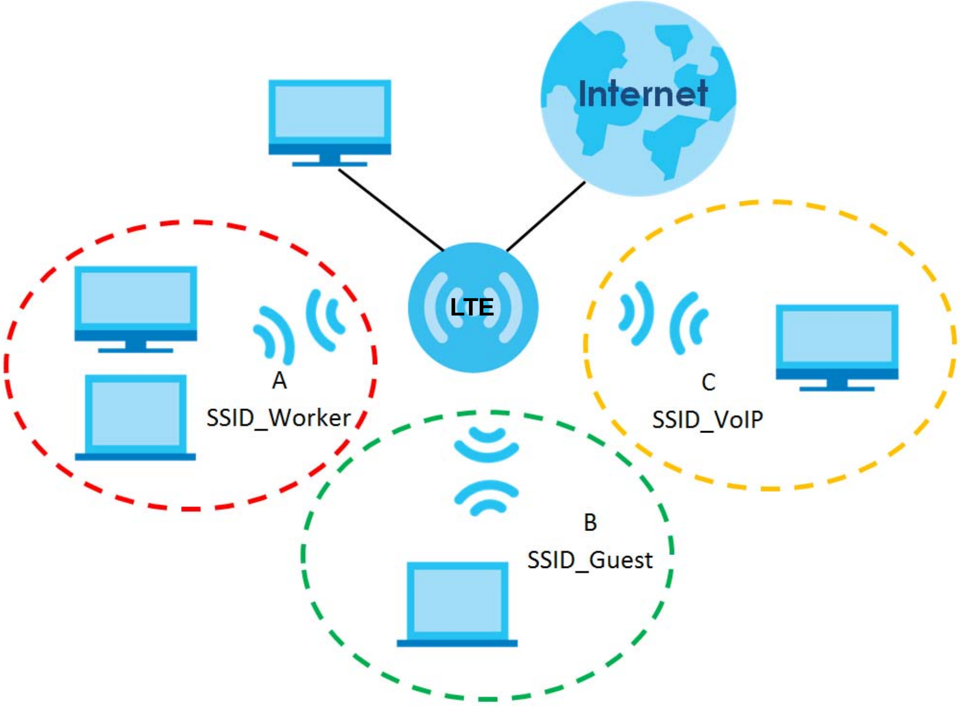
4.4 Use Multiple SSIDs on the LTE Device

You can configure more than one SSID on a LTE Device. See Section 7.4 on page 78.

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

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

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



4.4.1 Configuring Security Settings of Multiple SSIDs

The LTE Device is in router mode by default.

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

SSID	SECURITY TYPE	KEY
SSID_Worker	WPA2-PSK WPA Compatible	DoNotStealMyWirelessNetwork
SSID_VoIP	WPA-PSK	VoIPOnly12345678
SSID_Guest	WPA-PSK	keyexample123

1 Connect your computer to the LAN port of the LTE Device using an Ethernet cable.

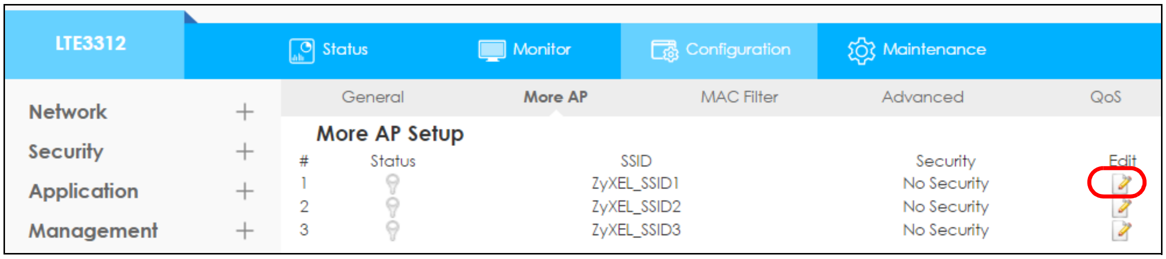
2 The default IP address of the LTE Deviceis “192.168.1.1”. In this case, your computer must have an IP address in the range between “192.168.1.2” and “192.168.1.254”.

3 Click **Start > Run** on your computer in Windows. Type “cmd” in the dialog box. Enter “ipconfig” to show your computer’s IP address. If your computer’s IP address is not in the correct range then see Appendix A on page 158 for information on changing your computer’s IP address.

4 After you’ve set your computer’s IP address, open a web browser such as Internet Explorer and type “http://192.168.1.1” as the web address in your web browser.

5 Enter “admin” as the user name and “1234” (default) as the password and click **Login**.

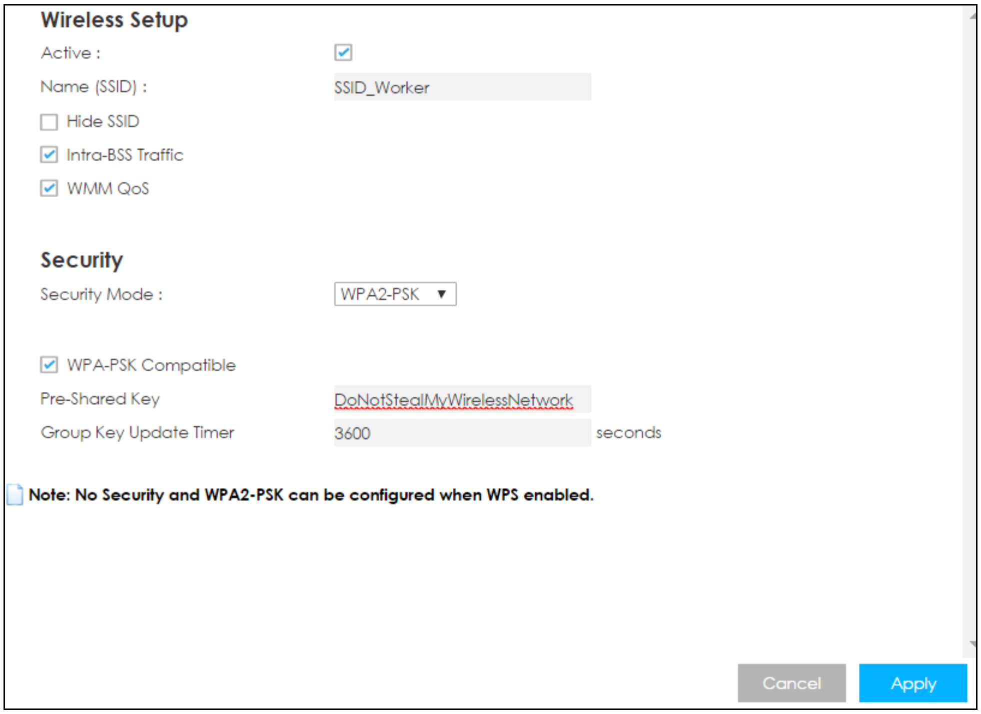
6 Go to **Configuration > Network > Wireless LAN > More AP**. Click the **Edit** icon of the first entry to configure wireless and security settings for **SSID_Worker**.



More AP Setup

#	Status	SSID	Security	Edit
1		ZyXEL_SSID1	No Security	
2		ZyXEL_SSID2	No Security	
3		ZyXEL_SSID3	No Security	

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



Wireless Setup

Active : ☑

Name (SSID) : SSID_Worker

□ Hide SSID

☑ Intra-BSS Traffic

☑ WMM QoS

Security

Security Mode : WPA2-PSK ▼

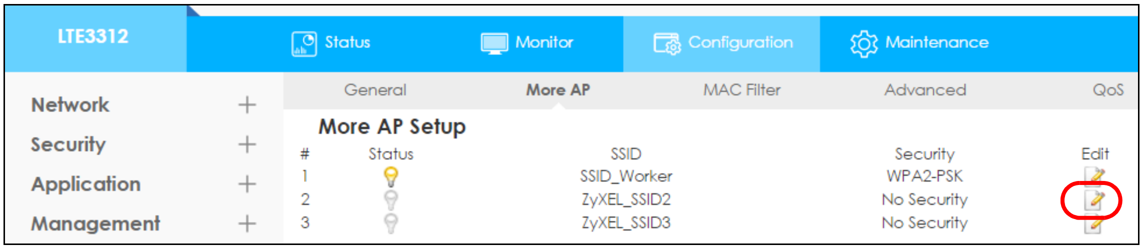
☑ WPA-PSK Compatible

Pre-Shared Key DoNotStealMyWirelessNetwork

Group Key Update Timer 3600 seconds

Note: No Security and WPA2-PSK can be configured when WPS enabled.

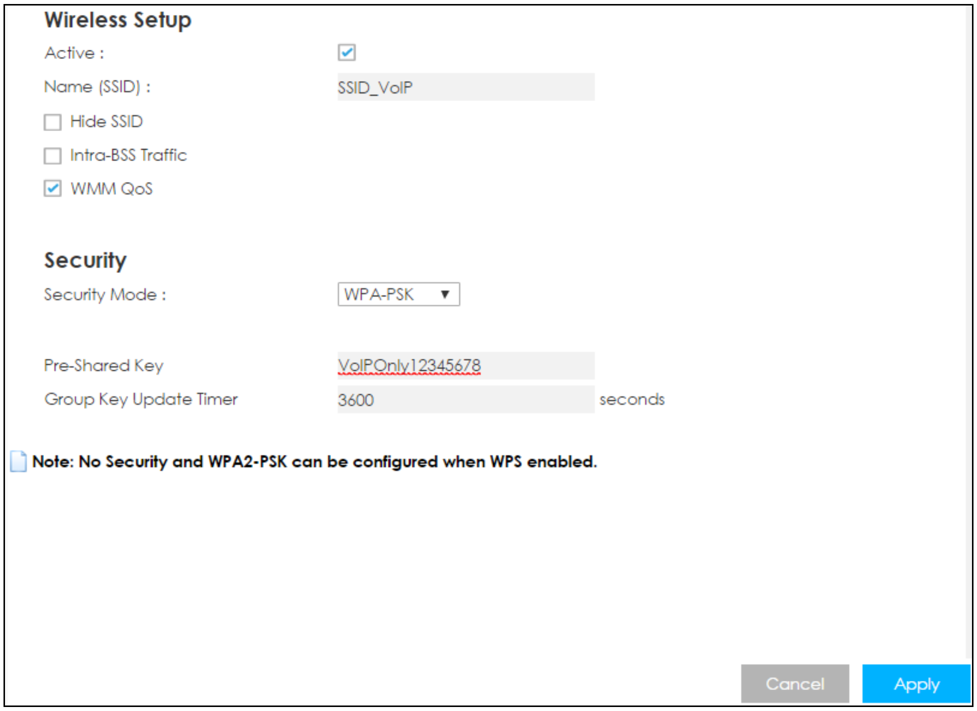
8 Click the **Edit** icon of the second entry to configure wireless and security settings for **SSID_VoIP**.



More AP Setup

#	Status	SSID	Security	Edit
1	💡	SSID_Worker	WPA2-PSK	📝
2	💡	ZyXEL_SSID2	No Security	📝
3	💡	ZyXEL_SSID3	No Security	📝

9 Configure the screen as follows. You do not enable **Intra-BSS Traffic** for **SSID_VoIP**. Click **Apply**.



Wireless Setup

Active : ☑

Name (SSID) : SSID_VoIP

☐ Hide SSID

☐ Intra-BSS Traffic

☑ WMM QoS

Security

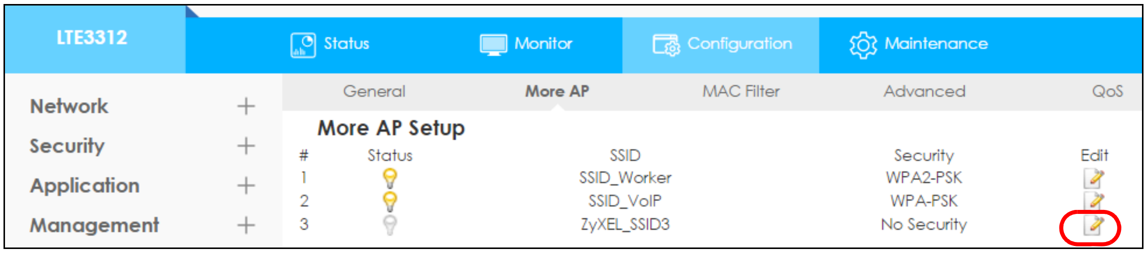
Security Mode : WPA-PSK

Pre-Shared Key: VoIPOnly12345678

Group Key Update Timer: 3600 seconds

Note: No Security and WPA2-PSK can be configured when WPS enabled.

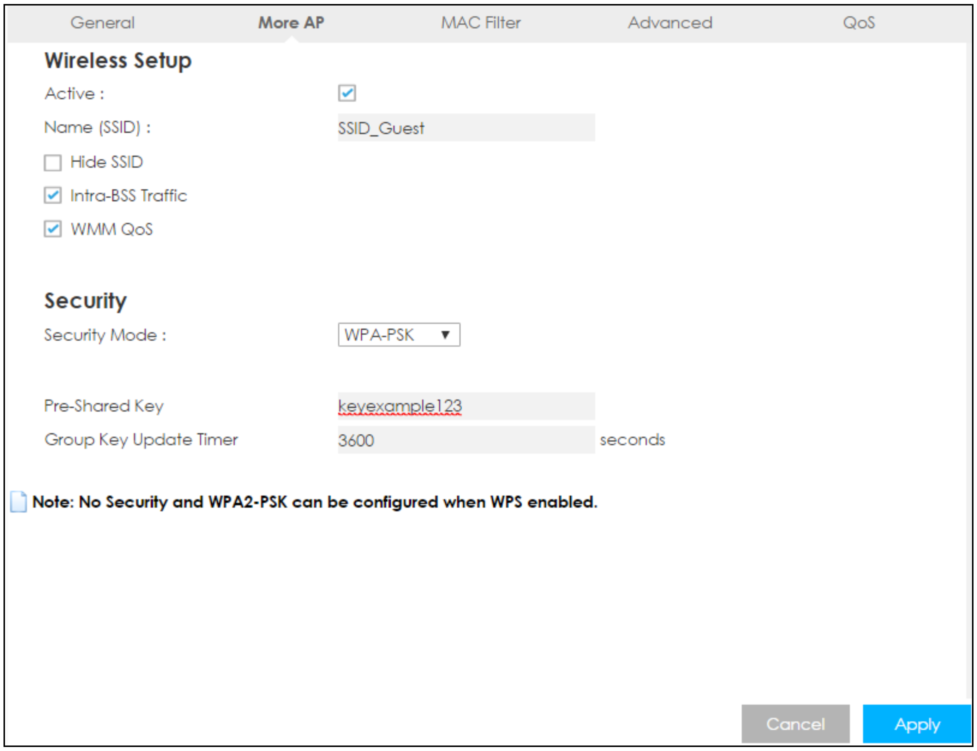
10 Click the **Edit** icon of the third entry to configure wireless and security settings for **SSID_Guest**.



More AP Setup

#	Status	SSID	Security	Edit
1		SSID_Worker	WPA2-PSK	
2		SSID_VoIP	WPA-PSK	
3		ZyXEL_SSID3	No Security	

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



Wireless Setup

Active : ☑

Name (SSID) : SSID_Guest

□ Hide SSID

☑ Intra-BSS Traffic

☑ WMM QoS

Security

Security Mode : WPA-PSK

Pre-Shared Key keyexample123

Group Key Update Timer 3600 seconds

Note: No Security and WPA2-PSK can be configured when WPS enabled.

4.5 Make an Internet Phone (Vo3G) Call on the LTE3312-M432

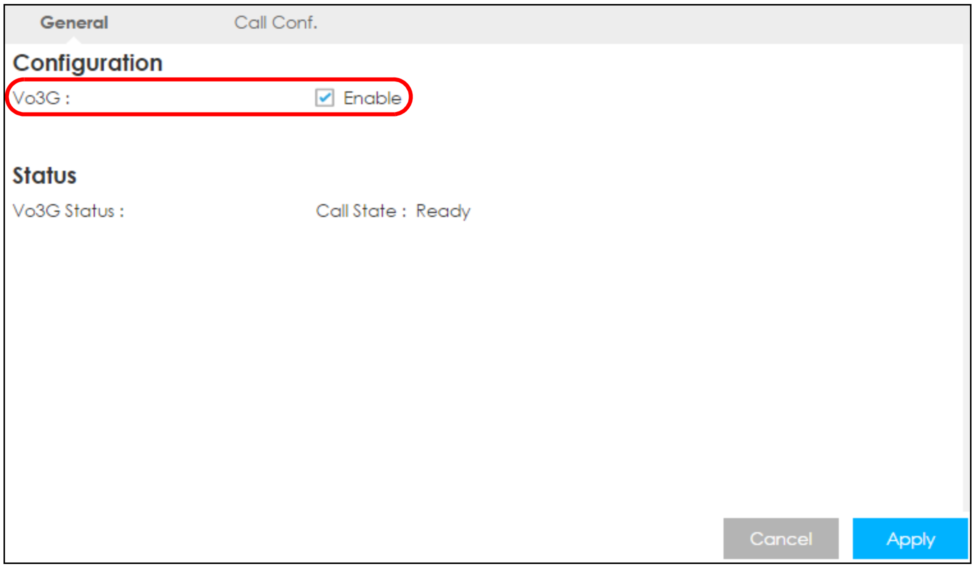
You can make phone calls over the Internet via the LTE3312-M432.

1 Make sure a SIM card is installed on the LTE3312-M432 to have Internet access.

2 Log into the Web Configurator.

3 Go to the **Configuration > Application > Voice over 3G > General** screen.

4 Select **Enable** in the **Vo3G** field to activate Voice over 3G on the LTE3312-M432. Click **Apply**.



Configuration

Vo3G : ☑ Enable

Status

Vo3G Status : Call State : Ready

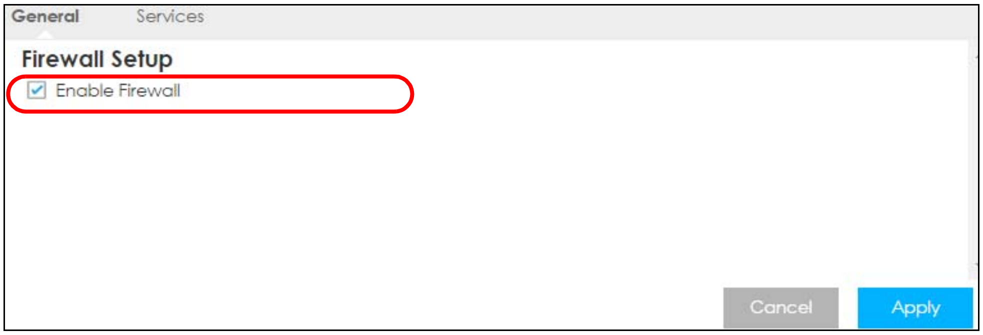
5 Connect an analog telephone to the **PHONE** port to make phone calls over the Internet.

4.6 Configure a Firewall Rule

You can enable the firewall to protect your LAN computers from malicious attacks from the Internet if you want to allow specific traffic in from the Internet.

1 Click **Configuration > Security > Firewall** to open the **General** screen.

2 Select the **Enable Firewall** check box to enable the firewall, and click **Apply**.



Firewall Setup

☑ Enable Firewall

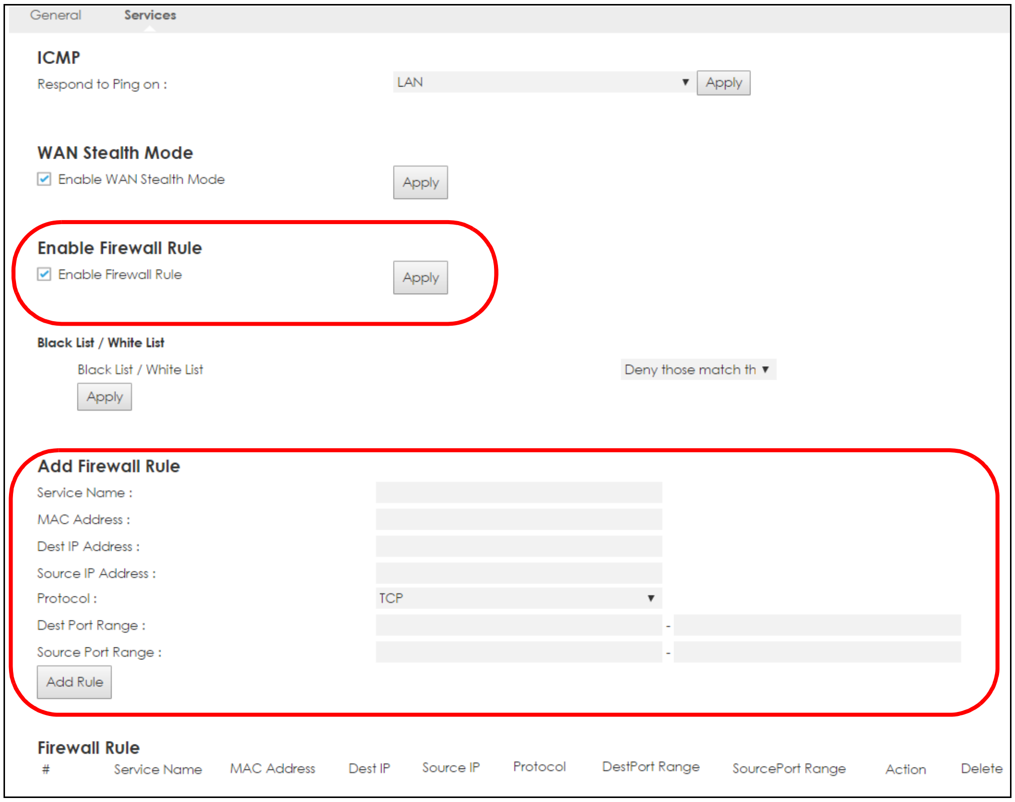
3 Open the **Services** screen to create a rule.

4 Go to the **Add Firewall Rule** section and set up a rule. Click **Add Rule**.

- **Service Name**: Enter a name to identify the firewall rule.
- **MAC Address**: Enter the MAC address of the computer.
- **Dest IP Address**: Enter the IP address of the computer to which traffic for the application or service is entering.
- **Source IP Address**: Enter the IP address of the computer that initializes traffic for the application or service.

- **Protocol**: Select the protocol (**TCP**, **UDP** or **ICMP**) used to transport the packets.
- **Dest Port Range**: Enter the port number/range of the destination that define the traffic type.
- **Source Port Range**: Enter the port number/range of the source that define the traffic type.

5 Select the **Enable Firewall Rule** check box to activate the rules you created, and click **Apply**.



ICMP

Respond to Ping on : LAN ▾ Apply

WAN Stealth Mode

☑ Enable WAN Stealth Mode

Apply

Enable Firewall Rule

☑ Enable Firewall Rule

Apply

Black List / White List

Black List / White List: Deny those match th ▾

Apply

Add Firewall Rule

Service Name :

MAC Address :

Dest IP Address :

Source IP Address :

Protocol : TCP ▾

Dest Port Range : -

Source Port Range : -

Add Rule

Firewall Rule

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

4.7 Configure Content Filtering

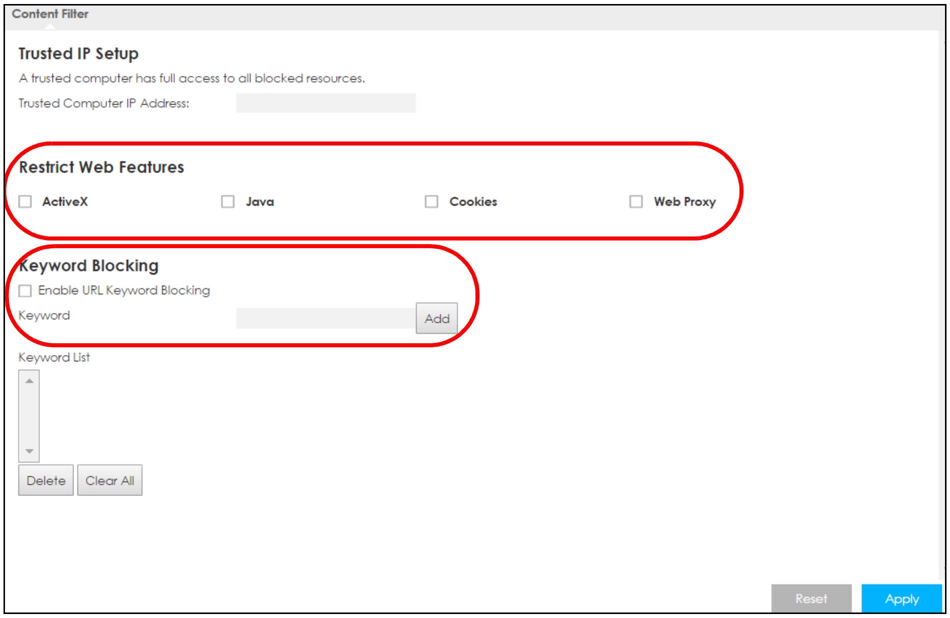
You can block certain web features and specific website addresses.

1 Go to the **Configuration > Security > Content Filter** screen.

2 Select a web feature that you want to block in the **Restrict Web Features** section.

3 Enter a keyword in the **Keyword** field to block web sites containing the keyword, and click **Add**.

4 Select the **Enable URL Keyword Blocking** check box. Click **Apply**.



Content Filter

Trusted IP Setup

A trusted computer has full access to all blocked resources.

Trusted Computer IP Address:

Restrict Web Features

□ ActiveX □ Java □ Cookies □ Web Proxy

Keyword Blocking

□ Enable URL Keyword Blocking

Keyword

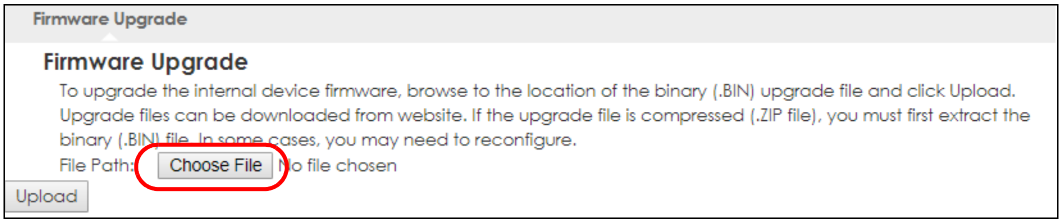
4.8 Upgrade Firmware on the LTE Device

Upload the router firmware to the LTE Device for feature enhancements.

1 Download the firmware file at www.zyxel.com in a compressed file. Decompress the file.

2 Go to the **Maintenance > Firmware Upgrade** screen.

3 Click **Choose File** and select the .bin file to upload. Click **Upload**.



Firmware Upgrade

Firmware Upgrade

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

File Path: Choose File No file chosen

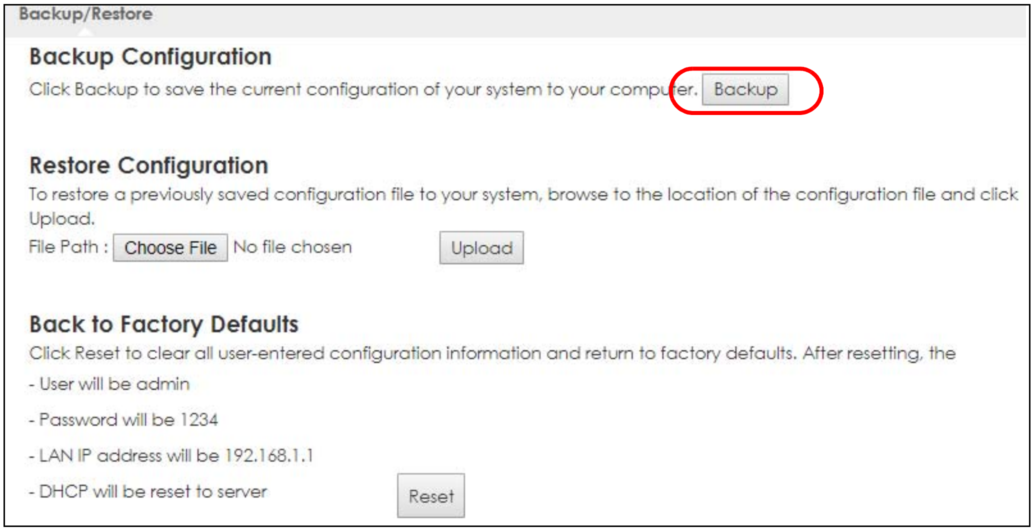
4 This process may take up to two minutes to finish. After two minutes, log in again and check your new firmware version in the **Status** screen.

4.9 Back up a Configuration File

Back up a configuration file in case you want to return to your previous settings.

1 Go to the **Maintenance > Backup/Restore** screen.

2 Click **Backup** in the **Backup Configuration** section, and a configuration file will be saved to your computer.



Backup/Restore

Backup Configuration

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

Restore Configuration

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.

File Path : Choose File No file chosen Upload

Back to Factory Defaults

Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the

- User will be admin
- Password will be 1234
- LAN IP address will be 192.168.1.1
- DHCP will be reset to server

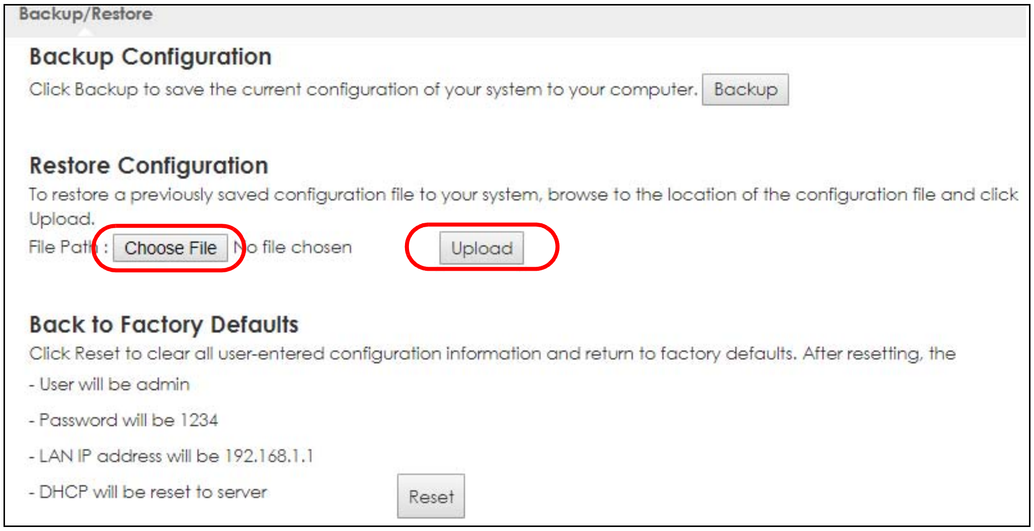
Reset

4.10 Restore Previous Configuration

You can upload a previously saved configuration file from your computer to your LTE Device to restore that previous configuration.

1 Go to the **Maintenance > Backup/Restore** screen.

2 Click **Choose File** in the **Restore Configuration** section, and select the configuration file that you want to upload. Click **Upload**.



Backup/Restore

Backup Configuration

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

Restore Configuration

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.

File Path : Choose File No file chosen Upload

Back to Factory Defaults

Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the

- User will be admin
- Password will be 1234
- LAN IP address will be 192.168.1.1
- DHCP will be reset to server

Reset

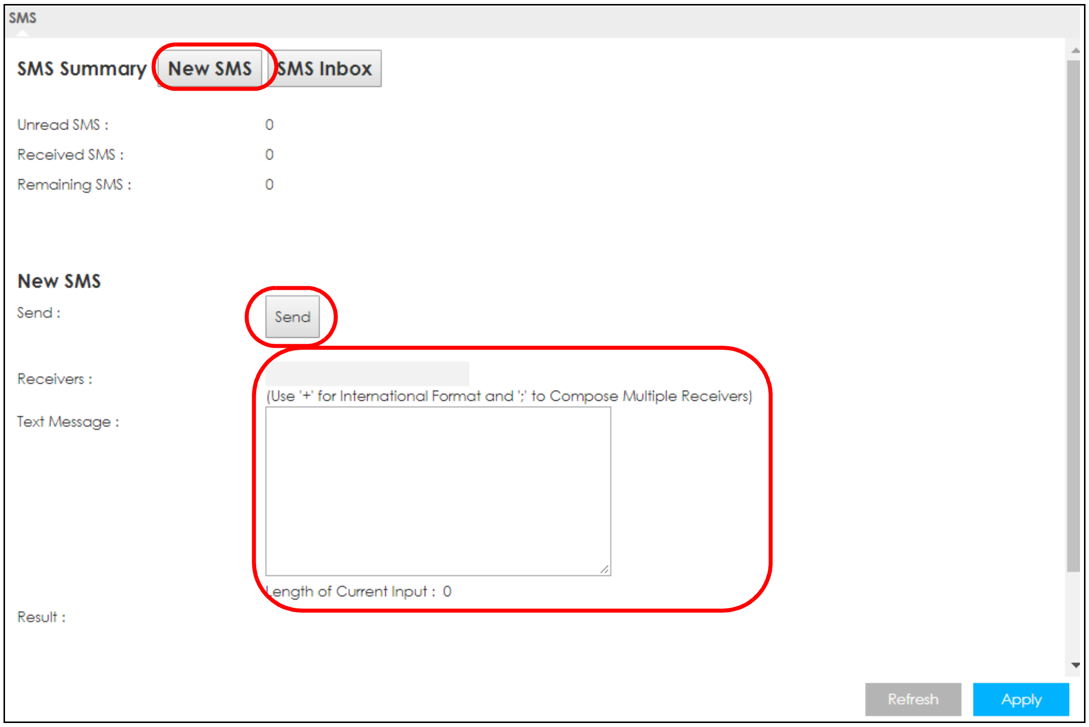
3 The LTE Device will restart automatically after the configuration file is successfully uploaded. Wait for one minute before logging into the LTE Device again.

4.11 Send a New SMS Text Message

You can send SMS text messages through the LTE Device.

1 Go to the **Configuration > Application > SMS** screen.

2 Click the **New SMS** button. Enter a cell phone number to which you want to send a text message in the **Receivers** field. Enter the text message content in the **Text Message** field, and click the **Send** button.



SMS

SMS Summary | New SMS | SMS Inbox

Unread SMS : 0

Received SMS : 0

Remaining SMS : 0

New SMS

Send : Send

Receivers :

(Use '+' for International Format and ';' to Compose Multiple Receivers)

Text Message :

Length of Current Input : 0

Result :

PART II

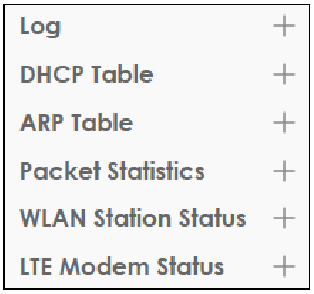
Technical Reference

CHAPTER 5
Monitor

5.1 Overview

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

To access the Monitor screens, click Monitor after login.



Log +

DHCP Table +

ARP Table +

Packet Statistics +

WLAN Station Status +

LTE Modem Status +

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

5.2 What You Can Do

- Use the **Log** screen to see the logs for the activity on the LTE Device (Section 5.3 on page 50).
- Use the **DHCP Table** screen to view information related to your DHCP status (Section 5.4 on page 51).
- Use the **ARP Table** screen to view the mappings of IP and MAC addresses. (Section 5.5 on page 53).
- use the **Packet Statistics** screen to view port status, packet specific statistics, the "system up time" and so on (Section 5.6 on page 53).
- Use the **WLAN Station Status** screen to view the wireless stations that are currently associated to the LTE Device (Section 5.7 on page 54).
- 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 55).

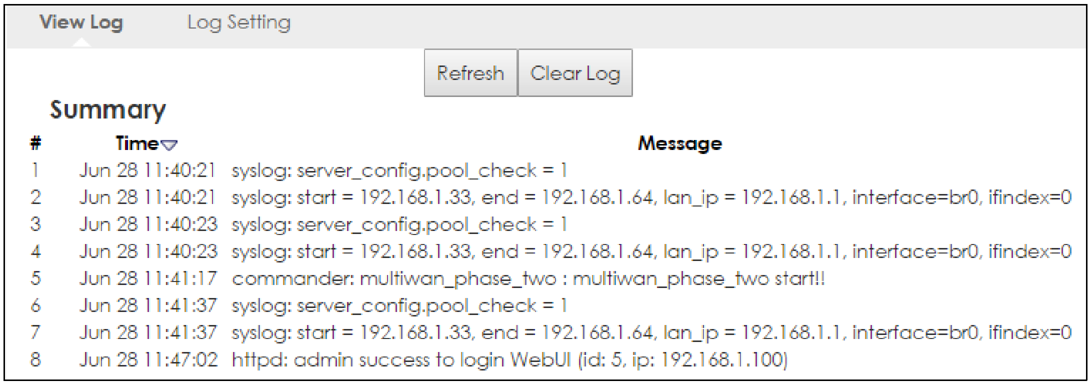
5.3 The Log Screen

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

5.3.1 View Log

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

Figure 26 View Log

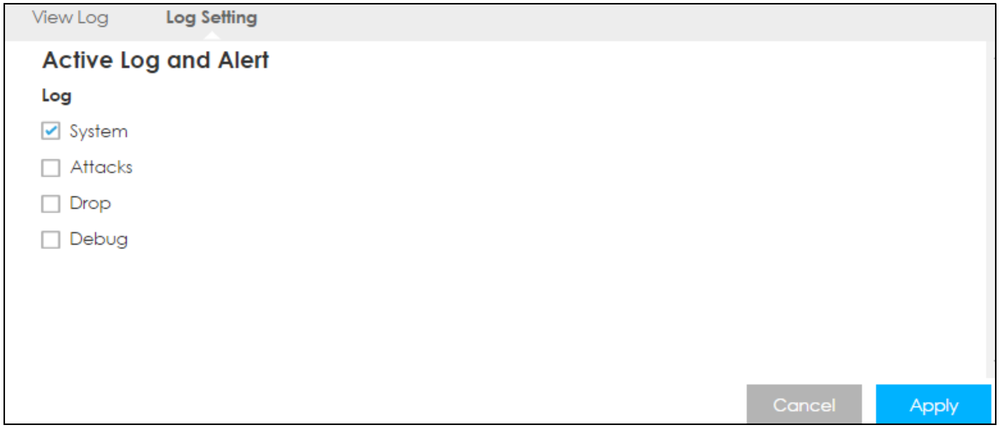


Summary

#	Time▽	Message
1	Jun 28 11:40:21	syslog: server_config.pool_check = 1
2	Jun 28 11:40:21	syslog: start = 192.168.1.33, end = 192.168.1.64, lan_ip = 192.168.1.1, interface=br0, ifindex=0
3	Jun 28 11:40:23	syslog: server_config.pool_check = 1
4	Jun 28 11:40:23	syslog: start = 192.168.1.33, end = 192.168.1.64, lan_ip = 192.168.1.1, interface=br0, ifindex=0
5	Jun 28 11:41:17	commander: multiwan_phase_two : multiwan_phase_two start!!
6	Jun 28 11:41:37	syslog: server_config.pool_check = 1
7	Jun 28 11:41:37	syslog: start = 192.168.1.33, end = 192.168.1.64, lan_ip = 192.168.1.1, interface=br0, ifindex=0
8	Jun 28 11:47:02	httpd: admin success to login WebUI (id: 5, ip: 192.168.1.100)

You can configure which logs to display in the **View Log** screen. Go to the **Log Setting** screen and select the logs you wish to display. Click **Apply** to save your settings. Click **Cancel** to start the screen afresh.

Figure 27 Log Settings



Active Log and Alert

Log

☑ System

☐ Attacks

☐ Drop

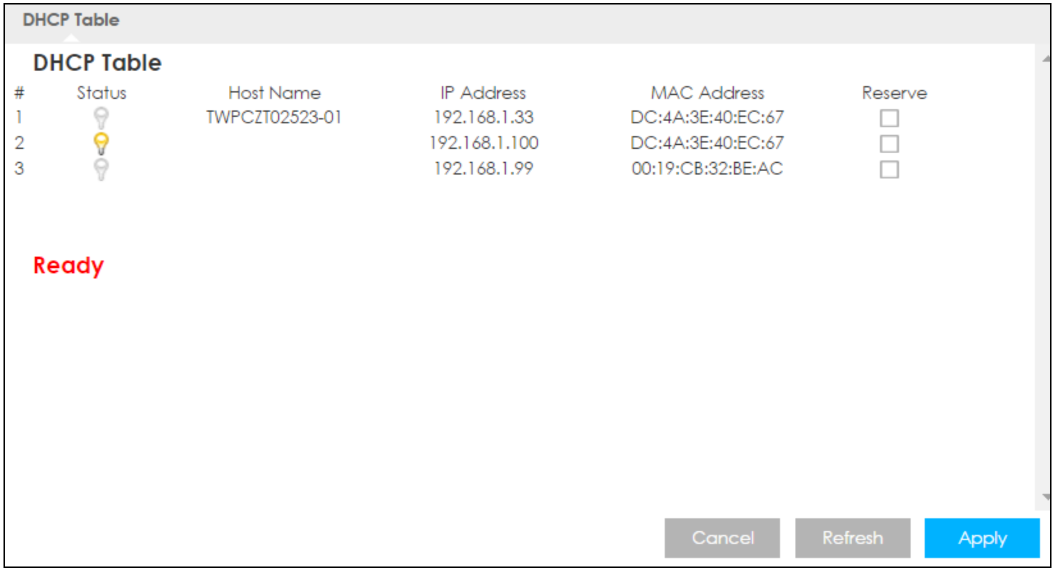
☐ Debug

5.4 DHCP Table

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the LTE Device's LAN as a DHCP server or disable it. When configured as a server, the LTE Device 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** or **Configuration > Network > DHCP Server > Client List**. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP client information (including **MAC Address**, and **IP Address**) of all network clients using the LTE Device's DHCP server.

Figure 28 Monitor > DHCP Table



DHCP Table

DHCP Table

#	Status	Host Name	IP Address	MAC Address	Reserve
1	○	TWPCZT02523-01	192.168.1.33	DC:4A:3E:40:EC:67	□
2	●		192.168.1.100	DC:4A:3E:40:EC:67	□
3	○		192.168.1.99	00:19:CB:32:BE:AC	□

Ready

The following table describes the labels in this screen.

Table 10 Monitor > DHCP Table

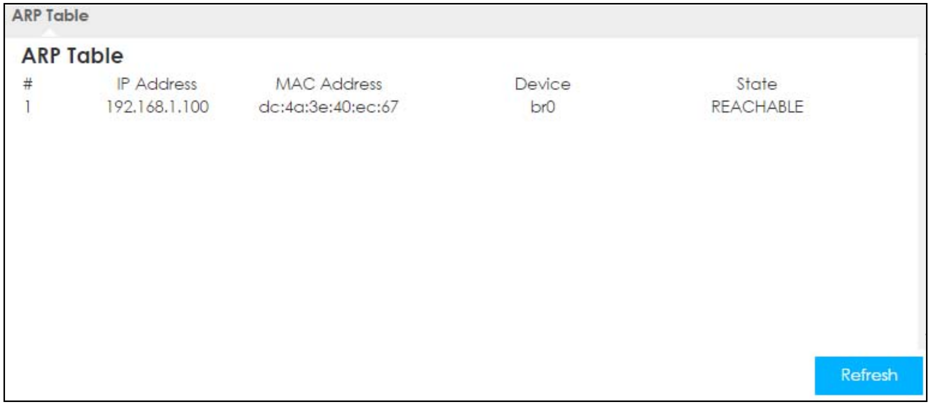
LABEL	DESCRIPTION
#	This is the index number of the host computer.
Status	This field displays whether the connection to the host computer is up (a yellow bulb) or down (a gray bulb).
Host Name	This field displays the computer host name.
IP Address	This field displays the IP address relative to the #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

5.5 ARP Table

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

Use the ARP table to view IP-to-MAC address mapping(s).

Figure 29 Monitor > ARP Table



ARP Table

#	IP Address	MAC Address	Device	State
1	192.168.1.100	dc:4a:3e:40:ec:67	br0	REACHABLE

The following table describes the labels in this screen.

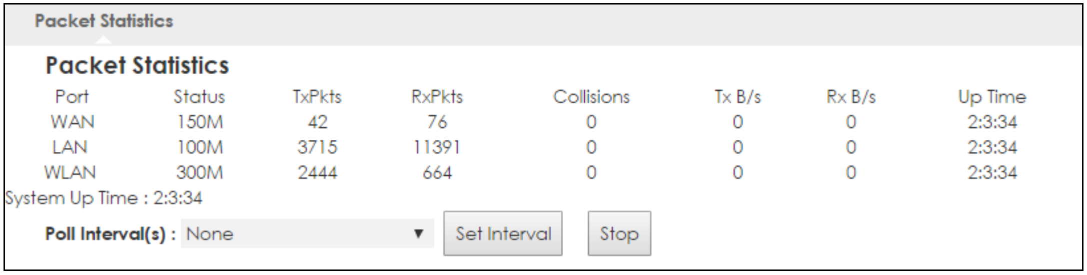
Table 11 System Monitor > ARP Table

LABEL	DESCRIPTION
#	This is the ARP table entry number.
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. **br0** indicates a LAN interface where 0 represents LAN1 or LAN2.
State	This column shows the status of the mapping.
Refresh	Click **Refresh** to update this screen.

5.6 Packet Statistics

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

Figure 30 Monitor > Packet Statistics



Packet Statistics

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	150M	42	76	0	0	0	2:3:34
LAN	100M	3715	11391	0	0	0	2:3:34
WLAN	300M	2444	664	0	0	0	2:3:34

System Up Time : 2:3:34

Poll Interval(s) : None

The following table describes the labels in this screen.

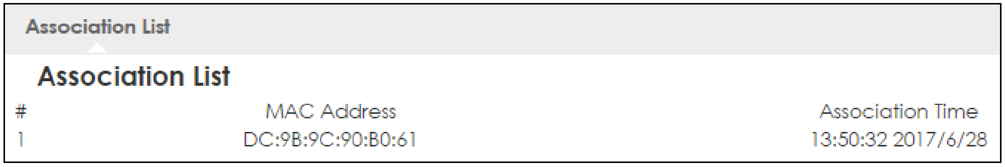
Table 12 Monitor > Packet Statistics

LABEL	DESCRIPTION
Port	This is the LTE Device'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 LTE Device 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/s	This displays the reception speed in bytes per second on this port.
Up Time	This is the total time the LTE Device has been for each session.
System Up Time	This is the total time the LTE Device has been on.
Poll Interval(s)	Enter the time interval in seconds for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the **Poll Interval(s)** field.
Stop	Click **Stop** to stop refreshing statistics.

5.7 WLAN Station Status

Click **Monitor > WLAN Station Status** or the **WLAN Station Status (Details...)** hyperlink in the **Status** screen. View the wireless stations that are currently associated to the LTE Device'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.

Figure 31 Monitor > WLAN Station Status



Association List

#	MAC Address	Association Time
1	DC:9B:9C:90:B0:61	13:50:32 2017/6/28

The following table describes the labels in this screen.

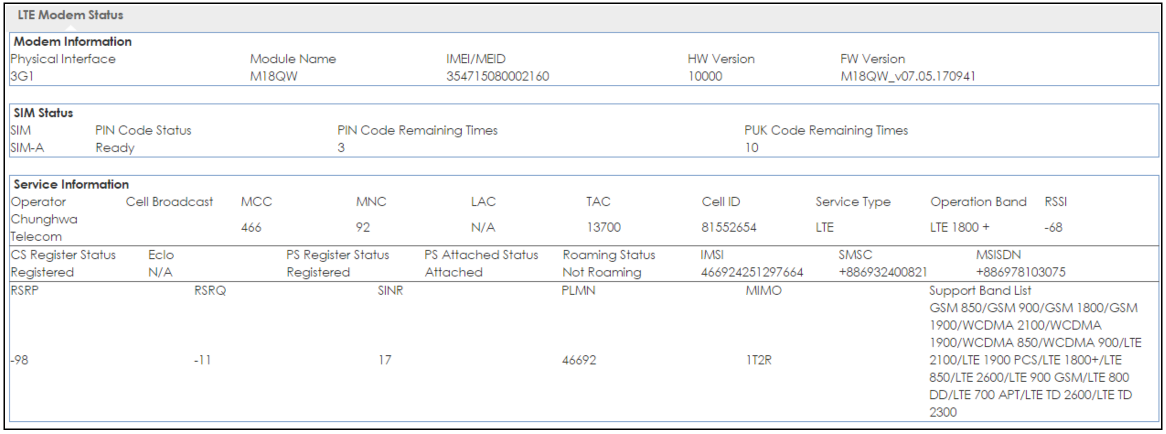
Table 13 Monitor > WLAN Station Status

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

5.8 LTE Modem Status

Click **Monitor > LTE Modem Status** or the **LTE Modem Status (Details...)** hyperlink in the **Status** screen. Use this screen to view the detailed information about the modem, SIM card status, and details. You can also check the LTE connection status.

Figure 32 Monitor > LTE Modem Status



LTE Modem Status

Modem Information

Physical Interface	Module Name	IMEI/MEID	HW Version	FW Version
3G1	M18QW	354715080002160	10000	M18QW_v07.05.170941

SIM Status

SIM	PIN Code Status	PIN Code Remaining Times	PUK Code Remaining Times
SIM-A	Ready	3	10

Service Information

Operator	Cell Broadcast	MCC	MNC	LAC	TAC	Cell ID	Service Type	Operation Band	RSSI
Chunghwa Telecom		466	92	N/A	13700	81552654	LTE	LTE 1800 +	-68

CS Register Status	Eclo	PS Register Status	PS Attached Status	Roaming Status	IMSI	SMSC	MSISDN
Registered	N/A	Registered	Attached	Not Roaming	466924251297664	+886932400821	+886978103075

RSRP	RSRQ	SINR	PLMN	MIMO	Support Band List
-98	-11	17	46692	1T2R	GSM 850/GSM 900/GSM 1800/GSM 1900/WCDMA 2100/WCDMA 1900/WCDMA 850/WCDMA 900/LTE 2100/LTE 1900 PCS/LTE 1800+/LTE 850/LTE 2600/LTE 900 GSM/LTE 800 DD/LTE 700 APT/LTE TD 2600/LTE TD 2300

The following table describes the labels in this screen.

Table 14 Monitor > LTE Modem Status

LABEL	DESCRIPTION
Modem Information	
Physical Interface	This displays the interface used for the mobile data connection.
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.

Table 14 Monitor > LTE Modem Status (continued)

LABEL	DESCRIPTION
Service Information	
Operator	This displays the name of the service provider.
Cell Broadcast	This displays whether the one-to-many messaging service is available.
MCC	This displays the Mobile Country Code (MCC), which is used to identify the country of a mobile subscriber.
MNC	This displays the Mobile Network Code (MNC), which is used in combination with MCC to identify the public land mobile network (PLMN) of a mobile subscriber.
LAC	This displays the 2-octet Location Area Code (LAC), which is used to identify a location area within a PLMN.
TAC	This displays the Tracking Area Code (TAC), which is to identify a tracking area within a PLMN.
~~Physical~~ Cell ID	This displays the ID of a cell at the physical layer.
Service Type	This displays the type of the mobile network to which the LTE Device is connecting.
Operation Band	This displays the network type and the frequency band used by the mobile network to which the LTE Device is connecting.
RSSI	This displays the received signal strength indicator (RSSI), that is, the received signal strength in dBm.
CS Register Status	This displays the Circuit Switched network registration status.
EcIo	This displays the ratio (in dB) of the received energy per chip and the interference level.
PS Register Status	This displays the packet switched network registration status.
PS Attached Status	This displays the Packet switched Domain Attachment status.
Roaming Status	This displays whether the LTE Device 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 LTE Device, such as 1T2R (1 Transmit and 2 Receive paths/antennas) or TM1-TM4 (Transmission Mode 4).
Support Band List	This displays the frequency bands that are supported by the LTE Device.

CHAPTER 6
WAN

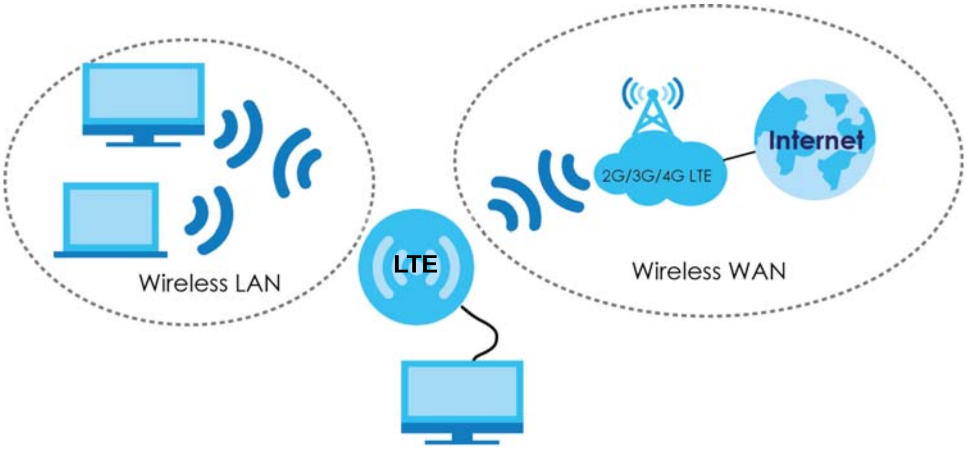
6.1 Overview

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

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

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

Figure 33 LAN/Wireless LAN and Wireless WAN



6.2 What You Can Do

- Use the **Management WAN** screen to configure 3G/4G WAN connection settings (Section 6.4 on page 60).
- Use the **Network Scan** screen to specify the type of the mobile network to which the LTE Device is connected and how you want the LTE Device to connect to an available mobile network (Section 6.5 on page 64).
- Use the **IPv6** screen to configure the LTE Device's IPv6 settings (Section 6.6 on page 66).
- Use the **PIN Management** screen to configure the LTE Device's PIN settings (Section 6.7 on page 67).

6.3 What You Need To Know

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

3G

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

4G

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

DNS Server Address Assignment

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

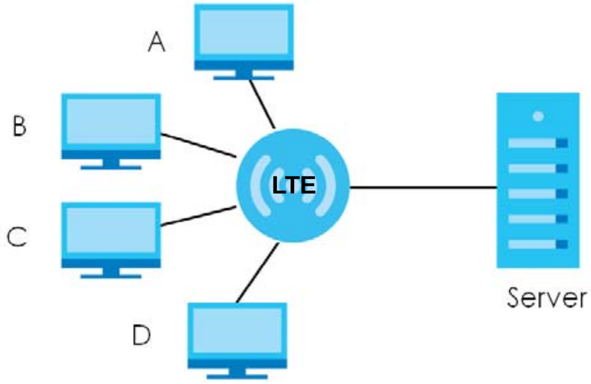
The LTE Device can get the DNS server addresses in the following ways.

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

Multicast

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

Figure 34 Multicast Example



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

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

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

IPv6 Introduction

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

IPv6 Addressing

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

IPv6 addresses can be abbreviated in two ways:

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

IPv6 Prefix and Prefix Length

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

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

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

IPv6 Subnet Masking

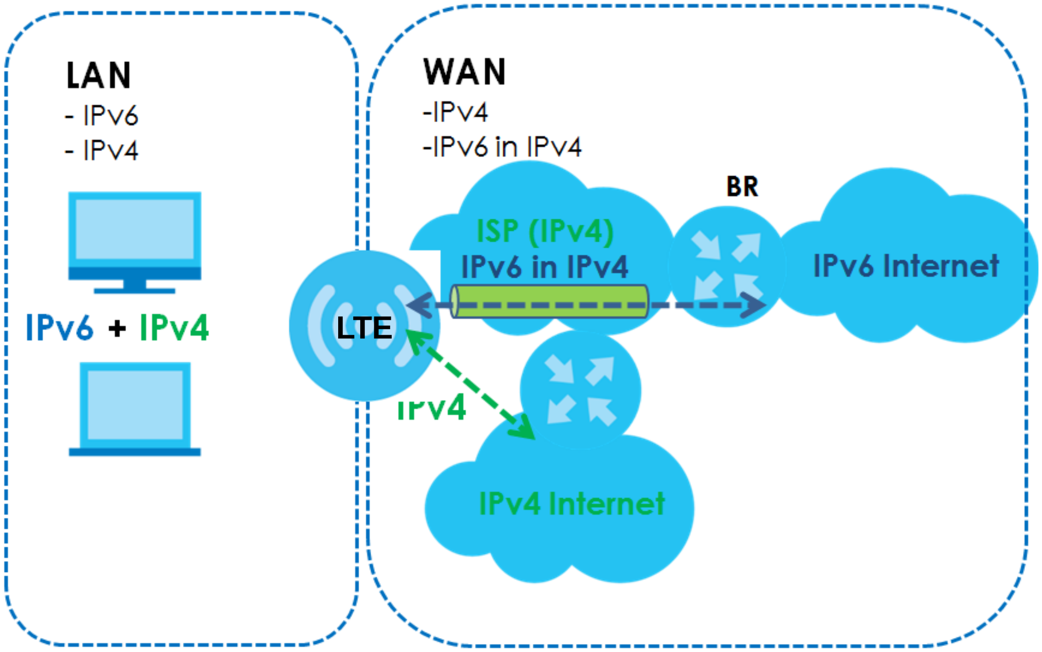
Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block’s 16 bits are then represented by four hexadecimal characters. For example,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

IPv6 Rapid Deployment

Use IPv6 Rapid Deployment (6rd) when the local network uses IPv6 and the ISP has an IPv4 network. When the LTE Device has an IPv4 WAN address, you can enable 6rd to encapsulate IPv6 packets in IPv4 packets to cross the ISP's IPv4 network.

The LTE Device generates a global IPv6 prefix from its IPv4 WAN address and tunnels IPv6 traffic to the ISP's Border Relay router (**BR** in the figure) to connect to the native IPv6 Internet. The local network can also use IPv4 services. The LTE Device uses it's configured IPv4 WAN IP to route IPv4 traffic to the IPv4 Internet.

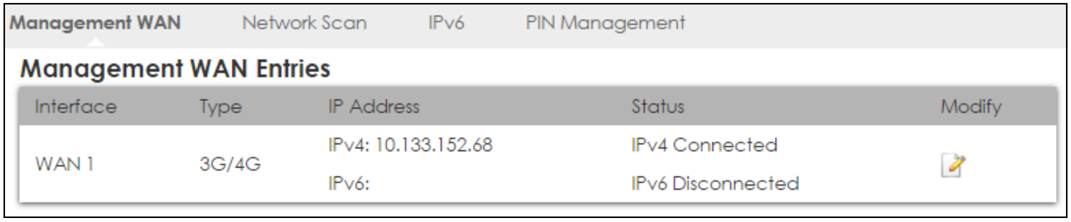
Figure 35 IPv6 Rapid Deployment



6.4 Management WAN

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

Figure 36 Configuration > Network > WAN > Management WAN



Management WAN Entries

Interface	Type	IP Address	Status	Modify
WAN 1	3G/4G	IPv4: 10.133.152.68 IPv6:	IPv4 Connected IPv6 Disconnected	📝

The following table describes the labels in this screen.

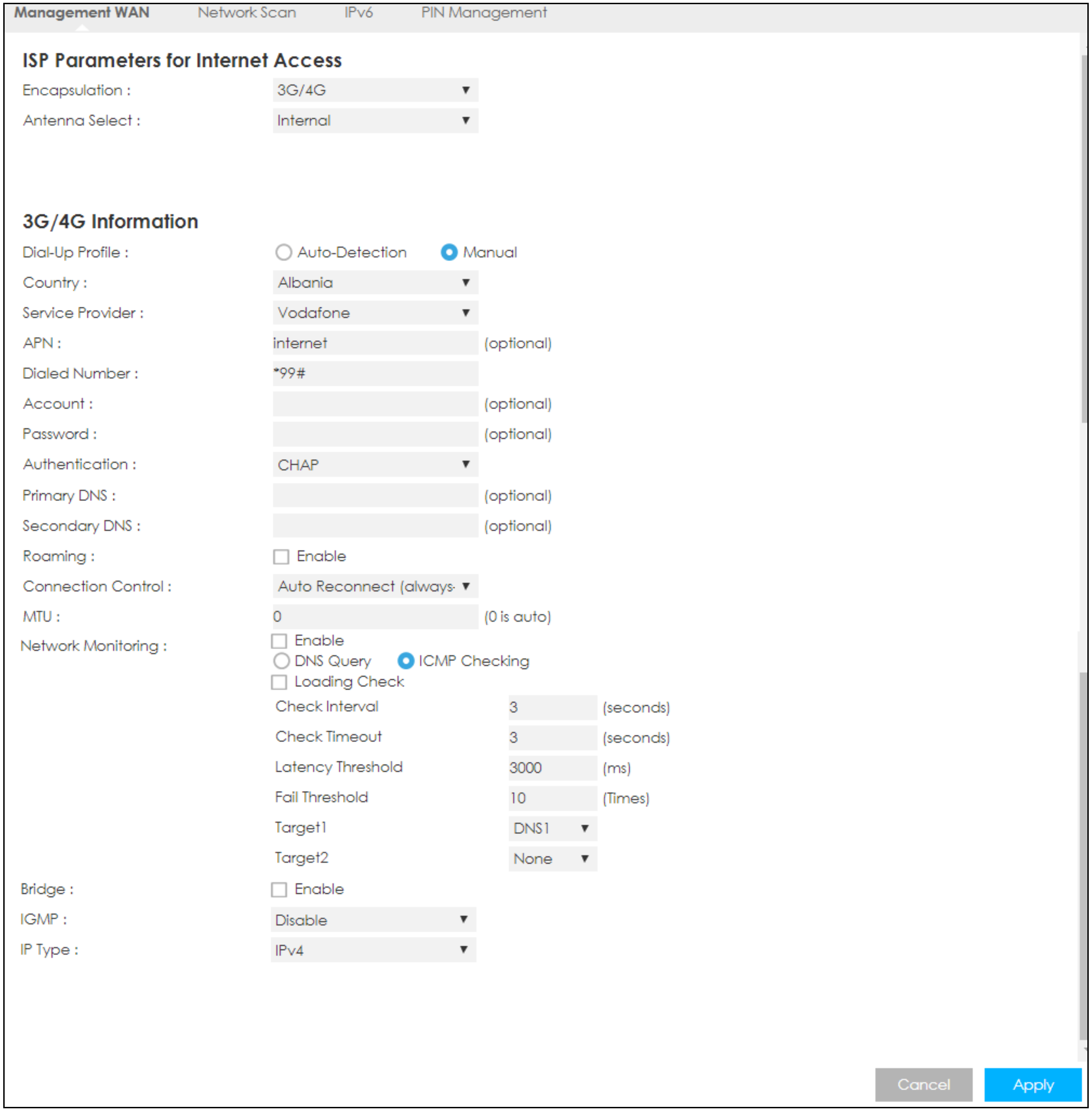
Table 15 Configuration > Network > WAN > Management WAN

LABEL	DESCRIPTION
Interface	This field displays the name of the WAN interface for this connection.
Type	This field displays the type of the WAN connection.
IP Address	This field displays the IPv4 and IPv6 addresses of the WAN connection.
Status	This field indicates whether the IPv4 and IPv6 connectivity is available.
Modify	Click the Edit icon to configure the WAN connection settings.

6.4.1 Management WAN Edit

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

Figure 37 Configuration > Network > WAN > Management WAN Edit



ISP Parameters for Internet Access

Encapsulation :	3G/4G ▼	
Antenna Select :	Internal ▼	

3G/4G Information

Dial-Up Profile :	○ Auto-Detection ● Manual	
Country :	Albania ▼	
Service Provider :	Vodafone ▼	
APN :	internet	(optional)
Dialed Number :	*99#	
Account :		(optional)
Password :		(optional)
Authentication :	CHAP ▼	
Primary DNS :		(optional)
Secondary DNS :		(optional)
Roaming :	□ Enable	
Connection Control :	Auto Reconnect (always- ▼	
MTU :	0	(0 is auto)
Network Monitoring :	□ Enable ○ DNS Query ● ICMP Checking □ Loading Check	
	Check Interval	3 (seconds)
	Check Timeout	3 (seconds)
	Latency Threshold	3000 (ms)
	Fail Threshold	10 (Times)
	Target1	DNS1 ▼
	Target2	None ▼
Bridge :	□ Enable	
IGMP :	Disable ▼	
IP Type :	IPv4 ▼	

The following table describes the labels in this screen.

Table 16 Configuration > Network > WAN > Management WAN Edit

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	This shows the WAN connection type.
Antenna Select	Select **Auto** to have the LTE Device select the default antennas for you. See the Introduction chapter for more information. Select **External** to have the external antennas work as default for signal transmission. Select **Internal** to have the internal antennas work as default for signal transmission.
3G/4G Information	

Table 16 Configuration > Network > WAN > Management WAN Edit (continued)

LABEL	DESCRIPTION
Dial-Up Profile	Select **Auto-Detection** to have the LTE Device use the inserted SIM card's default settings to connect to any available mobile network. Select **Manual** and enter the information provided by your service provider to connect to the service provider's mobile network.
Country	Select the country in which you use the LTE Device.
Service Provider	Select the name of your service provider. The options vary depending on the country you selected. If your service provider is not in the list, select **Others**.
APN	Connections with different APNs (Access Point Names) may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charge method. The corresponding APN automatically displays when you select a pre-defined service provider. If you select **Others** in the **Service Provider** field, manually enter the APN provided by your service provider. You can enter up to 32 ASCII printable characters. Spaces are allowed.
Dialed Number	This is the phone number (dial string) used to dial up a connection to your service provider's base station. Your service provider should provide the phone number. For example, *99# is the dial string to establish a GPRS or 3G/4G connection in Taiwan. The corresponding phone number automatically displays when you select a pre-defined service provider. If you select **Others** in the **Service Provider** field, manually enter the phone number provided by your service provider.
Account	Type the user name (of up to 64 ASCII printable characters) given to you by your service provider.
Password	Type the password (of up to 64 ASCII printable characters) associated with the user name above.
Authentication	The LTE Device 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 (**PAP**, or **CHAP**) used by the service provider. Otherwise, select **Auto** to have the LTE Device accept either CHAP or PAP.
Primary DNS	Enter the first DNS server address assigned by the service provider.
Secondary DNS	Enter the second DNS server address assigned by the service provider.
Roaming	3G/4G roaming is to use your mobile device in an area which is not covered by your service provider. Enable roaming to ensure that your LTE Device 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 Reconnect (always-on)** if you do not want the connection to time out. Select **Connect-on-Demand** if you do not want the connection up all the time and specify an idle time-out in the **Maximum Idle Time** field.
Maximum Idle Time	Specify the time in minutes that elapses before the LTE Device automatically disconnects from the service provider.
MTU	Enter the MTU (Maximum Transmission Unit) of each data packet, in bytes, that can move through the WAN connection.
Network Monitoring	Select this option to have the LTE Device test the WAN connection by periodically sending **DNS Query** to a DNS server or sending a ping (**ICMP Checking**) to either the default gateway or the addresses you specify in the **Target1** and **Target2** fields.
Loading Check	Select this option to check how many packets have been transmitted or received through the WAN connection within a time period specified in the **Check Interval** field.

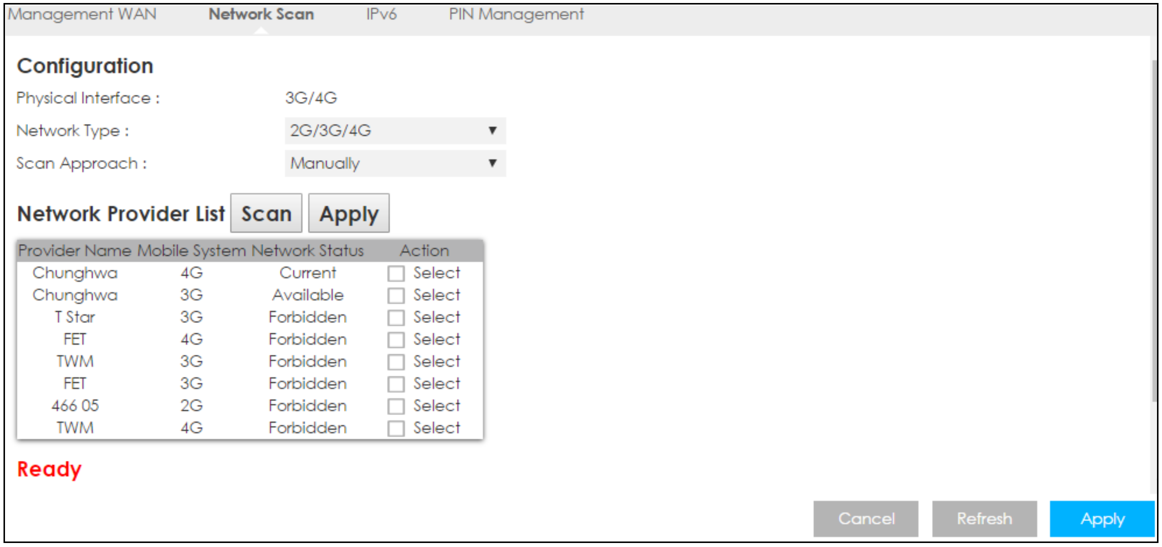
Table 16   Configuration > Network > WAN > Management WAN Edit (continued)

LABEL	DESCRIPTION
Check Interval	Type a number of seconds (0 to 99999) to set the time interval between checks. Allow more time if your destination IP address handles lots of traffic.
Check Timeout	Type the number of seconds (0 to 99999) for your LTE Device to wait for a response to the ping or DNS query before considering the check to have failed. This setting must be less than the **Check Interval**. Use a higher value in this field if your network is busy or congested.
Latency Threshold	Type a number of milliseconds (0 to 99999) for the latency threshold. If the specified latency threshold is exceeded, the LTE Device considers the check to have failed and makes a new connection after (Latency Threshold * Fail Threshold) seconds.
Fail Threshold	Type how many WAN connection checks can fail (0 to 99999) before the connection is considered "down" (not connected). The LTE Device still checks a "down" connection to detect if it reconnects.
Target1/Target2	Select **DNS1** to have the LTE Device send a DNS query to the first DNS server address assigned by the service provider. Select **DNS2** to have the LTE Device send a DNS query to the second DNS server address assigned by the service provider. Select **Gateway** to have the LTE Device ping the WAN interface's default gateway IP address. Select **Other Host** and enter a domain name or IP address of a reliable nearby computer to have the LTE Device ping that address.
Bridge	Select this check box to change the LTE Device's operating mode to **Bridge mode**. The computer connected to the first Ethernet LAN port is allowed to get an individual IP address from the ISP's DHCP server directly.
IGMP	Select **IGMP v1**, **IGMP v2**, **IGMP v3** or **Auto** to enable multicasting. This applies to traffic routed from the WAN to the LAN. Select **Disable** to turn off this feature. This may cause incoming traffic to be dropped or sent to all connected network devices.
IGMP Proxy	This field is available only when IGMP is enabled. Select this option to have the LTE Device act as an IGMP proxy on this connection. This allows the LTE Device to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
IP Type	Select **IPv4** if you want the LTE Device to run IPv4 only. Select **IPv4/IPv6** to allow the LTE Device to run IPv4 and IPv6 at the same time. Select **IPv6** if you want the LTE Device to run IPv6 only.

6.5 Network Scan

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

Figure 38 Configuration > Network > WAN > Network Scan



Configuration

Physical Interface : 3G/4G

Network Type : 2G/3G/4G

Scan Approach : Manually

Network Provider List Scan Apply

Provider Name	Mobile System	Network Status	Action
Chunghwa	4G	Current	□ Select
Chunghwa	3G	Available	□ Select
T Star	3G	Forbidden	□ Select
FET	4G	Forbidden	□ Select
TWM	3G	Forbidden	□ Select
FET	3G	Forbidden	□ Select
466 05	2G	Forbidden	□ Select
TWM	4G	Forbidden	□ Select

Ready

The following table describes the labels in this screen.

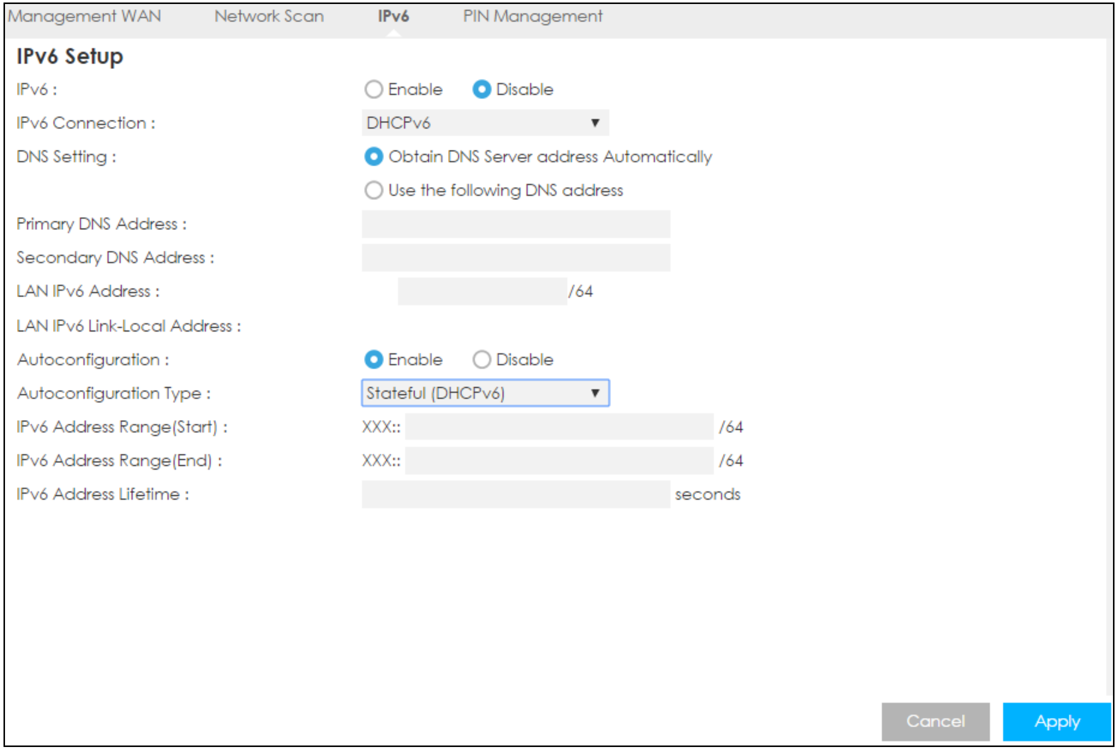
Table 17 Configuration > Network > WAN > Network Scan

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

6.6 IPv6

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

Figure 39 Configuration > Network > WAN > IPv6



IPv6 Setup

IPv6 : ○ Enable ● Disable

IPv6 Connection : DHCPv6 ▾

DNS Setting : ● Obtain DNS Server address Automatically

○ Use the following DNS address

Primary DNS Address :

Secondary DNS Address :

LAN IPv6 Address : /64

LAN IPv6 Link-Local Address :

Autoconfiguration : ● Enable ○ Disable

Autoconfiguration Type : Stateful (DHCPv6) ▾

IPv6 Address Range(Start) : XXX:: /64

IPv6 Address Range(End) : XXX:: /64

IPv6 Address Lifetime : seconds

The following table describes the labels in this screen.

Table 18 Configuration > Network > WAN > IPv6

LABEL	DESCRIPTION
IPv6	Select **Enable** to allow the LTE Device to run IPv6. Otherwise, select **Disable**.
IPv6 Connection	Select **DHCPv6** if you want to obtain an IPv6 address from a DHCPv6 server.
DNS Setting	Select **Obtain DNS Server address Automatically** to have the LTE Device get the IPv6 DNS server addresses from the ISP automatically. Select **Use the following DNS address** to have the LTE Device use the IPv6 DNS server addresses you configure manually.
Primary DNS Address	Enter the first IPv6 DNS server address assigned by the ISP.
Secondary DNS Address	Enter the second IPv6 DNS server address assigned by the ISP.
LAN IPv6 Address	Enter the IPv6 address for the LTE Device LAN interface in this field.
LAN IPv6 Link-Local Address	This shows the IPv6 Link-local address in the LAN side. This is used by LTE Device when communicating with neighboring devices on the same link. It allows IPv6-capable devices to communicate with each other in the LAN side.i
Autoconfiguration	Click **Enable** if you want the devices on your local area network to obtain network address that are not managed by a DHCPv6 server. Otherwise, select **Disable**.

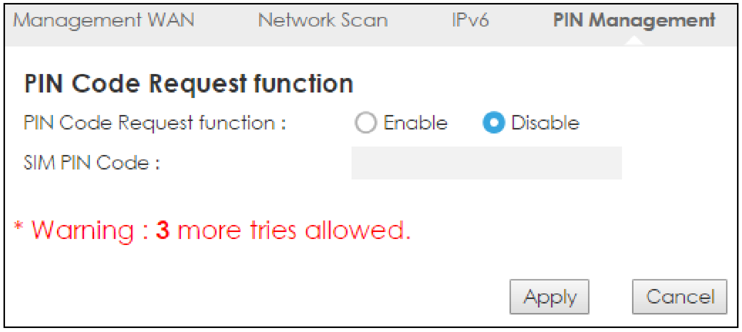
Table 18 Configuration > Network > WAN > IPv6 (continued)

LABEL	DESCRIPTION
Autoconfiguration Type	Select **Stateless** if you want the LTE Device interface to automatically generate a link-local address via stateless autoconfiguration. Select **Stateful (DHCPv6)** when the devices connected to your LAN needs to have their TCP/IP configuration set to DHCPv6 or obtain an IPv6 address automatically.
IPv6 Address Range(Start)	If you select **Stateful (DHCPv6)**, specify the range of IPv6 addresses from which the DHCPv6 server assigns to the clients. Enter the smallest value of the last block of the IPv6 addresses which are to be allocated.
IPv6 Address Range(End)	If you select **Stateful (DHCPv6)**, specify the range of IPv6 addresses from which the DHCPv6 server assigns to the clients. Enter the largest value of the last block of the IPv6 addresses which are to be allocated.
IPv6 Address Lifetime	If you select **Stateful (DHCPv6)**, specify how long (in minutes) the IPv6 addresses remain valid.
Cancel	Click **Cancel** to reload the previous configuration for this screen.
Apply	Click **Apply** to save your changes back to the LTE Device.

6.7 PIN Management

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

Figure 40 Configuration > Network > WAN > PIN Management



PIN Code Request function

PIN Code Request function : ○ Enable ● Disable

SIM PIN Code :

* Warning : **3** more tries allowed.

The following table describes the labels in this screen.

Table 19 Configuration > Network > WAN > PIN Management

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

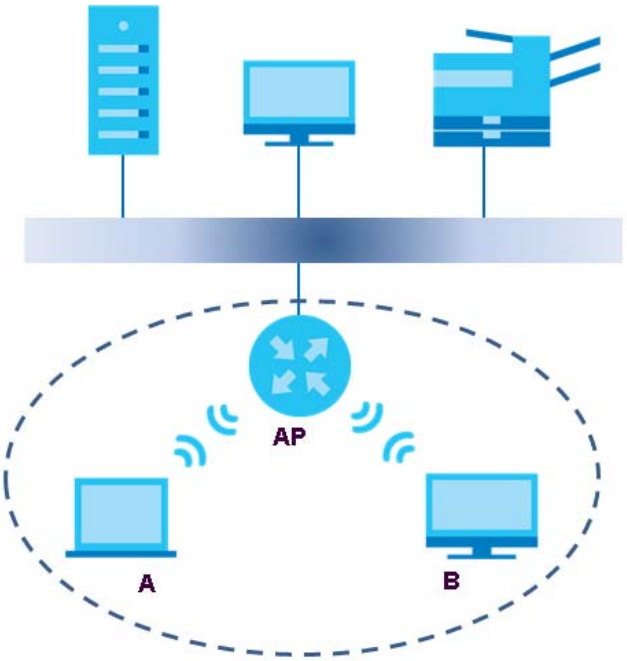
CHAPTER 7
Wireless LAN

7.1 Overview

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

The following figure provides an example of a wireless network.

Figure 41 Example of a Wireless Network



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

7.1.1 What You Can Do

- Use the **General** screen to turn the wireless connection on or off, set up wireless security between the LTE Device and the wireless clients, and make other basic configuration changes (Section 7.2 on page 71).
- Use the **More AP** screen to set up multiple wireless networks on your LTE Device (Section 7.4 on page 78).
- Use the **MAC Filter** screen to allow or deny wireless stations based on their MAC addresses from connecting to the LTE Device (Section 7.5 on page 80).

- Use the **Advanced** screen to allow intra-BSS networking and set the RTS/CTS Threshold (Section 7.6 on page 82).
- Use the **QoS** screen to ensure Quality of Service (QoS) in your wireless network (Section 7.7 on page 83).
- Use the **WPS** screen to quickly set up a wireless network with strong security, without having to configure security settings manually (Section 7.8 on page 83).
- Use the **WPS Station** screen to add a wireless station using WPS (Section 7.9 on page 85).
- Use the **Scheduling** screen to set the times your wireless LAN is turned on and off (Section 7.10 on page 85).
- Use the **WDS** screen to configure the LTE Device's WDS settings (Section 7.11 on page 86).

7.1.2 What You Should Know

Every wireless network must follow these basic guidelines.

- Every wireless client in the same wireless network must use the same SSID.

  The SSID is the name of the wireless network. It stands for Service Set IDentity.
- If two wireless networks overlap, they should use different channels.

  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every wireless client in the same wireless network must use security compatible with the AP.

  Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

Wireless Security Overview

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

SSID

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

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

MAC Address Filter

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

[1] Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.

[2] Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

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

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

User Authentication

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

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

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

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

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

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

Encryption

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

The types of encryption you can choose depend on the type of user authentication. (See page 70 for information about this.)

Table 20 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 wireless client in the wireless network supports. For example, suppose the AP does not have a local user database, and you do not have a RADIUS server. Therefore, there is no user authentication. Suppose the wireless network has two wireless clients. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.

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

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

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

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

WPS

WiFi Protected Setup (WPS) is an industry standard specification, defined by the WiFi Alliance. WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Depending on the devices in your network, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (Personal Identification Number) in the devices. Then, they connect and set up a secure network by themselves. See how to set up a secure wireless network using WPS in the Section 4.2 on page 33.

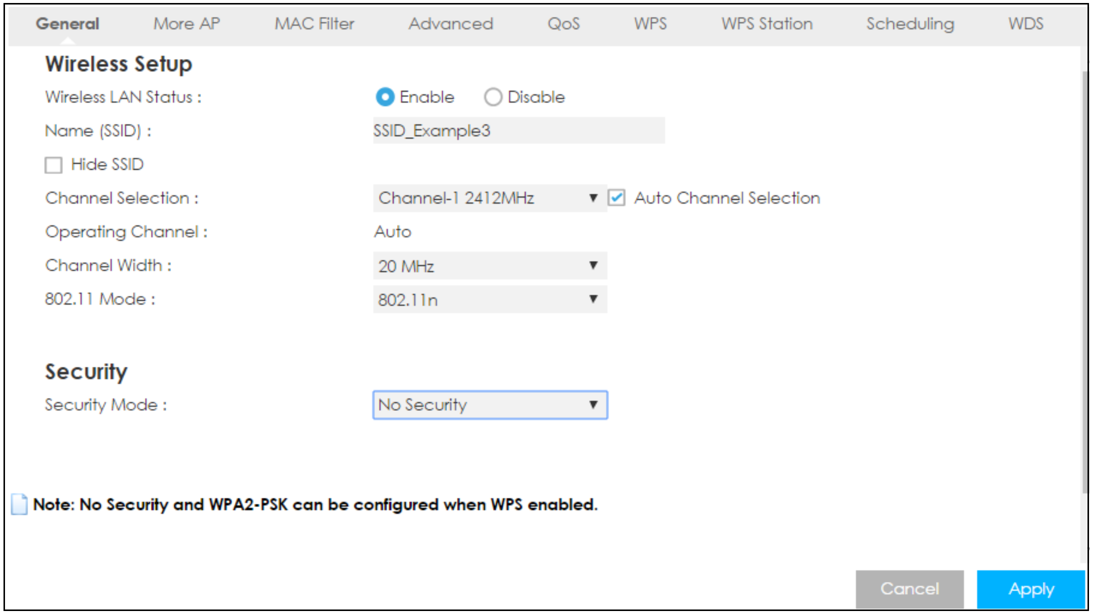
7.2 General Wireless LAN Screen

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

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

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

Figure 42 Configuration > Network > Wireless LAN > General



Wireless Setup

Wireless LAN Status : ● Enable ○ Disable

Name (SSID) : SSID_Example3

□ Hide SSID

Channel Selection : Channel-1 2412MHz ☑ Auto Channel Selection

Operating Channel : Auto

Channel Width : 20 MHz

802.11 Mode : 802.11n

Security

Security Mode : No Security

Note: No Security and WPA2-PSK can be configured when WPS enabled.

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

Table 21 Configuration > Network > Wireless LAN > General

LABEL	DESCRIPTION
Wireless Setup	
Wireless LAN Status	Select **Enable** to activate the 2.4GHz wireless LAN. Select **Disable** to turn it off. You can also enable or disable the 2.4GHz wireless LANs by using the **WIFI** button located on the back panel of the LTE Device.
Name (SSID)	The SSID (Service Set IDentity) identifies the Service Set with which a wireless client is associated. Enter a descriptive name (up to 32 printable characters found on a typical English language keyboard) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Channel Selection	Set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in. Refer to the Connection Wizard chapter for more information on channels. This option is only available if **Auto Channel Selection** is disabled.
Auto Channel Selection	Select this check box for the LTE Device to automatically choose the channel with the least interference. Deselect this check box if you wish to manually select the channel using the **Channel Selection** field.
Operating Channel	This displays the channel the LTE Device is currently using.

Table 21 Configuration > Network > Wireless LAN > General (continued)

LABEL	DESCRIPTION
Channel Width	Select the wireless channel width used by LTE Device. 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). Because not all devices support 40 MHz channels, select **Auto 20/40MHz** to allow the LTE Device to adjust the channel bandwidth automatically. **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. 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.
802.11 Mode	You can select from the following: • **802.11b**: allows either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the LTE Device. In this mode, all wireless devices can only transmit at the data rates supported by IEEE 802.11b. • **802.11g**: allows IEEE 802.11g compliant WLAN devices to associate with the Device. IEEE 802.11b compliant WLAN devices can associate with the LTE Device only when they use the short preamble type. • **802.11bg**: allows either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the LTE Device. The LTE Device adjusts the transmission rate automatically according to the wireless standard supported by the wireless devices. • **802.11n**: allows IEEE 802.11n compliant WLAN devices to associate with the LTE Device. This can increase transmission rates, although IEEE 802.11b or IEEE 802.11g clients will not be able to connect to the LTE Device. • **802.11gn**: allows either IEEE 802.11g or IEEE 802.11n compliant WLAN devices to associate with the LTE Device. The transmission rate of your LTE Device might be reduced. • **802.11bgn**: allows IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the LTE Device. The transmission rate of your LTE Device might be reduced.
Security	
Security Mode	Select **Static WEP**, **WPA-PSK**, **WPA**, **WPA2-PSK** or **WPA2** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as this device. After you select to use a security, additional options appears in this screen. See Section 7.3 on page 73 for detailed information on different security modes. Or you can select **No Security** to allow any client to associate this network without authentication. Note: If the WPS function is enabled (default), only **No Security** and **WPA2-PSK** are available in this field.
Apply	Click **Apply** to save your changes back to the LTE Device.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

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

7.3 Wireless Security

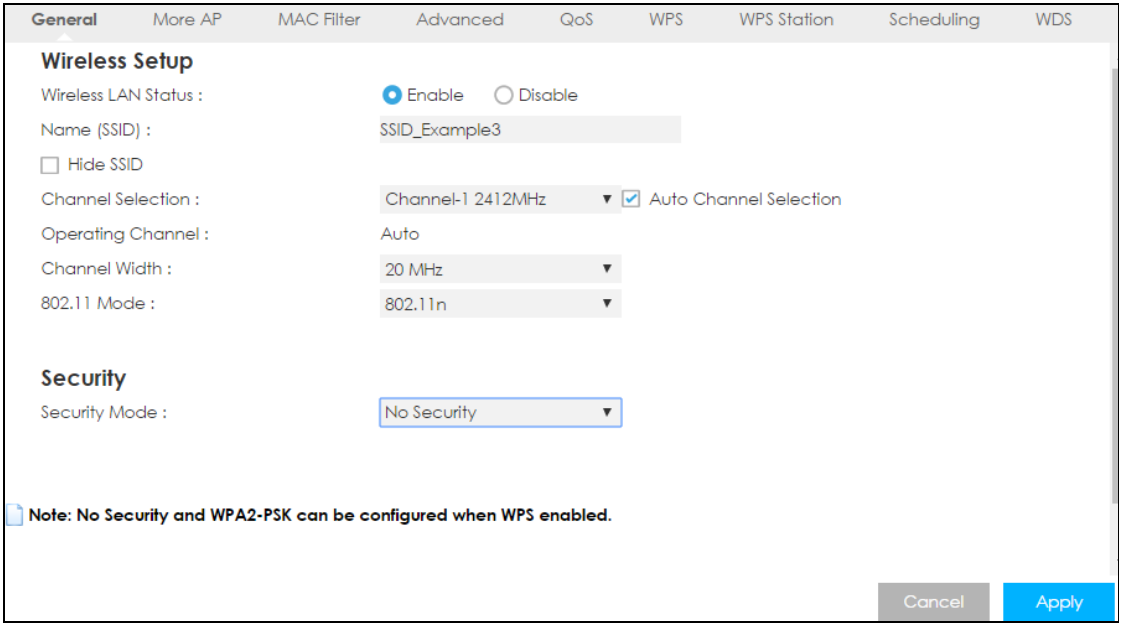
The screen varies depending on what you select in the **Security Mode** field.

7.3.1 No Security

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

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

Figure 43 Configuration > Network > Wireless LAN > General: No Security



Wireless Setup

Wireless LAN Status : ● Enable ○ Disable

Name (SSID) : SSID_Example3

□ Hide SSID

Channel Selection : Channel-1 2412MHz ☑ Auto Channel Selection

Operating Channel : Auto

Channel Width : 20 MHz

802.11 Mode : 802.11n

Security

Security Mode : No Security

Note: No Security and WPA2-PSK can be configured when WPS enabled.

The following table describes the labels in this screen.

Table 22 Configuration > Network > Wireless LAN > General: No Security

LABEL	DESCRIPTION
Security Mode	Choose **No Security** from the drop-down list box.
Cancel	Click **Cancel** to reload the previous configuration for this screen.
Apply	Click **Apply** to save your changes back to the LTE Device.

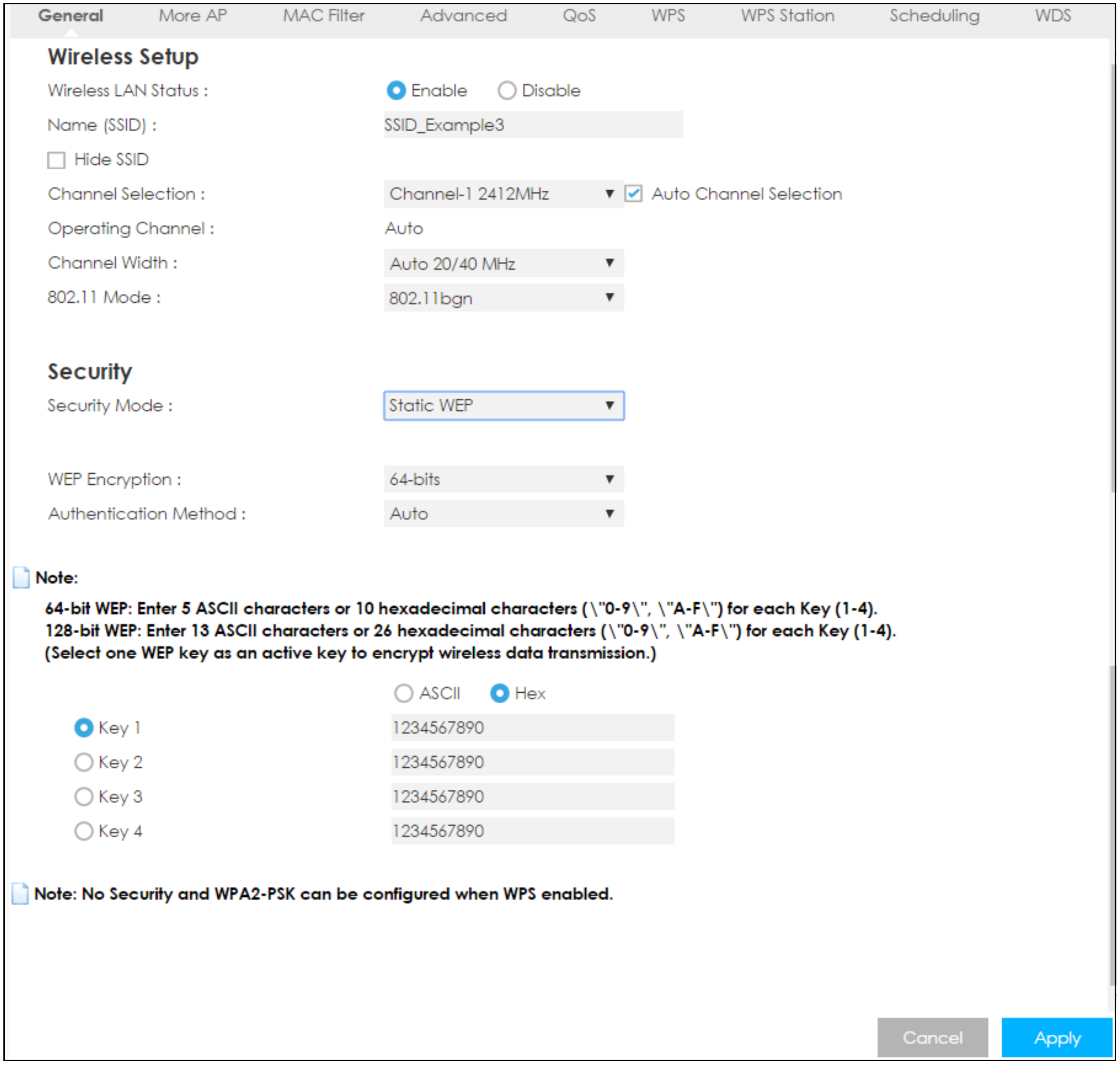
7.3.2 WEP Encryption

WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the access points must use the same WEP key.

Your LTE Device allows you to configure up to four 64-bit or 128-bit WEP keys but only one key can be enabled at any one time.

Select **Static WEP** from the **Security Mode** list.

Figure 44 Configuration > Network > Wireless LAN > General: Static WEP



Wireless Setup

Wireless LAN Status : ● Enable ○ Disable

Name (SSID) : SSID_Example3

□ Hide SSID

Channel Selection : Channel-1 2412MHz ▼ ☑ Auto Channel Selection

Operating Channel : Auto

Channel Width : Auto 20/40 MHz ▼

802.11 Mode : 802.11bgn ▼

Security

Security Mode : Static WEP ▼

WEP Encryption : 64-bits ▼

Authentication Method : Auto ▼

Note:

64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters (\"0-9\", \"A-F\") for each Key (1-4).
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters (\"0-9\", \"A-F\") for each Key (1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

○ ASCII ● Hex

● Key 1 1234567890

○ Key 2 1234567890

○ Key 3 1234567890

○ Key 4 1234567890

Note: No Security and WPA2-PSK can be configured when WPS enabled.

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

Table 23 Configuration > Network > Wireless LAN > General: Static WEP

LABEL	DESCRIPTION
Security Mode	Select **Static WEP** to enable data encryption.
WEP Encryption	Select **64-bits** or **128-bits**. This dictates the length of the security key that the network is going to use.
Authentication Method	Select **Auto** or **Shared Key** from the drop-down list box. This field specifies whether the wireless clients have to provide the WEP key to log into the wireless network. Keep this setting at **Auto** unless you want to force a key verification before communication between the wireless client and the LTE Device occurs. Select **Shared Key** to force the clients to provide the WEP key prior to communication.
ASCII	Select this option in order to enter ASCII characters as WEP key.
Hex	Select this option in order to enter hexadecimal characters as a WEP key. The preceding "0x", that identifies a hexadecimal key, is entered automatically.

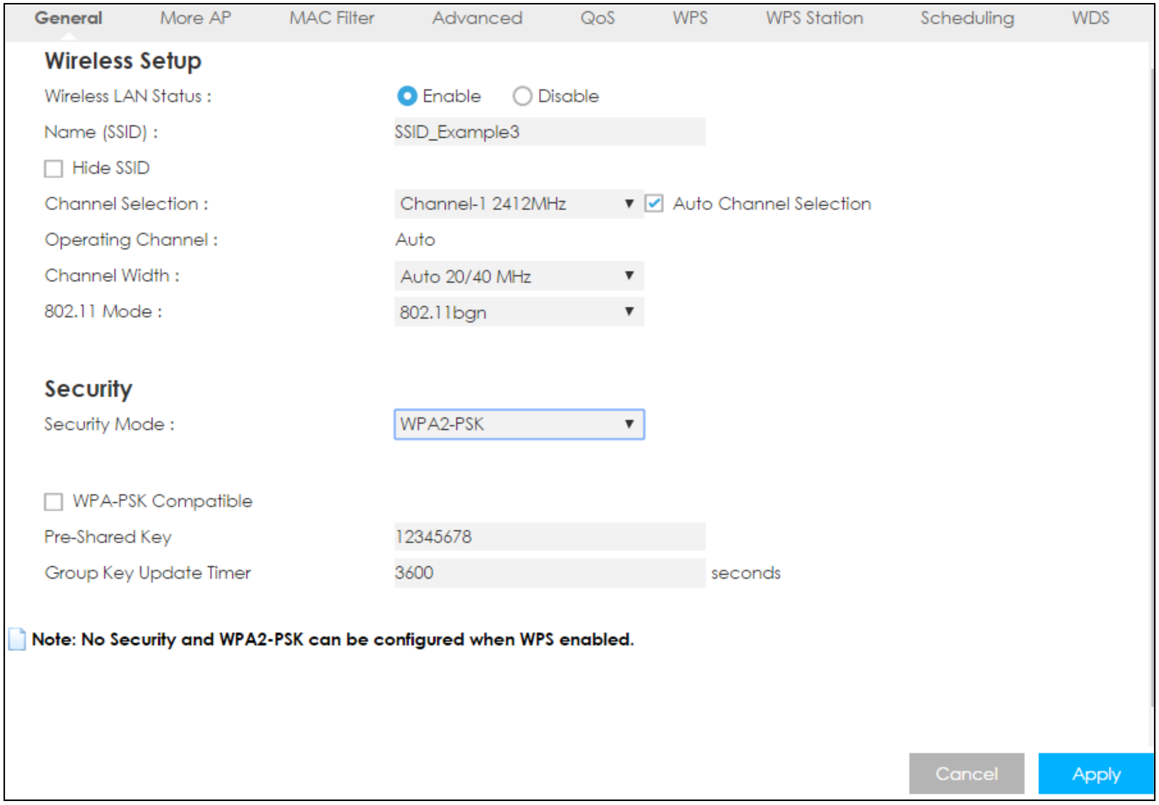
Table 23   Configuration > Network > Wireless LAN > General: Static WEP (continued)

LABEL	DESCRIPTION
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the LTE Device and the wireless stations must use the same WEP key for data transmission. If you chose **64-bits**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bits**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure at least one key, only one key can be activated at any one time. The default key is key 1.
Cancel	Click **Cancel** to reload the previous configuration for this screen.
Apply	Click **Apply** to save your changes back to the LTE Device.

7.3.3 WPA-PSK/WPA2-PSK

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

Figure 45   Configuration > Network > Wireless LAN > General: WPA-PSK/WPA2-PSK



Wireless Setup

Wireless LAN Status : ● Enable ○ Disable

Name (SSID) : SSID_Example3

□ Hide SSID

Channel Selection : Channel-1 2412MHz ▼ ☑ Auto Channel Selection

Operating Channel : Auto

Channel Width : Auto 20/40 MHz ▼

802.11 Mode : 802.11bgn ▼

Security

Security Mode : WPA2-PSK ▼

□ WPA-PSK Compatible

Pre-Shared Key 12345678

Group Key Update Timer 3600 seconds

Note: No Security and WPA2-PSK can be configured when WPS enabled.

The following table describes the labels in this screen.

Table 24 Configuration > Network > Wireless LAN > General: WPA-PSK/WPA2-PSK

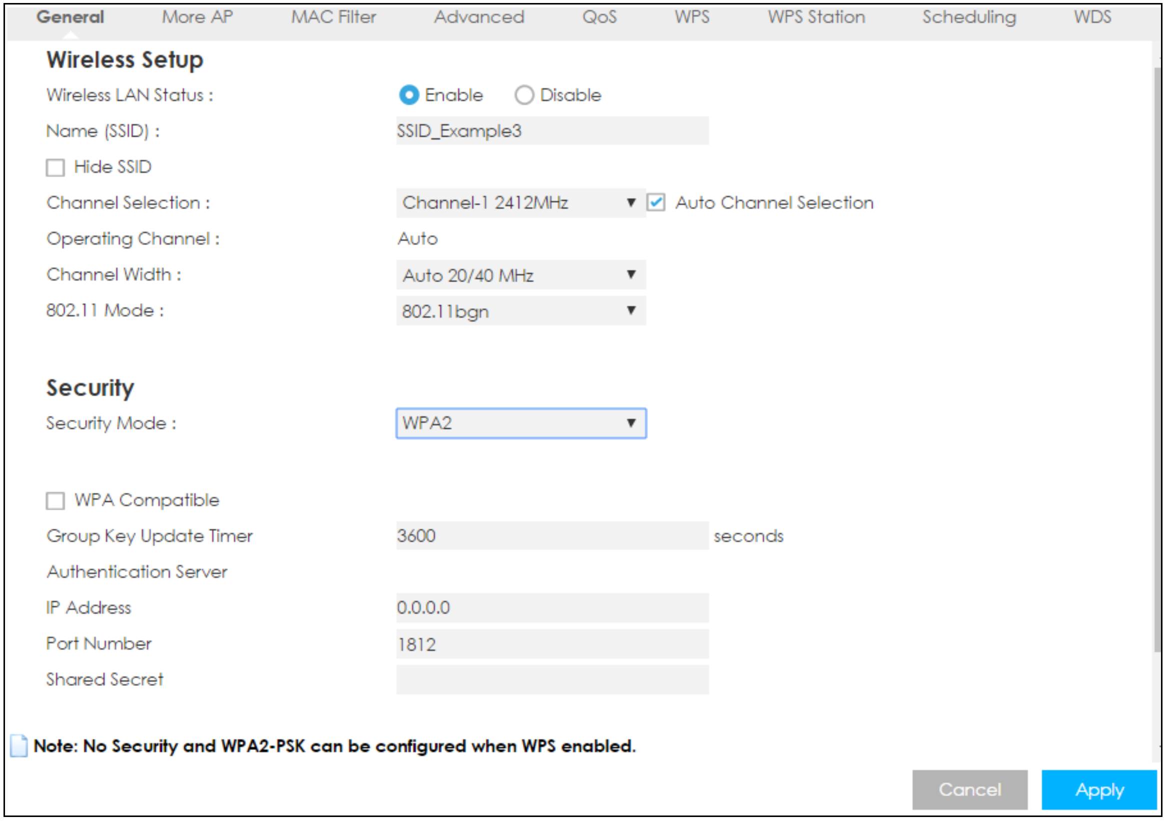
LABEL	DESCRIPTION
Security Mode	Select **WPA-PSK** or **WPA2-PSK** to enable data encryption.
WPA-PSK Compatible	This field appears when you choose **WPA2-PSK** as the **Security Mode**. Check this field to allow wireless devices using **WPA-PSK** security mode to connect to your LTE Device.
Pre-Shared Key	**WPA-PSK/WPA2-PSK** uses a simple common password for authentication. Type a pre-shared key from 8 to 63 case-sensitive keyboard characters.
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP sends a new group key out to all clients. The default is **3600** seconds (60 minutes).
Cancel	Click **Cancel** to reload the previous configuration for this screen.
Apply	Click **Apply** to save your changes back to the LTE Device.

7.3.4 WPA/WPA2

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

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

Figure 46 Configuration > Network > Wireless LAN > General: WPA/WPA2



Wireless Setup

Wireless LAN Status : ● Enable ○ Disable

Name (SSID) : SSID_Example3

□ Hide SSID

Channel Selection : Channel-1 2412MHz ☑ Auto Channel Selection

Operating Channel : Auto

Channel Width : Auto 20/40 MHz

802.11 Mode : 802.11bgn

Security

Security Mode : WPA2

□ WPA Compatible

Group Key Update Timer 3600 seconds

Authentication Server

IP Address 0.0.0.0

Port Number 1812

Shared Secret

Note: No Security and WPA2-PSK can be configured when WPS enabled.

The following table describes the labels in this screen.

Table 25 Configuration > Network > Wireless LAN > General: WPA/WPA2

LABEL	DESCRIPTION
Security Mode	Select **WPA** or **WPA2** to enable data encryption.
WPA Compatible	This check box is available only when you select **WPA2-PSK** or **WPA2** in the **Security Mode** field. Select the check box to have both WPA2 and WPA wireless clients be able to communicate with the LTE Device even when the LTE Device is using WPA2-PSK or WPA2.
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP (if using **WPA-PSK/WPA2-PSK** key management) or RADIUS server (if using **WPA/WPA2** key management) sends a new group key out to all clients. The re-keying process is the WPA/WPA2 equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in **WPA-PSK/WPA2-PSK** mode.
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 127 alphanumeric characters) as the key to be shared between the external authentication server and the LTE Device. The key must be the same on the external authentication server and your LTE Device. The key is not sent over the network.
Cancel	Click **Cancel** to reload the previous configuration for this screen.
Apply	Click **Apply** to save your changes back to the LTE Device.

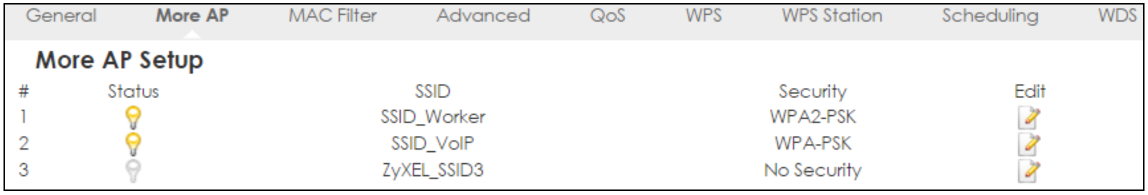
7.4 More AP Screen

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

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

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

Figure 47 Configuration > Network > Wireless LAN > More AP



More AP Setup

#	Status	SSID	Security	Edit
1	●	SSID_Worker	WPA2-PSK	✎
2	●	SSID_VoIP	WPA-PSK	✎
3	○	ZyXEL_SSID3	No Security	✎

The following table describes the labels in this screen.

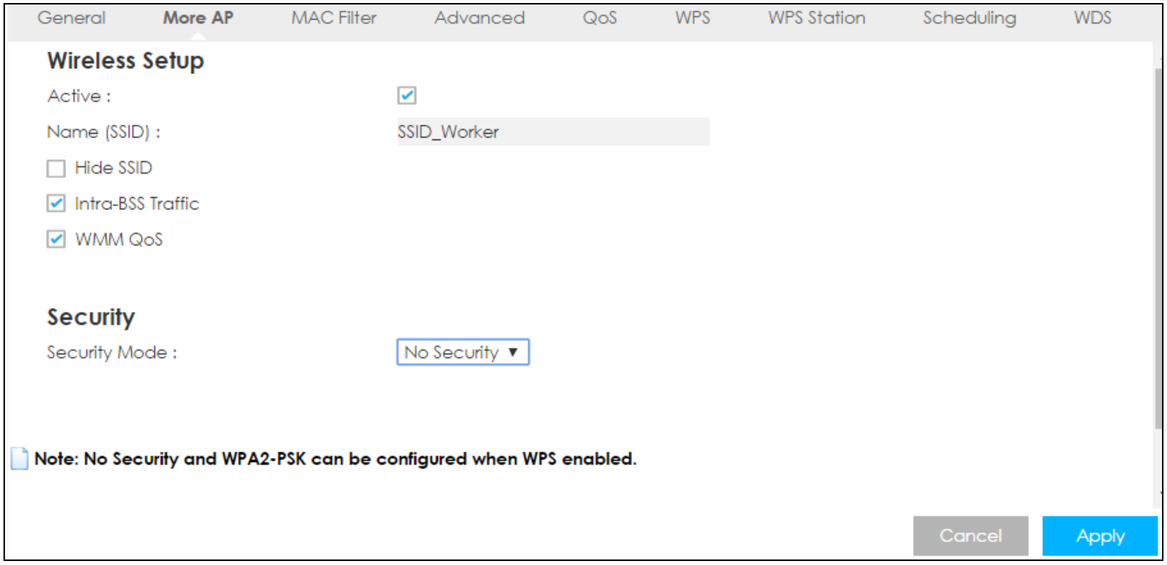
Table 26 Configuration > Network > Wireless LAN > More AP

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

7.4.1 More AP Edit

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

Figure 48 Configuration > Network > Wireless LAN > More AP: Edit



Wireless Setup

Active : ☑

Name (SSID) : SSID_Worker

☐ Hide SSID

☑ Intra-BSS Traffic

☑ WMM QoS

Security

Security Mode : No Security ▼

Note: No Security and WPA2-PSK can be configured when WPS enabled.

The following table describes the labels in this screen.

Table 27 Configuration > Network > Wireless LAN > More AP: Edit

LABEL	DESCRIPTION
Wireless Setup	
Active	Select this to activate the SSID profile.
Name (SSID)	The SSID (Service Set IDentity) identifies the Service Set with which a wireless client is associated. Enter a descriptive name (up to 32 printable characters found on a typical English language keyboard) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.

Table 27 Configuration > Network > Wireless LAN > More AP: Edit (continued)

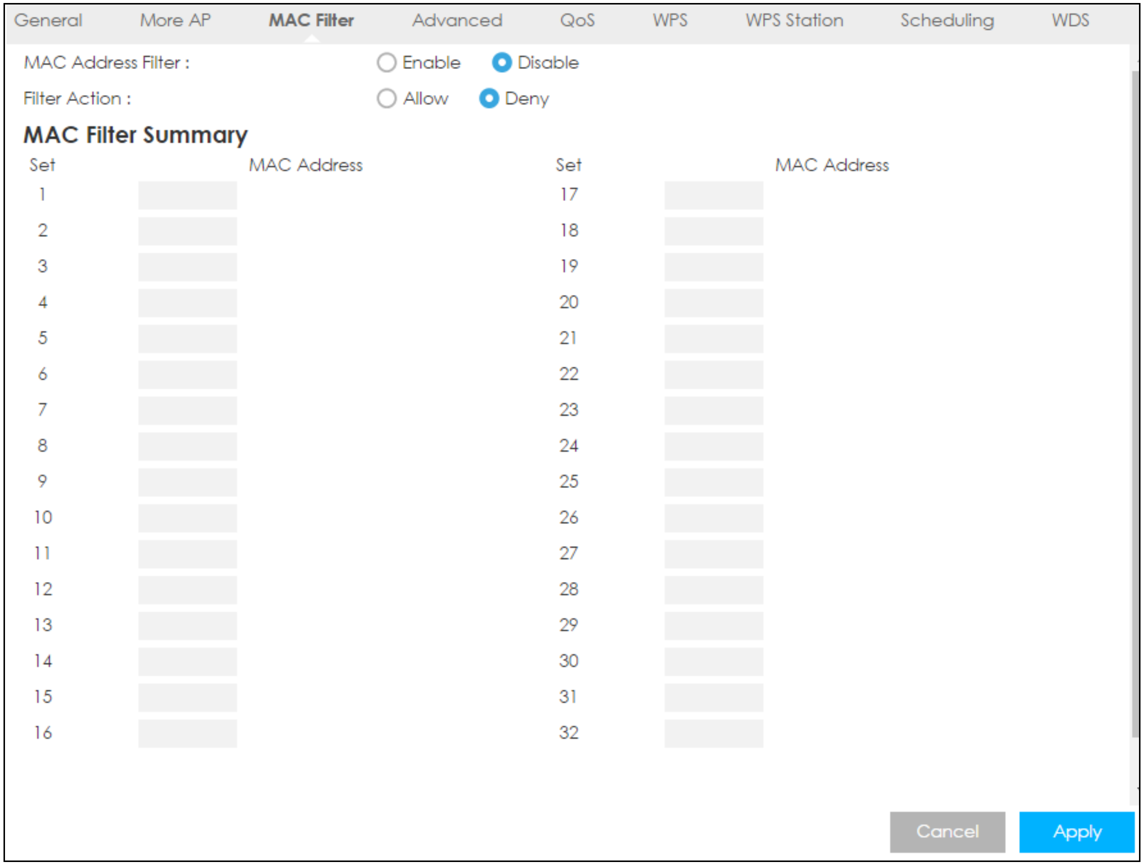
LABEL	DESCRIPTION
Intra-BSS Traffic	A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP). Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless clients can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless clients can still access the wired network but cannot communicate with each other.
WMM QoS	Check this to have the LTE Device automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly.
Security	
Security Mode	Select **Static WEP**, **WPA-PSK**, **WPA**, **WPA2-PSK** or **WPA2** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as this device. After you select to use a security, additional options appears in this screen. See Section 7.3 on page 73 for detailed information on different security modes. Or you can select **No Security** to allow any client to associate this network without authentication. Note: If the WPS function is enabled (default), only **No Security** and **WPA2-PSK** are available in this field.
Cancel	Click **Cancel** to reload the previous configuration for this screen.
Apply	Click **Apply** to save your changes back to the LTE Device.

7.5 MAC Filter Screen

The MAC filter screen allows you to configure the LTE Device to give exclusive access to devices (**Allow**) or exclude devices from accessing the LTE Device (**Deny**). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

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

Figure 49 Configuration > Network > Wireless LAN > MAC Filter



MAC Address Filter : ○ Enable ● Disable

Filter Action : ○ Allow ● Deny

MAC Filter Summary

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

The following table describes the labels in this menu.

Table 28 Configuration > Network > Wireless LAN > MAC Filter

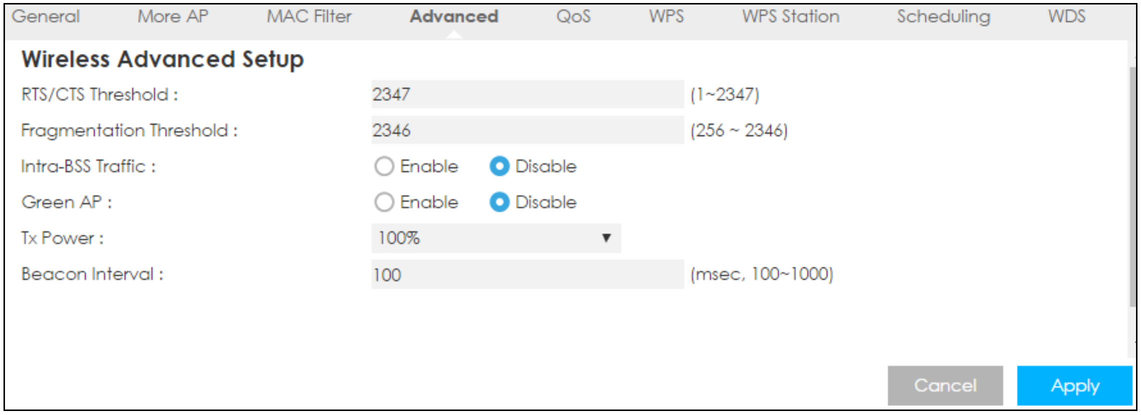
LABEL	DESCRIPTION
MAC Address Filter	Select to turn on (**Enable**) or off (**Disable**) MAC address filtering.
Filter Action	Define the filter action for the list of MAC addresses in the **MAC Filter Summary** table. Select **Allow** to permit access to the LTE Device, MAC addresses not listed will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

7.6 Wireless LAN Advanced Screen

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

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

Figure 50 Configuration > Network > Wireless LAN > Advanced



Wireless Advanced Setup

RTS/CTS Threshold : 2347 (1~2347)

Fragmentation Threshold : 2346 (256 ~ 2346)

Intra-BSS Traffic : ○ Enable ● Disable

Green AP : ○ Enable ● Disable

Tx Power : 100%

Beacon Interval : 100 (msec, 100~1000)

The following table describes the labels in this screen.

Table 29 Configuration > Network > Wireless LAN > Advanced

LABEL	DESCRIPTION
Wireless Advanced Setup	
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. This field is not configurable and the LTE Device automatically changes to use the maximum value if you select **802.11n**, **802.11gn** or **802.11bgn** in the **Wireless LAN > General** screen.
Fragmentation Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. This field is not configurable and the LTE Device automatically changes to use the maximum value if you select **802.11n**, **802.11gn** or **802.11bgn** in the **Wireless LAN > General** screen.
Intra-BSS Traffic	A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP). Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless clients can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless clients can still access the wired network but cannot communicate with each other.
Green AP	Select **Enable** to reduce the power consumption by adjusting the output power. The LTE Device reduces the output power of the transmitter from about 260mA to 188mA when there is no IEEE 802.11 wireless clients associated with the LTE Device wireless network.
Tx Power	Set the output power of the LTE Device in this field. If there is a high density of APs in an area, decrease the output power of the LTE Device to reduce interference with other APs. Select one of the following **100%**, **90%**, **75%**, **50%**, **25%** or **10%**.
Beacon Interval	When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low-power mode before waking up to handle the beacon. A high value helps save current consumption of the access point.

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

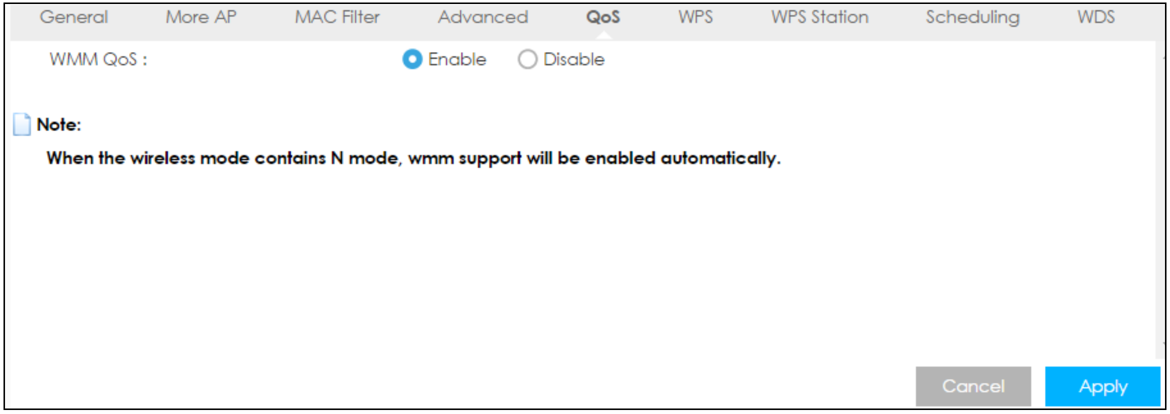
LABEL	DESCRIPTION
Cancel	Click **Cancel** to reload the previous configuration for this screen.
Apply	Click **Apply** to save your changes back to the LTE Device.

7.7 Quality of Service (QoS) Screen

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

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

Figure 51 Configuration > Network > Wireless LAN > QoS



WMM QoS : ● Enable ○ Disable

Note:

When the wireless mode contains N mode, wmm support will be enabled automatically.

The following table describes the labels in this screen.

Table 30 Configuration > Network > Wireless LAN > QoS

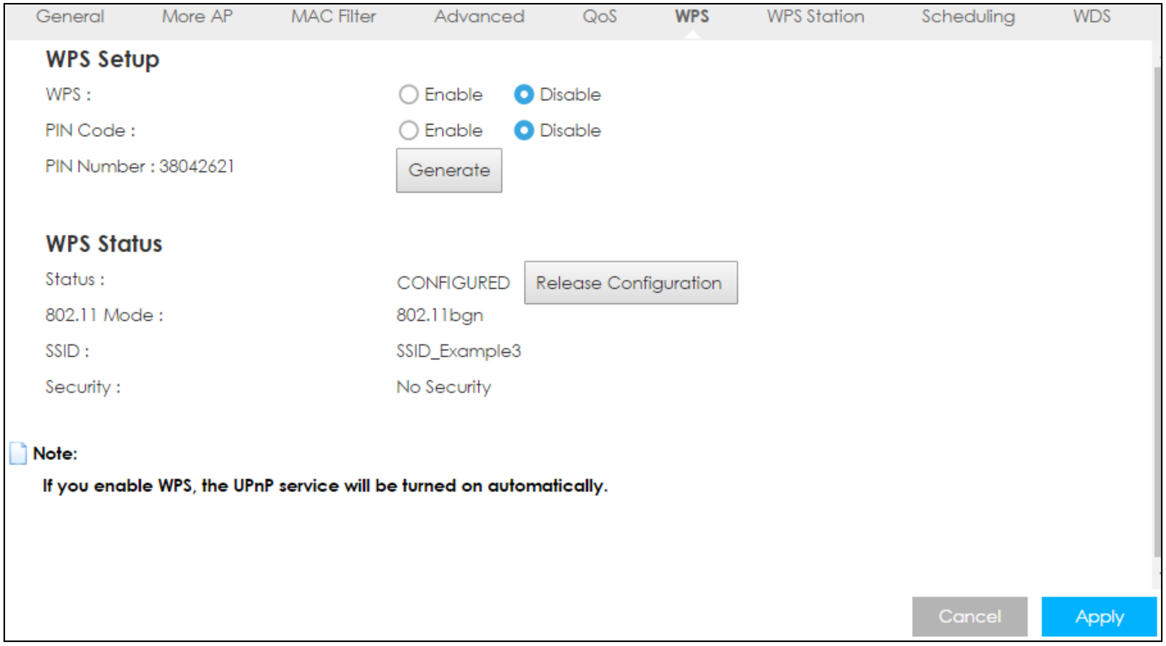
LABEL	DESCRIPTION
WMM QoS	Select **Enable** to have the LTE Device automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly. This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

7.8 WPS Screen

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

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

Figure 52 Configuration > Network > Wireless LAN > WPS



WPS Setup

WPS : ○ Enable ● Disable

PIN Code : ○ Enable ● Disable

PIN Number : 38042621

WPS Status

Status : CONFIGURED

802.11 Mode : 802.11bgn

SSID : SSID_Example3

Security : No Security

Note:

If you enable WPS, the UPnP service will be turned on automatically.

The following table describes the labels in this screen.

Table 31 Configuration > Network > Wireless LAN > WPS

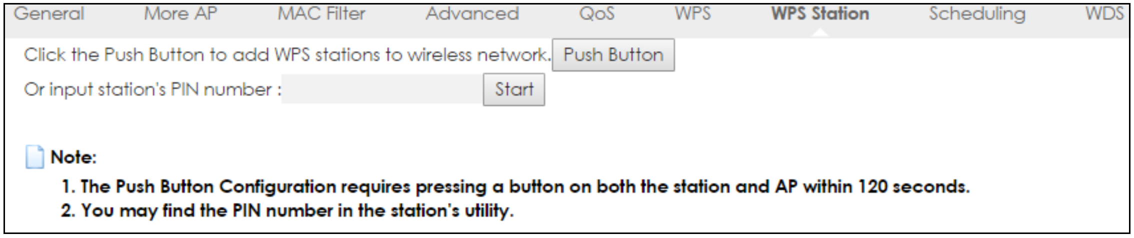
LABEL	DESCRIPTION
WPS Setup	
WPS	Select **Enable** to turn on the WPS feature. Otherwise, select **Disable**.
PIN Code	Select **Enable** and click **Apply** to allow the PIN Configuration method. If you select **Disable**, you cannot create a new PIN number.
PIN Number	This is the WPS PIN (Personal Identification Number) of the LTE Device. Enter this PIN in the configuration utility of the device you want to connect to the LTE Device using WPS. The PIN is not necessary when you use WPS push-button method. Click **Generate** to generate a new PIN number.
WPS Status	
Status	This displays **Configured** when the LTE Device has connected to a wireless network using WPS or when **WPS Enable** is selected and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the screen. This displays **Unconfigured** if WPS is disabled and there are no wireless or wireless security changes on the LTE Device or you click **Release Configuration** to remove the configured wireless and wireless security settings.
Release Configuration	This button is only available when the WPS status displays **Configured**. Click this button to remove all configured wireless and wireless security settings for WPS connections on the LTE Device.
802.11 Mode	This is the 802.11 mode used. Only compliant WLAN devices can associate with the LTE Device.
SSID	This is the name of the wireless network (the LTE Device's first SSID).
Security	This is the type of wireless security employed by the network.
Cancel	Click **Cancel** to reload the previous configuration for this screen.
Apply	Click **Apply** to save your changes back to the LTE Device.

7.9 WPS Station Screen

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

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

Figure 53 Configuration > Network > Wireless LAN > WPS Station



Click the Push Button to add WPS stations to wireless network.

Or input station's PIN number :

Note:

1. **The Push Button Configuration requires pressing a button on both the station and AP within 120 seconds.**
2. **You may find the PIN number in the station's utility.**

The following table describes the labels in this screen.

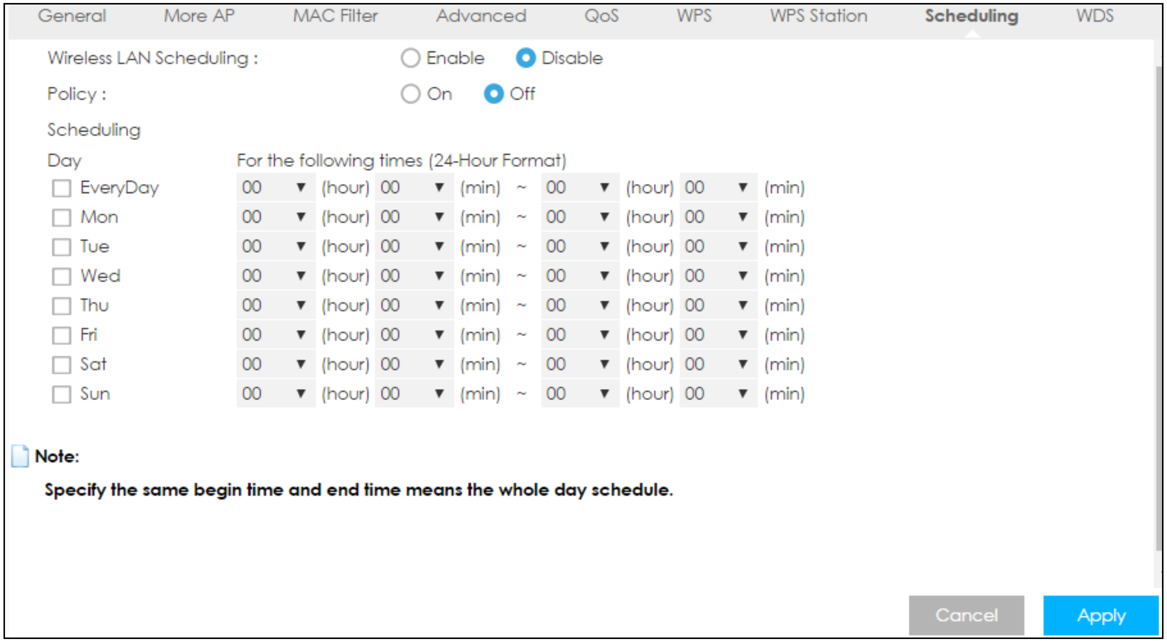
Table 32 Configuration > Network > Wireless LAN > WPS Station

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

7.10 Scheduling Screen

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

Figure 54 Configuration > Network > Wireless LAN > Scheduling



Wireless LAN Scheduling : ○ Enable ● Disable

Policy : ○ On ● Off

Scheduling

Day	For the following times (24-Hour Format)							
□ EveryDay	00 ▼	(hour)	00 ▼	(min) ~	00 ▼	(hour)	00 ▼	(min)
□ Mon	00 ▼	(hour)	00 ▼	(min) ~	00 ▼	(hour)	00 ▼	(min)
□ Tue	00 ▼	(hour)	00 ▼	(min) ~	00 ▼	(hour)	00 ▼	(min)
□ Wed	00 ▼	(hour)	00 ▼	(min) ~	00 ▼	(hour)	00 ▼	(min)
□ Thu	00 ▼	(hour)	00 ▼	(min) ~	00 ▼	(hour)	00 ▼	(min)
□ Fri	00 ▼	(hour)	00 ▼	(min) ~	00 ▼	(hour)	00 ▼	(min)
□ Sat	00 ▼	(hour)	00 ▼	(min) ~	00 ▼	(hour)	00 ▼	(min)
□ Sun	00 ▼	(hour)	00 ▼	(min) ~	00 ▼	(hour)	00 ▼	(min)

Note:

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

The following table describes the labels in this screen.

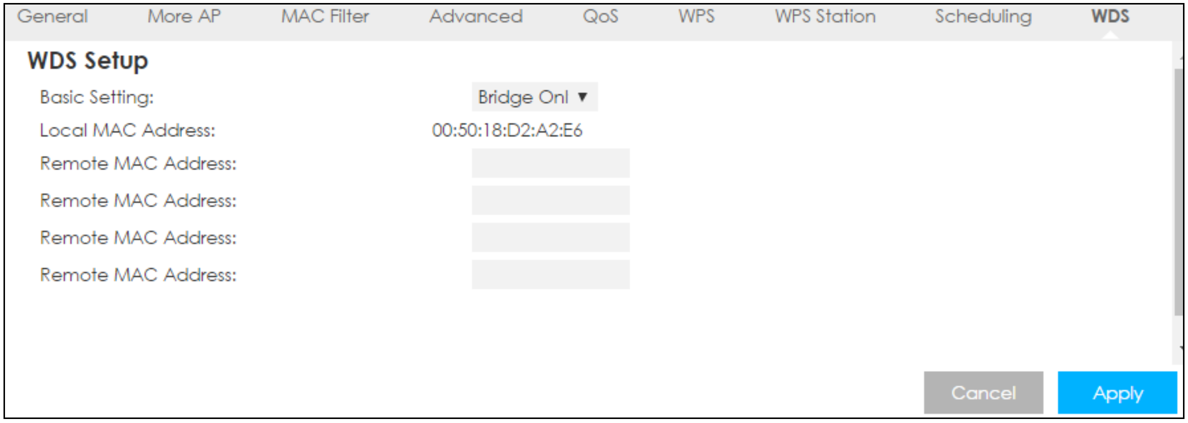
Table 33 Configuration > Network > Wireless LAN > Scheduling

LABEL	DESCRIPTION
Wireless LAN Scheduling	Select **Enable** to activate the wireless LAN scheduling feature. Select **Disable** to turn it off.
Policy	Select **On** or **Off** to specify whether the Wireless LAN is turned on or off. This field works in conjunction with the **Day** and **For the following times** fields.
Scheduling	
Day	Select **Everyday** or the specific days to turn the Wireless LAN on or off. If you select **Everyday** you can not select any specific days. This field works in conjunction with the **For the following times** field.
For the following times (24-Hour Format)	Select a begin time using the first set of **hour** and minute (**min**) drop down boxes and select an end time using the second set of **hour** and minute (**min**) drop down boxes. If you have chosen **On** earlier for the WLAN Status the Wireless LAN will turn on between the two times you enter in these fields. If you have chosen **Off** earlier for the WLAN Status the Wireless LAN will turn off between the two times you enter in these fields.
Cancel	Click **Cancel** to reload the previous configuration for this screen.
Apply	Click **Apply** to save your changes back to the LTE Device.

7.11 WDS Screen

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

Figure 55 Configuration > Network > Wireless LAN > WDS



WDS Setup

Basic Setting: Bridge Onl ▼

Local MAC Address: 00:50:18:D2:A2:E6

Remote MAC Address:

Remote MAC Address:

Remote MAC Address:

Remote MAC Address:

The following table describes the labels in this screen.

Table 34 Configuration > Network > Wireless LAN > WDS

LABEL	DESCRIPTION
WDS Setup	
Basic Setting	Select **Disable** to turn off the WDS function on the LTE Device. Select **AP+Bridge** to have the LTE Device function as a bridge and access point simultaneously. Select **Bridge Only** to have the LTE Device act as a wireless bridge only.
Local MAC Address	This shows the MAC address of the LTE Device.
Remote MAC Address	Type the MAC address of the peer device in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Cancel	Click **Cancel** to reload the previous configuration for this screen.
Apply	Click **Apply** to save your changes back to the LTE Device.

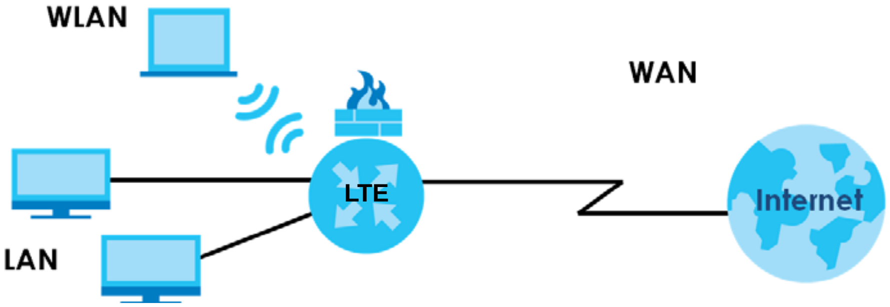
CHAPTER 8
LAN

8.1 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 56 LAN Example



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

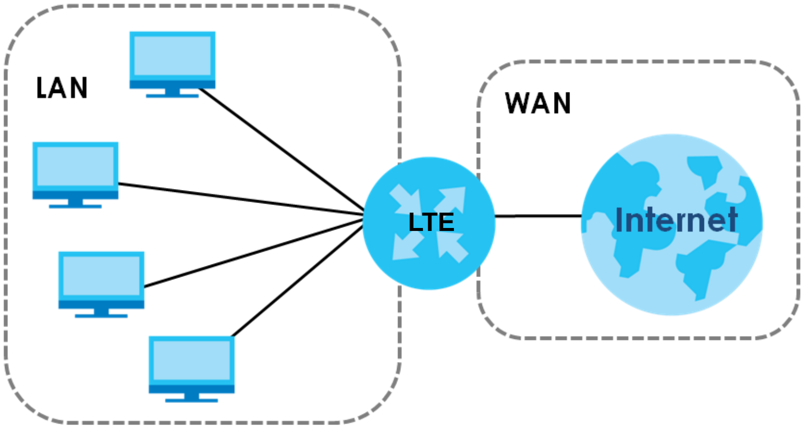
8.2 What You Can Do

- Use the **IP** screen to change the IP address for your LTE Device (Section 8.4 on page 89).

8.3 What You Need To Know

The actual physical connection determines whether the LTE Device 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 57 LAN and WAN IP Addresses



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

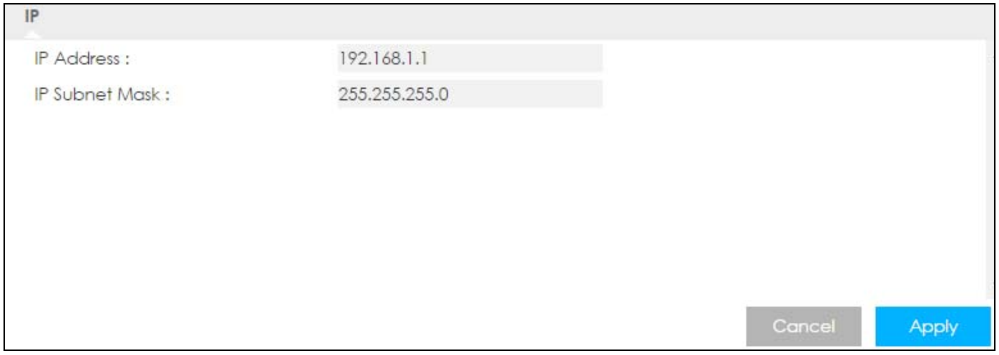
- IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

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.

8.4 LAN IP Screen

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

Figure 58 Configuration > Network > LAN > IP



IP Address : 192.168.1.1

IP Subnet Mask : 255.255.255.0

The following table describes the labels in this screen.

Table 35 Configuration > Network > LAN > IP

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

CHAPTER 9
DHCP Server

9.1 Overview

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

9.1.1 What You Can Do

- Use the **General** screen to enable the DHCP server (Section 9.2 on page 90).
- Use the **Advanced** screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses (Section 9.3 on page 92).
- Use the **Client List** screen to view the current DHCP client information (Section 9.4 on page 94).

9.1.2 What You Need To Know

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

MAC Addresses

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. Find out the MAC addresses of your network devices if you intend to add them to the **DHCP Client List** screen.

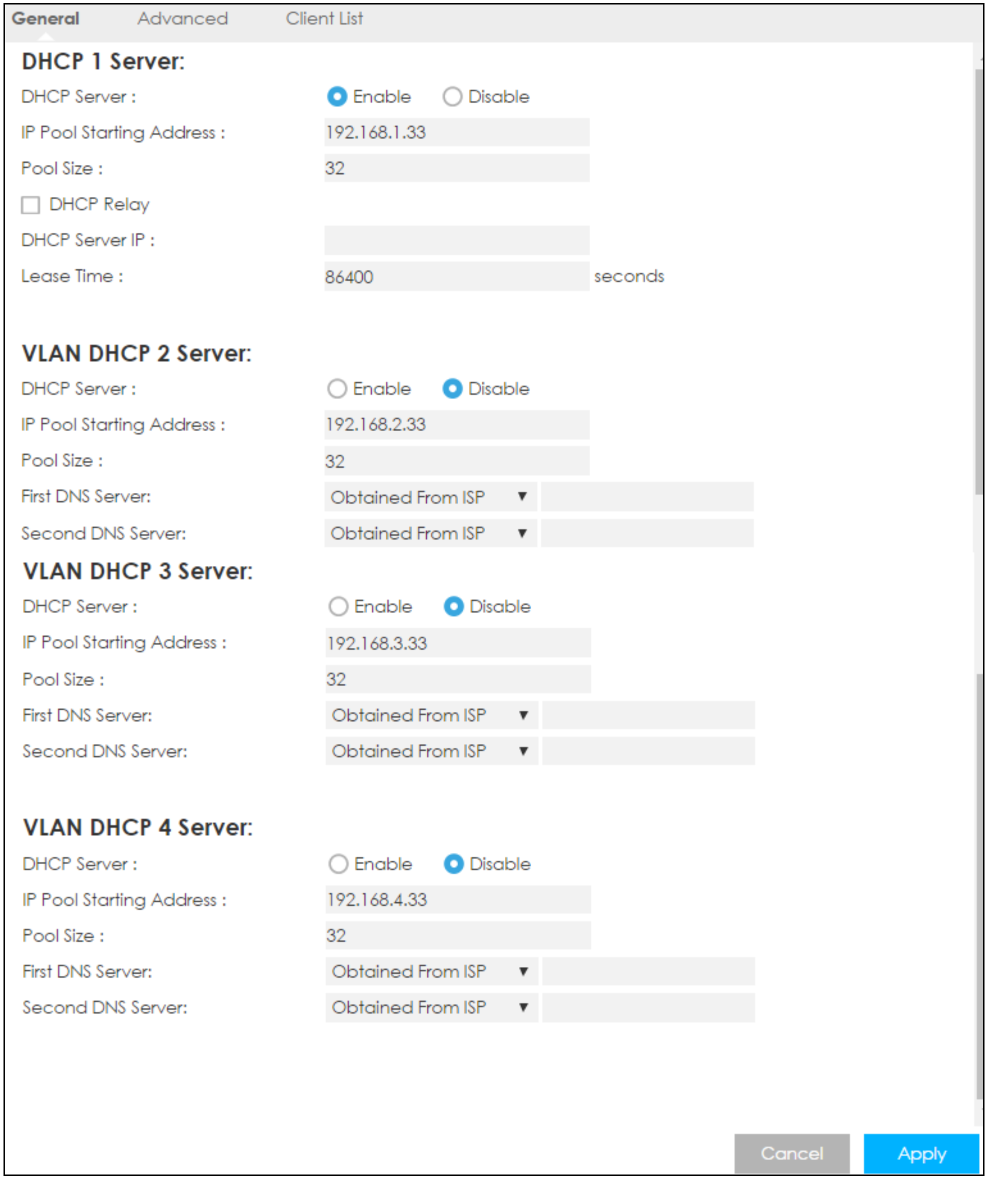
IP Pool Setup

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

9.2 DHCP Server General Screen

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

Figure 59 Configuration > Network > DHCP Server > General



DHCP 1 Server:

DHCP Server : ● Enable ○ Disable

IP Pool Starting Address : 192.168.1.33

Pool Size : 32

□ DHCP Relay

DHCP Server IP :

Lease Time : 86400 seconds

VLAN DHCP 2 Server:

DHCP Server : ○ Enable ● Disable

IP Pool Starting Address : 192.168.2.33

Pool Size : 32

First DNS Server: Obtained From ISP ▼

Second DNS Server: Obtained From ISP ▼

VLAN DHCP 3 Server:

DHCP Server : ○ Enable ● Disable

IP Pool Starting Address : 192.168.3.33

Pool Size : 32

First DNS Server: Obtained From ISP ▼

Second DNS Server: Obtained From ISP ▼

VLAN DHCP 4 Server:

DHCP Server : ○ Enable ● Disable

IP Pool Starting Address : 192.168.4.33

Pool Size : 32

First DNS Server: Obtained From ISP ▼

Second DNS Server: Obtained From ISP ▼

The following table describes the labels in this screen.

Table 36 Configuration > Network > DHCP Server > General

LABEL	DESCRIPTION
DHCP 1 Server	
DHCP Server	Select **Enable** to activate DHCP for LAN. DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. Enable the DHCP server unless your ISP instructs you to do otherwise. Select **Disable** to stop the LTE Device acting as a DHCP server. When configured as a server, the LTE Device provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computers must be manually configured. When set as a server, fill in the following four fields.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool for LAN.
Pool Size	This field specifies the size, or count of the IP address pool for LAN.

Table 36 Configuration > Network > DHCP Server > General (continued)

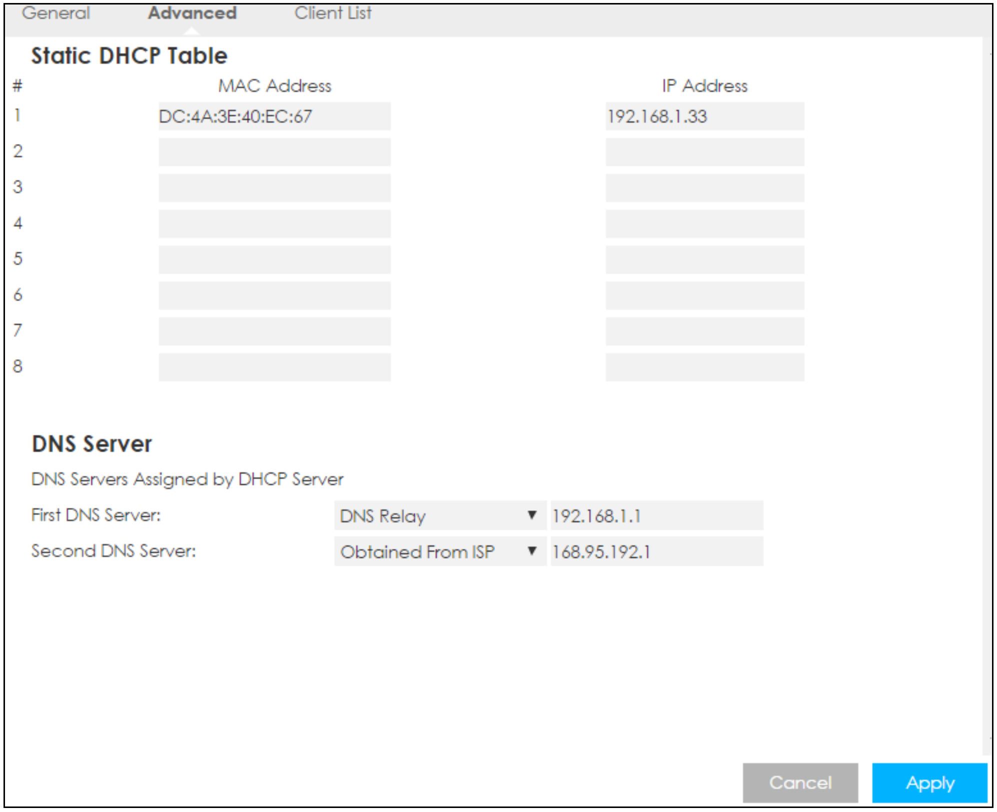
LABEL	DESCRIPTION
DHCP Relay	Select this option to have the LTE Device forward DHCP requests to the DHCP server.
DHCP Server IP	This field is configurable only when you select **DHCP Relay**. Enter the IP address of the actual remote DHCP server in this field.
Lease Time	This is the period of time DHCP-assigned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

9.3 DHCP Server Advanced Screen

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

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

Figure 60 Configuration > Network > DHCP Server > Advanced



Static DHCP Table

#	MAC Address	IP Address
1	DC:4A:3E:40:EC:67	192.168.1.33
2		
3		
4		
5		
6		
7		
8		

DNS Server

DNS Servers Assigned by DHCP Server

First DNS Server: DNS Relay ▼ 192.168.1.1

Second DNS Server: Obtained From ISP ▼ 168.95.192.1

The following table describes the labels in this screen.

Table 37 Configuration > Network > DHCP Server > Advanced

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

Table 37 Configuration > Network > DHCP Server > Advanced (continued)

LABEL	DESCRIPTION
Cancel	Click **Cancel** to begin configuring this screen afresh.
Apply	Click **Apply** to save your changes back to the LTE Device.

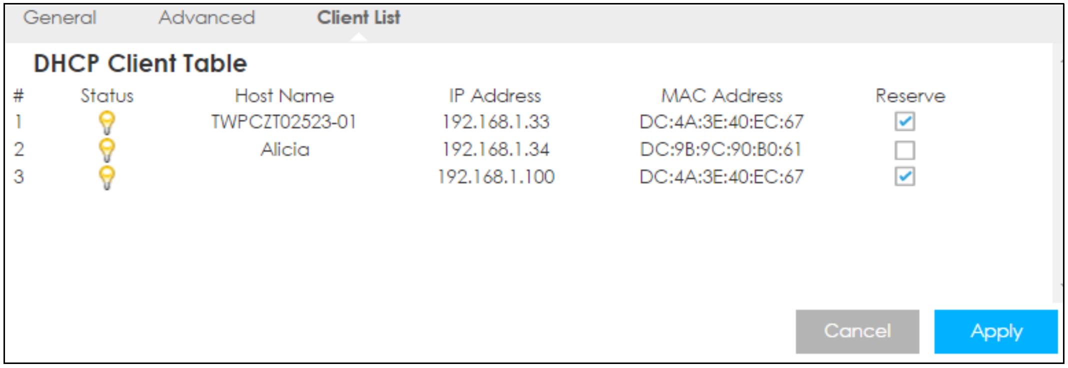
9.4 DHCP Client List Screen

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

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

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

Figure 61 Configuration > Network > DHCP Server > Client List



DHCP Client Table

#	Status	Host Name	IP Address	MAC Address	Reserve
1	💡	TWPCZT02523-01	192.168.1.33	DC:4A:3E:40:EC:67	☑
2	💡	Alicia	192.168.1.34	DC:9B:9C:90:B0:61	□
3	💡		192.168.1.100	DC:4A:3E:40:EC:67	☑

The following table describes the labels in this screen.

Table 38 Configuration > Network > DHCP Server > Client List

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

CHAPTER 10 NAT

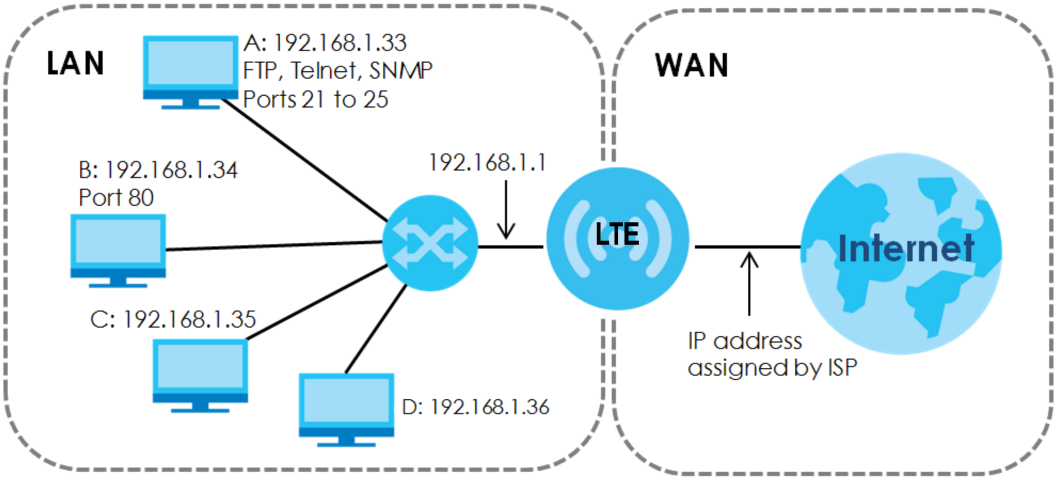
10.1 Overview

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 LTE Device. The ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet. All traffic coming from **A** to **D** going out to the Internet use the IP address of the LTE Device, which is 192.168.1.1.

Figure 62 NAT Example



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

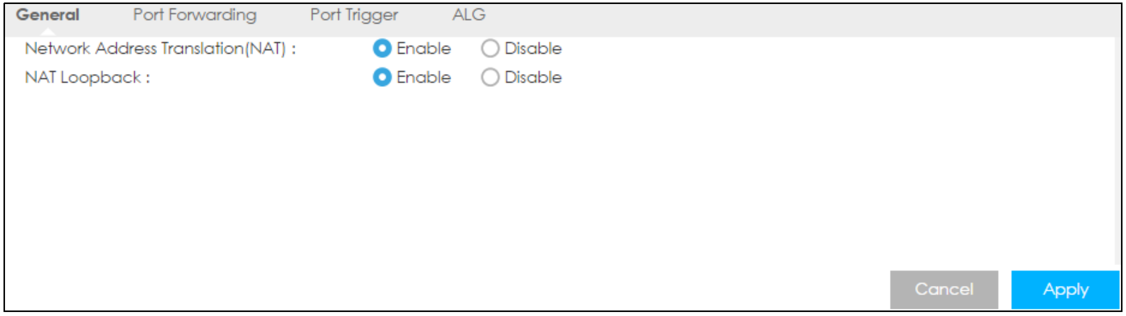
10.1.1 What You Can Do

- Use the **General** screen to enable NAT (Section 10.2 on page 96).
- Use the **Port Forwarding** screen to set a default server and change your LTE Device's port forwarding settings to forward incoming service requests to the server(s) on your local network (Section 10.3 on page 96).
- Use the **Port Trigger** screen to change your LTE Device's trigger port settings (Section 10.4 on page 99).
- Use the **ALG** screen to enable or disable SIP (VoIP) ALG (Application Layer Gateway) in the LTE Device (Section 10.5 on page 101).

10.2 General Screen

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

Figure 63 Configuration > Network > NAT > General



Network Address Translation(NAT) : ● Enable ○ Disable

NAT Loopback : ● Enable ○ Disable

The following table describes the labels in this screen.

Table 39 Configuration > Network > NAT > General

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

10.3 Port Forwarding Screen

Use this screen to forward incoming service requests to the server(s) on your local network and set a default server. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers.

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

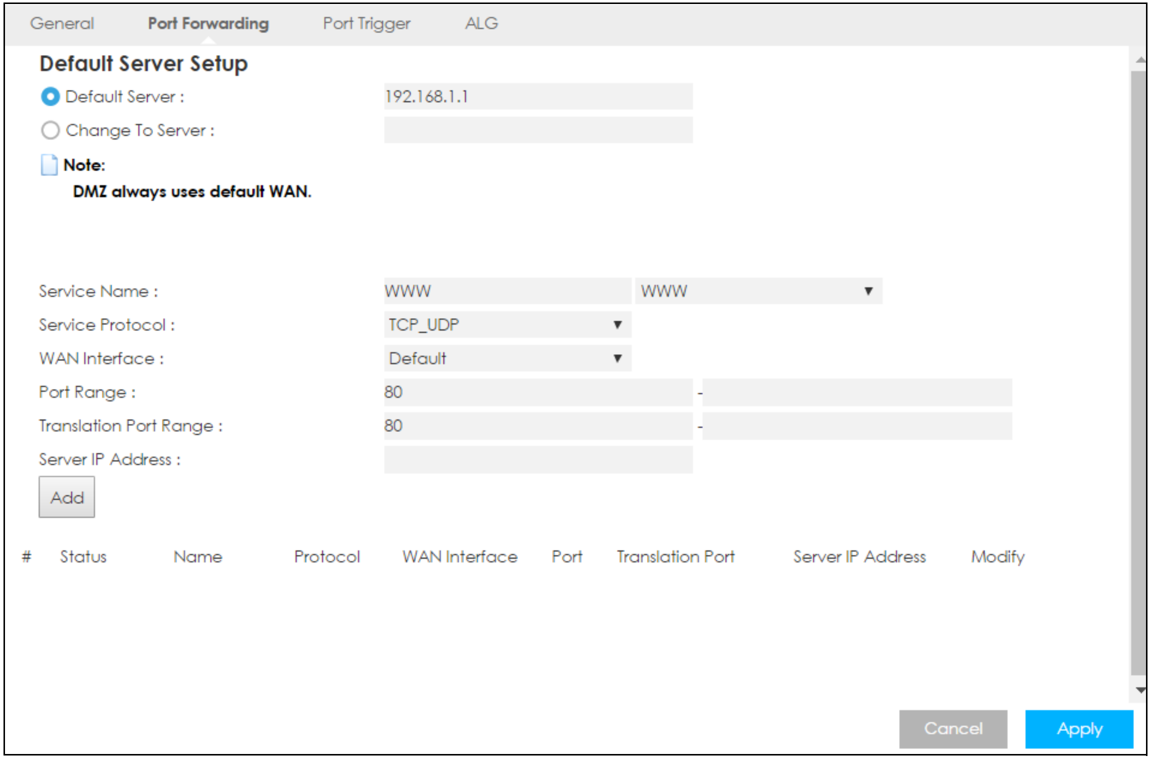
Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your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

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

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

Refer to Appendix B on page 183 for port numbers commonly used for particular services.

Figure 64 Configuration > Network > NAT > Port Forwarding



Default Server Setup

● Default Server : 192.168.1.1

○ Change To Server :

Note:
DMZ always uses default WAN.

Service Name : WWW | WWW ▼

Service Protocol : TCP_UDP ▼

WAN Interface : Default ▼

Port Range : 80 -

Translation Port Range : 80 -

Server IP Address :

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

The following table describes the labels in this screen.

Table 40 Configuration > Network > NAT > Port Forwarding

LABEL	DESCRIPTION
Default Server Setup	
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in the **Port Forwarding** screen. You can decide whether you want to use the default server or specify a server manually. Select this to use the default server.
Change to Server	Select this and manually enter the server's IP address.

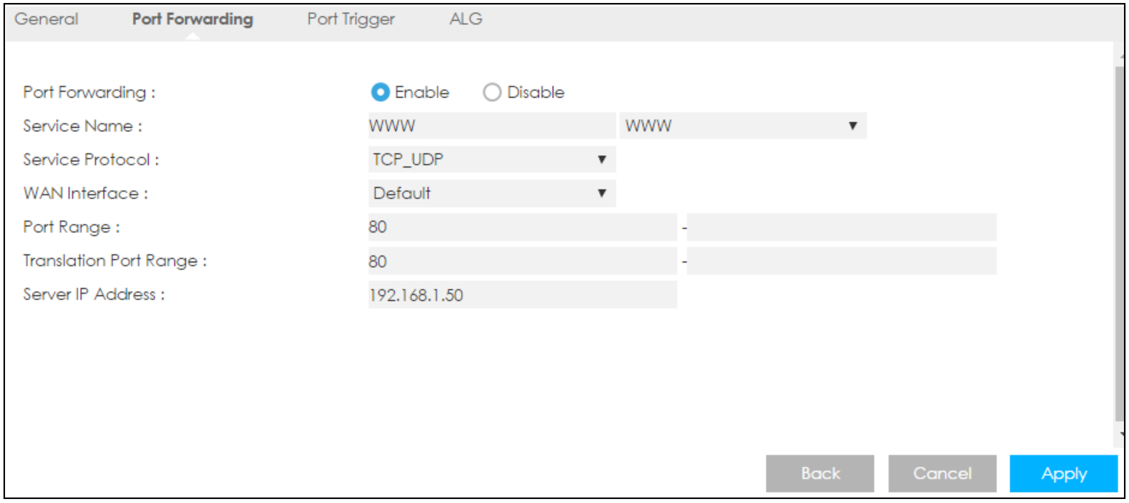
Table 40 Configuration > Network > NAT > Port Forwarding (continued)

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

10.3.1 Port Forwarding Edit Screen

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

Figure 65 Configuration > Network > NAT > Port Forwarding Edit



Port Forwarding : ● Enable ○ Disable
Service Name : WWW | WWW ▼
Service Protocol : TCP_UDP ▼
WAN Interface : Default ▼
Port Range : 80 -
Translation Port Range : 80 -
Server IP Address : 192.168.1.50

The following table describes the labels in this screen.

Table 41 Configuration > Network > NAT > Port Forwarding Edit

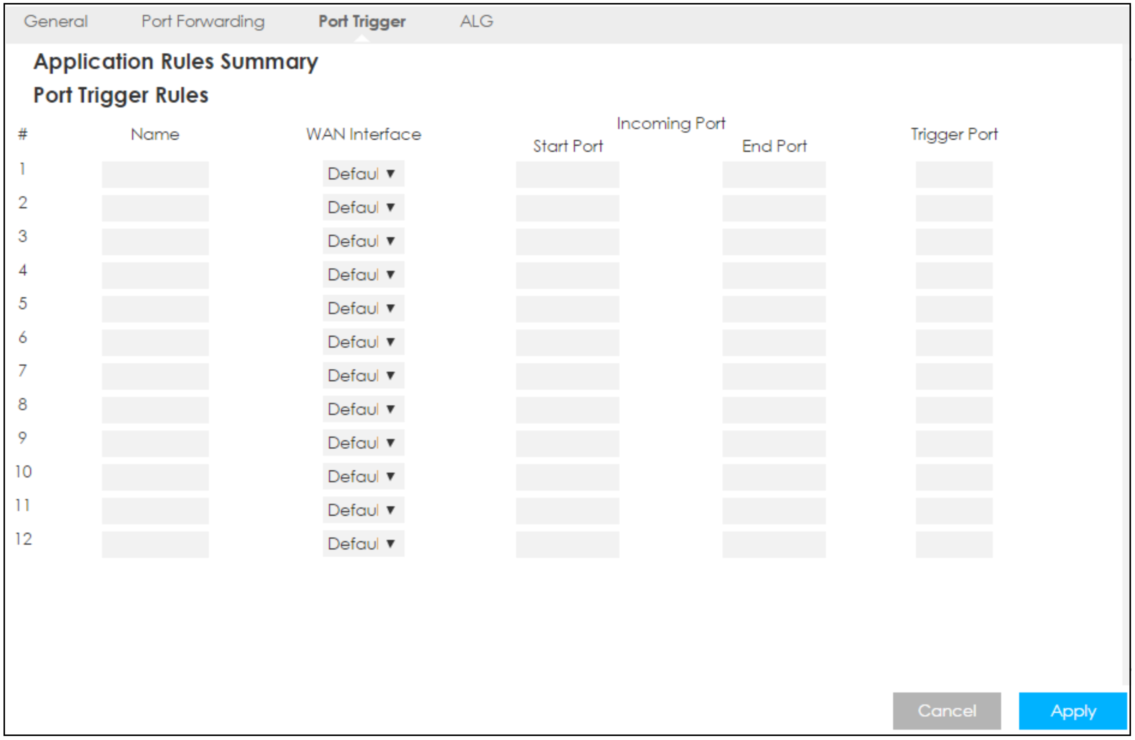
LABEL	DESCRIPTION
Port Forwarding	Select **Enable** to turn on this rule and the requested service can be forwarded to the host with a specified internal IP address. Select **Disable** to disallow forwarding of these ports to an inside server without having to delete the entry.
Service Name	Select **User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

10.4 Port Trigger Screen

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

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

Figure 66 Configuration > Network > NAT > Port Trigger



Application Rules Summary

Port Trigger Rules

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

The following table describes the labels in this screen.

Table 42 Configuration > Network > NAT > Port Trigger

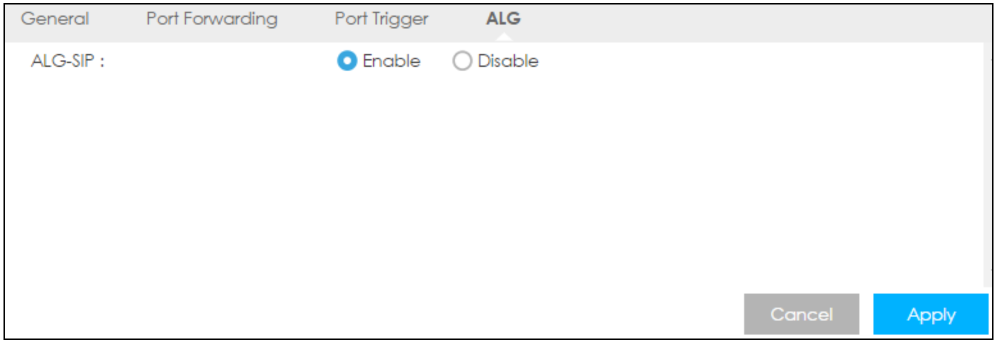
LABEL	DESCRIPTION
Application Rule Summary	
Port Trigger Rules	
#	This is the rule index number (read-only).
Name	Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces.
WAN Interface	Select the WAN interface through which the matched packets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

10.5 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 > Network > NAT > ALG**. The screen appears as shown.

Figure 67 Configuration > Network > NAT > ALG



ALG-SIP : ● Enable ○ Disable

The following table describes the labels in this screen.

Table 43 Configuration > Network > NAT > ALG

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

10.6 Technical Reference

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

10.6.1 NATPort Forwarding: Services and Port Numbers

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

Use the **Port Forwarding** screen to forward incoming service requests to the server(s) on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers.

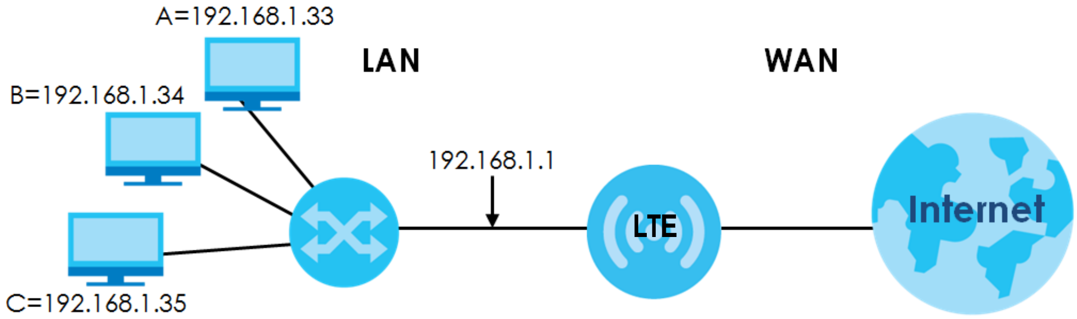
In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

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

10.6.2 NAT Port Forwarding Example

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 68 Multiple Servers Behind NAT Example



10.6.3 Trigger Port Forwarding

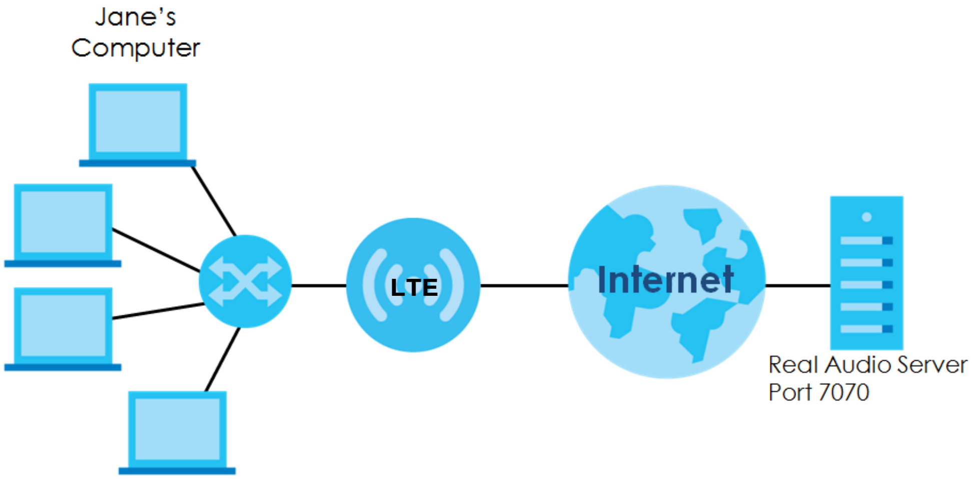
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem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

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The LTE Device records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the LTE Device's WAN port receives a response with a specific port number and protocol ("incoming" port), the LTE Device forwards the traffic to the LAN IP address of the computer that sent the request. After that computer’s connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

10.6.4 Trigger Port Forwarding Example

The following is an example of trigger port forwarding.

Figure 69 Trigger Port Forwarding Process: Example



1. Jane requests a file from the Real Audio server (port 7070).

2. Port 7070 is a "trigger" port and causes the LTE Device to record Jane's computer IP address. The LTE Device associates Jane's computer IP address with the "incoming" port range of 6970-7170.

3. The Real Audio server responds using a port number ranging between 6970-7170.

4. The LTE Device forwards the traffic to Jane's computer IP address.

5. Only Jane can connect to the Real Audio server until the connection is closed or times out. The LTE Device times out in three minutes with UDP (User Datagram Protocol), or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

10.6.5 Two Points To Remember About Trigger Ports

1. Trigger events only happen on data that is coming from inside the LTE Device and going to the outside.

2. If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can't trigger it.

CHAPTER 11
DDNS

11.1 Overview

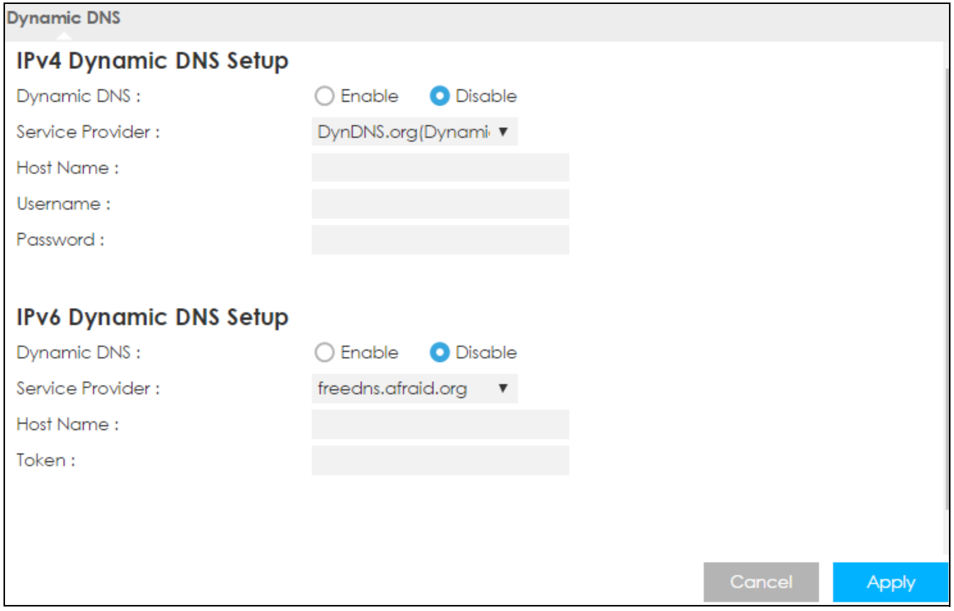
Dynamic Domain Name Service (DDNS) services let you use a fixed domain name with a dynamic IP address. Users can always use the same domain name instead of a different dynamic IP address that changes each time to connect to the LTE Device or a server in your network.

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

11.2 General

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

Figure 70 Configuration > Network > Dynamic DNS



Dynamic DNS

IPv4 Dynamic DNS Setup

Dynamic DNS : ○ Enable ● Disable

Service Provider : DynDNS.org(Dynami ▼

Host Name :

Username :

Password :

IPv6 Dynamic DNS Setup

Dynamic DNS : ○ Enable ● Disable

Service Provider : freedns.afraid.org ▼

Host Name :

Token :

The following table describes the labels in this screen.

Table 44 Configuration > Network > Dynamic DNS

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

Table 44   Configuration > Network > Dynamic DNS (continued)

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

CHAPTER 12 Routing

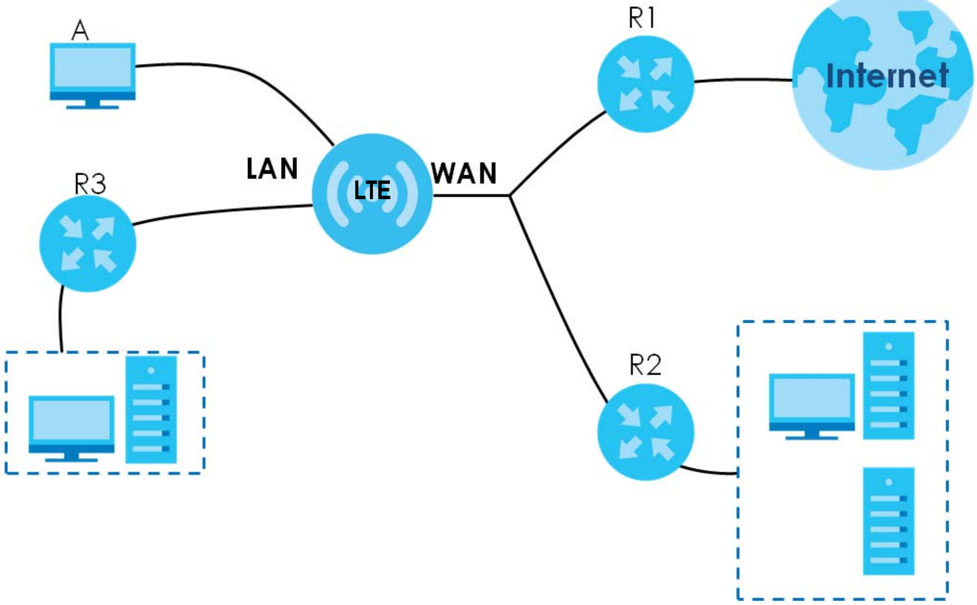
12.1 Overview

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

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

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

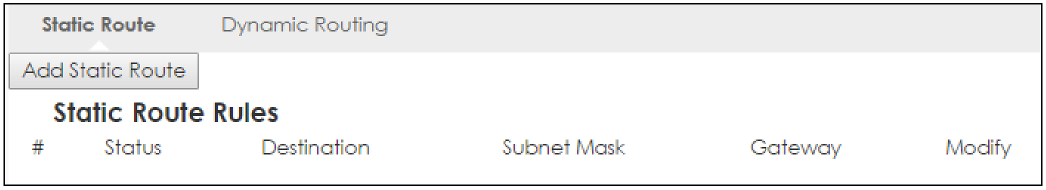
Figure 71 Example of Static Routing Topology



12.2 Static Route Screen

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

Figure 72 Configuration > Network > Routing > Static Route



Static Route Rules

#	Status	Destination	Subnet Mask	Gateway	Modify

The following table describes the labels in this screen.

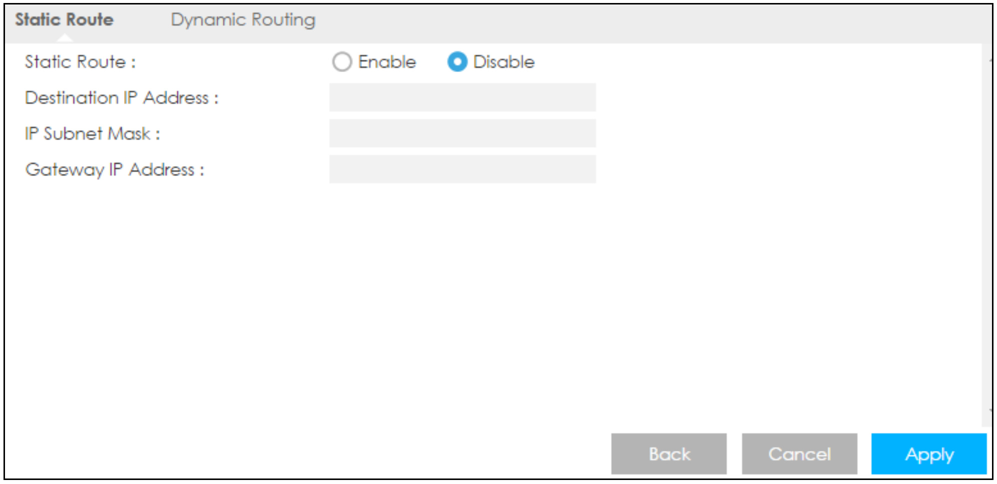
Table 45 Configuration > Network > Routing > Static Route

LABEL	DESCRIPTION
Add Static Route	Click this to create a new rule.
#	This is the number of an individual static route.
Status	This field indicates whether the rule is active (yellow bulb) or not (gray bulb).
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Subnet Mask	This parameter specifies the IP network subnet mask of the final destination.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Modify	Click the **Edit** icon to open a screen where you can modify an existing rule. Click the **Delete** icon to remove a rule from the LTE Device.

12.2.1 Add/Edit Static Route

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

Figure 73 Configuration > Network > Routing > Static Route: Add/Edit



Static Route : ○ Enable ● Disable

Destination IP Address :

IP Subnet Mask :

Gateway IP Address :

The following table describes the labels in this screen.

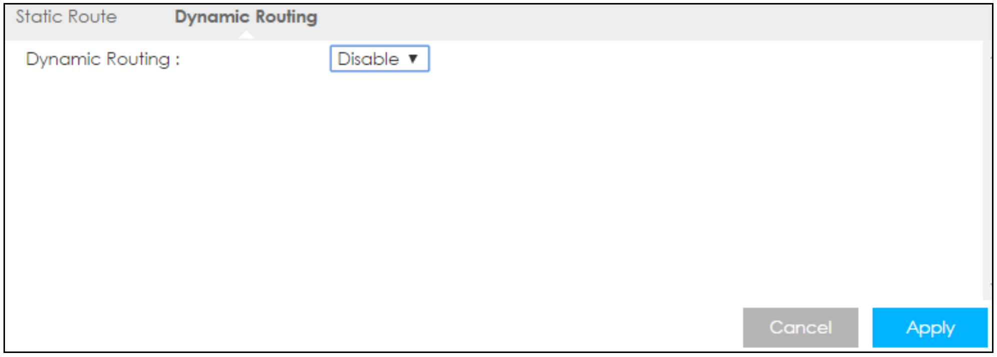
Table 46 Configuration > Network > Routing > Static Route: Add/Edit

LABEL	DESCRIPTION
Static Route	Select to enable or disable this rule.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your LTE Device's interface(s). The gateway helps forward packets to their destinations.
Back	Click **Back** to return to the previous screen without saving.
Cancel	Click **Cancel** to set every field in this screen to its last-saved value.
Apply	Click **Apply** to save your changes back to the LTE Device.

12.3 Dynamic Routing Screen

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

Figure 74 Configuration > Network > Routing > Dynamic Routing



Dynamic Routing : Disable ▼

The following table describes the labels in this screen.

Table 47 Configuration > Network > Routing > Dynamic Routing

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

CHAPTER 13
Interface Group

13.1 Overview

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

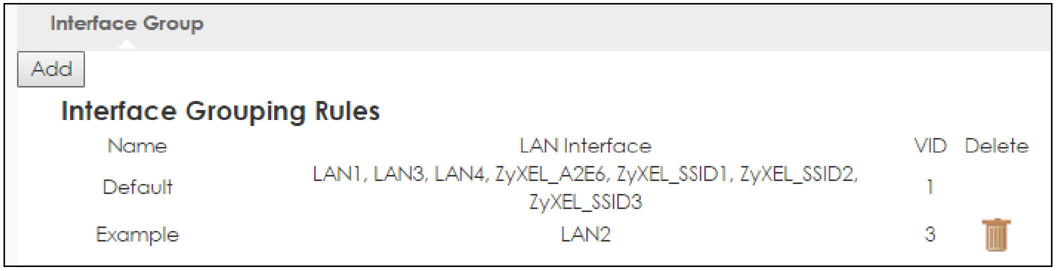
13.2 Interface Group Screen

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

Use the **DHCP** screen to configure the private IP addresses the DHCP server on the LTE Device assigns to the clients in the default and/or user-defined groups. See Chapter 9 on page 90 for more information.

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

Figure 75 Configuration > Network > Interface Group



Interface Grouping Rules

Name	LAN Interface	VID	Delete
Default	LAN1, LAN3, LAN4, ZyXEL_A2E6, ZyXEL_SSID1, ZyXEL_SSID2, ZyXEL_SSID3	1	
Example	LAN2	3	🗑

The following table describes the fields in this screen.

Table 48 Configuration > Network > Interface Group

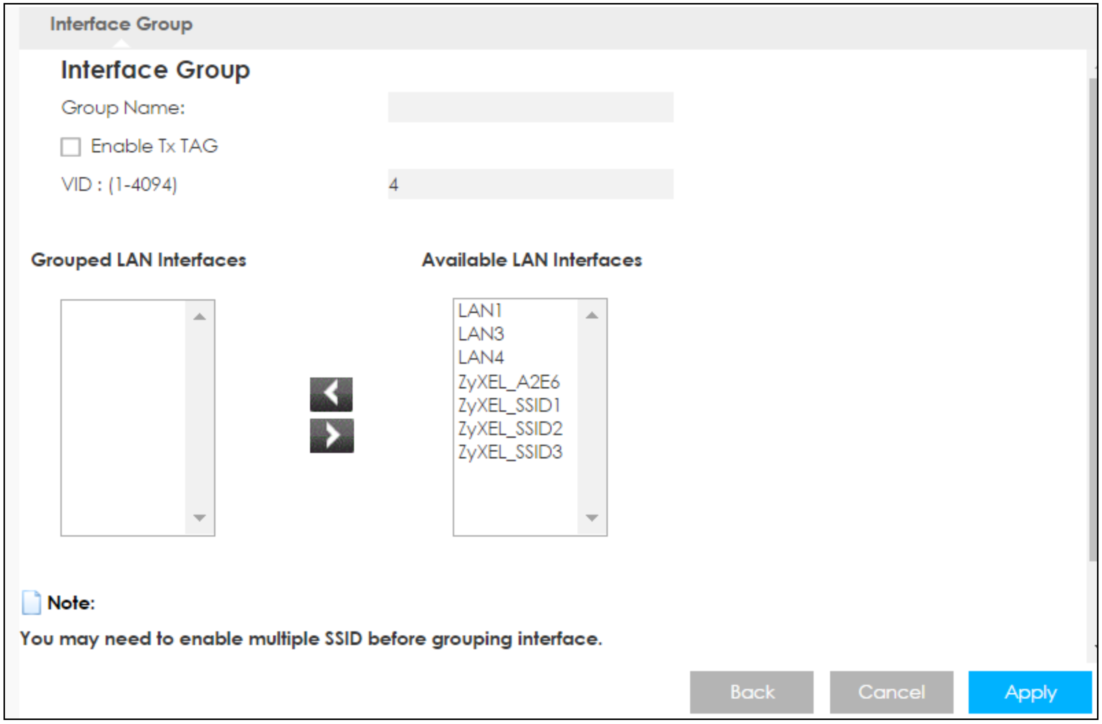
LABEL	DESCRIPTION
Add	Click this button to create a new interface group.
Interface Grouping Rules	
Name	This shows the descriptive name of the group.
LAN Interface	This shows the interface group.
VID	This shows the VLAN ID number (from 0 to 4094) of the interface group.
Modify	Click the **Delete** icon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

13.2.1 Interface Group > Add Screen

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

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

Figure 76 Configuration > Network > Interface Group > Add



Interface Group

Interface Group

Group Name:

□ Enable Tx TAG

VID : (1-4094) 4

Grouped LAN Interfaces

Available LAN Interfaces

LAN1
LAN3
LAN4
ZyXEL_A2E6
ZyXEL_SSID1
ZyXEL_SSID2
ZyXEL_SSID3

Note:

You may need to enable multiple SSID before grouping interface.

The following table describes the fields in this screen.

Table 49 Configuration > Network > Interface Group > Add

LABEL	DESCRIPTION
Group Name	Enter a name to identify this group. You can enter up to 30 characters. You can use letters, numbers, hyphens (-) and underscores (_). Spaces are not allowed.
Enable Tx TAG	Click the check box to set the port to tag or not to tag all outgoing traffic with the VLAN ID.
VID	This shows the VLAN ID number (from 0 to 4094) for traffic through the interfaces in this group. This field is not configurable and the VLAN ID is assigned automatically by the system.
Grouped LAN Interfaces	This shows the LAN port(s) or WLAN interface(s) as a member of the VLAN interface group. Select any interfaces that you don't want and click the right arrow button to remove them from this group.
Available LAN Interfaces	This shows the available LAN interface(s) (Ethernet LAN or Wireless LAN) that can be selected to form a VLAN interface group. Select the interfaces that you want and click the left arrow button to add them to this group.
Back	Click **Back** to quit and return to the previous screen.
Cancel	Click **Cancel** to exit this screen without saving.
Apply	Click **Apply** to save your changes back to the LTE Device.

CHAPTER 14 Firewall

14.1 Overview

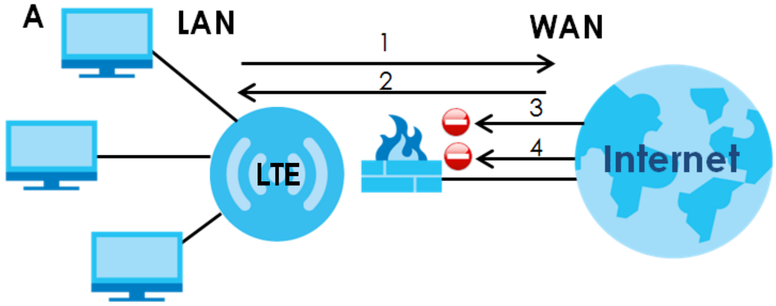
Use these screens to enable and configure the firewall that protects your LTE Device and your LAN from unwanted or malicious traffic.

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 77 Default Firewall Action



14.1.1 What You Can Do

- Use the **General** screen to enable or disable the LTE Device's firewall (Section 14.2 on page 112).
- Use the **Services** screen enable service blocking, enter/delete/modify the services you want to block and the date/time you want to block them (Section 14.3 on page 113).

14.1.2 What You Need To Know

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

About the LTE Device Firewall

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

It is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (click the **General** tab under **Firewall** and then click the **Enable Firewall** check box). The LTE Device's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The LTE Device can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network.

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

The LTE Device 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.

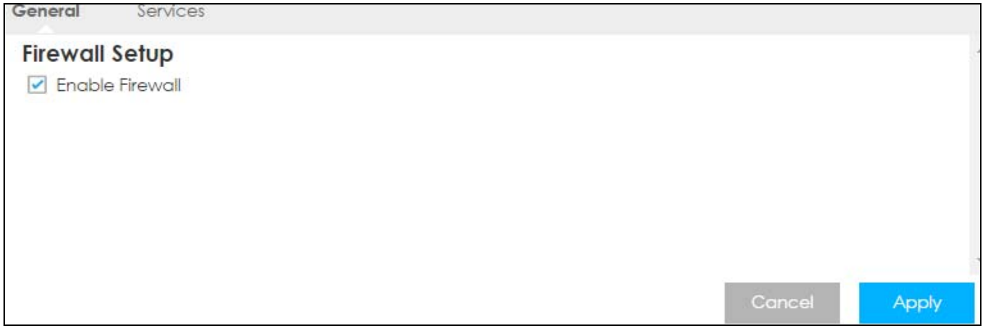
Guidelines For Enhancing Security With Your Firewall

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.

14.2 General Screen

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

Figure 78 Configuration > Security > Firewall > General I



Firewall Setup

☑ Enable Firewall

The following table describes the labels in this screen.

Table 50 Configuration > Security > Firewall > General

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

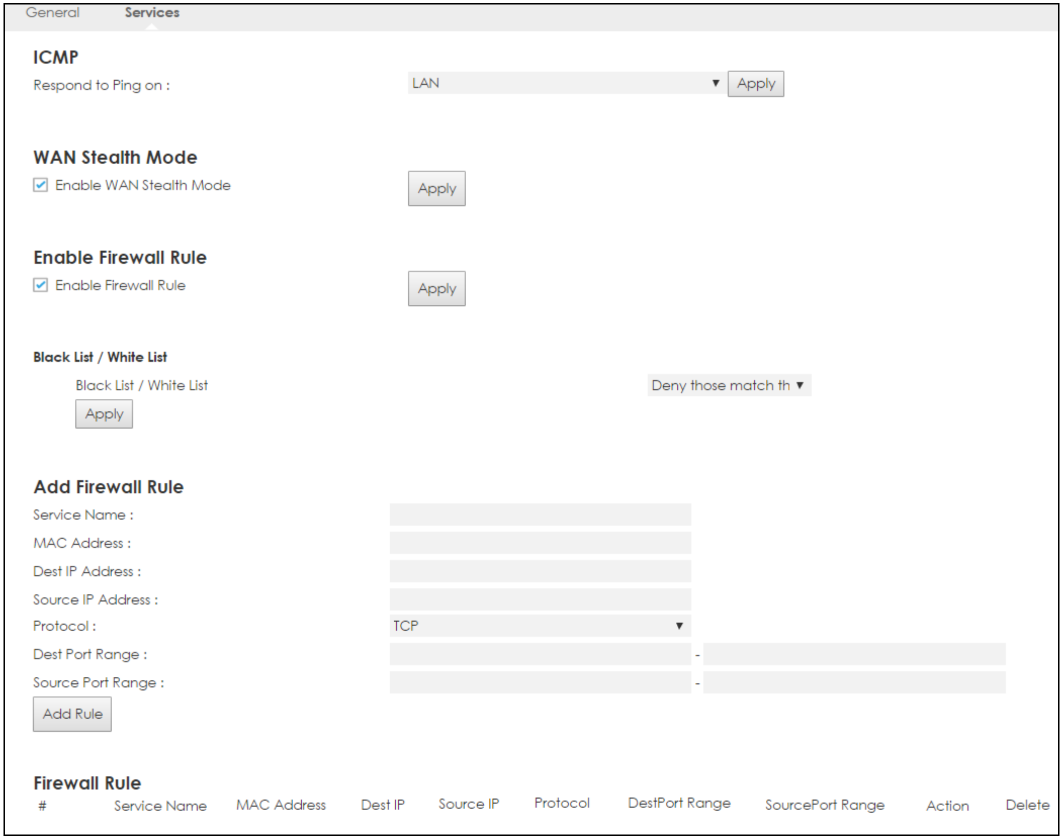
14.3 Services Screen

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

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

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

Figure 79 Configuration > Security > Firewall > Services I



General Services

ICMP

Respond to Ping on : LAN ▾ Apply

WAN Stealth Mode

☑ Enable WAN Stealth Mode Apply

Enable Firewall Rule

☑ Enable Firewall Rule Apply

Black List / White List

Black List / White List Deny those match th ▾

Apply

Add Firewall Rule

Service Name :

MAC Address :

Dest IP Address :

Source IP Address :

Protocol : TCP ▾

Dest Port Range : -

Source Port Range : -

Add Rule

Firewall Rule

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

The following table describes the labels in this screen.

Table 51 Configuration > Security > Firewall > Services

LABEL	DESCRIPTION
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The LTE Device will not respond to any incoming Ping requests when **Disable** is selected. Select **LAN** to reply to incoming LAN Ping requests. Select **WAN** to reply to incoming WAN Ping requests. Otherwise select **LAN&WAN** to reply to all incoming LAN and WAN Ping requests.
Apply	Click **Apply** to save the settings.
WAN Stealth Mode	
Enable WAN Stealth Mode	Select this check box to silently discard the matched packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender.
Apply	Click **Apply** to save the settings.
Enable Firewall Rule	
Enable Firewall Rule	Select this check box to activate the firewall rules that you define (see **Add Firewall Rule** below).
Apply	Click **Apply** to save the settings.
Black List / White List	

Table 51 Configuration > Security > Firewall > Services (continued)

LABEL	DESCRIPTION
Black List / White List	Select **Deny those match the following rules.** to block access to the MAC addresses in the list and allow access to other URLs. Select **Allow those match the following rules.** to allow access to the MAC addresses in the list and block access to other URLs.
Apply	Click **Apply** to save the settings.
Add Firewall Rule	
Service Name	Enter a name that identifies or describes the firewall rule.
MAC Address	Enter the MAC address of the computer for which the firewall rule applies.
Dest IP Address	Enter the IP address of the computer to which traffic for the application or service is entering. The LTE Device applies the firewall rule to traffic initiating from this computer.
Source IP Address	Enter the IP address of the computer that initializes traffic for the application or service. The LTE Device applies the firewall rule to traffic initiating from this computer.
Protocol	Select the protocol (**TCP**, **UDP** or **ICMP**) used to transport the packets for which you want to apply the firewall rule.
Dest Port Range	Enter the port number/range of the destination that define the traffic type, for example TCP port 80 defines web traffic.
Source Port Range	Enter the port number/range of the source that define the traffic type, for example TCP port 80 defines web traffic.
Add Rule	Click **Add** to save the firewall rule.
Firewall Rule	
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.
Service Name	This is a name that identifies or describes the firewall rule.
MAC address	This is the MAC address of the computer for which the firewall rule applies.
Dest IP	This is the IP address of the computer to which traffic for the application or service is entering.
Source IP	This is the IP address of the computer from which traffic for the application or service is initialized.
Protocol	This is the protocol (**TCP**, **UDP** or **ICMP**) used to transport the packets for which you want to apply the firewall rule.
Dest Port Range	This is the port number/range of the destination that define the traffic type, for example TCP port 80 defines web traffic.
Source Port Range	This is the port number/range of the source that define the traffic type, for example TCP port 80 defines web traffic.
Action	**DROP** - Traffic matching the conditions of the firewall rule are stopped.
Delete	Click **Delete** to remove the firewall rule.

See Appendix B on page 183 for commonly used services and port numbers.

CHAPTER 15
Content Filtering

15.1 Overview

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

Keyword Blocking URL Checking

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

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

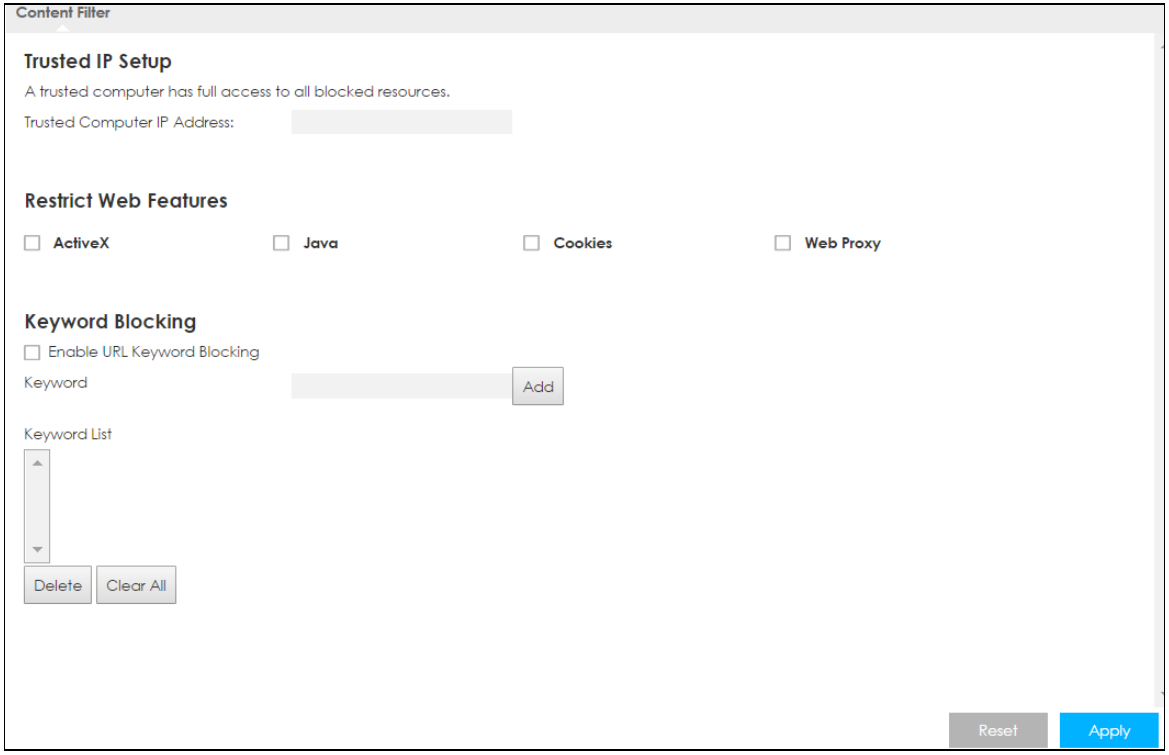
The file path is the characters that come after the first slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the file path is news/pressroom.php.

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

15.2 Content Filter

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

Figure 80 Configuration > Security > Content Filter



Content Filter

Trusted IP Setup

A trusted computer has full access to all blocked resources.

Trusted Computer IP Address:

Restrict Web Features

□ ActiveX □ Java □ Cookies □ Web Proxy

Keyword Blocking

□ Enable URL Keyword Blocking

Keyword

The following table describes the labels in this screen.

Table 52 Configuration > Security > Content Filter

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

Table 52 Configuration > Security > Content Filter (continued)

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

CHAPTER 16
IPv6 Firewall

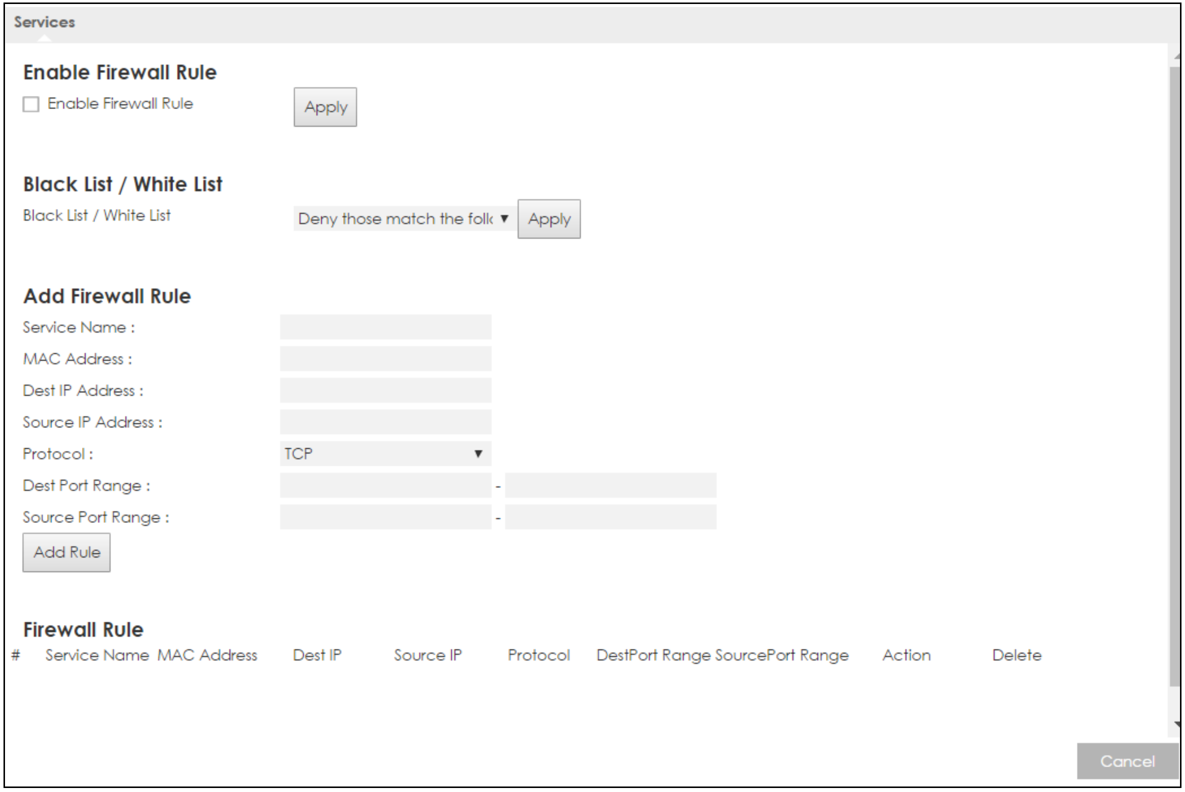
16.1 Overview

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

16.2 IPv6 Firewall Screen

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

Figure 81 Configuration > Security > IPv6 Firewall



□ Enable Firewall Rule

Black List / White List: Deny those match the follc ▾

Protocol : TCP ▾

The following table describes the labels in this screen.

Table 53 Configuration > Security > IPv6 Firewall

LABEL	DESCRIPTION
Enable Firewall Rule	
Enable Firewall Rule	Select this check box to activate the firewall rules that you define (see **Add Firewall Rule** below).

Table 53 Configuration > Security > IPv6 Firewall (continued)

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

CHAPTER 17 SMS

17.1 Overview

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

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

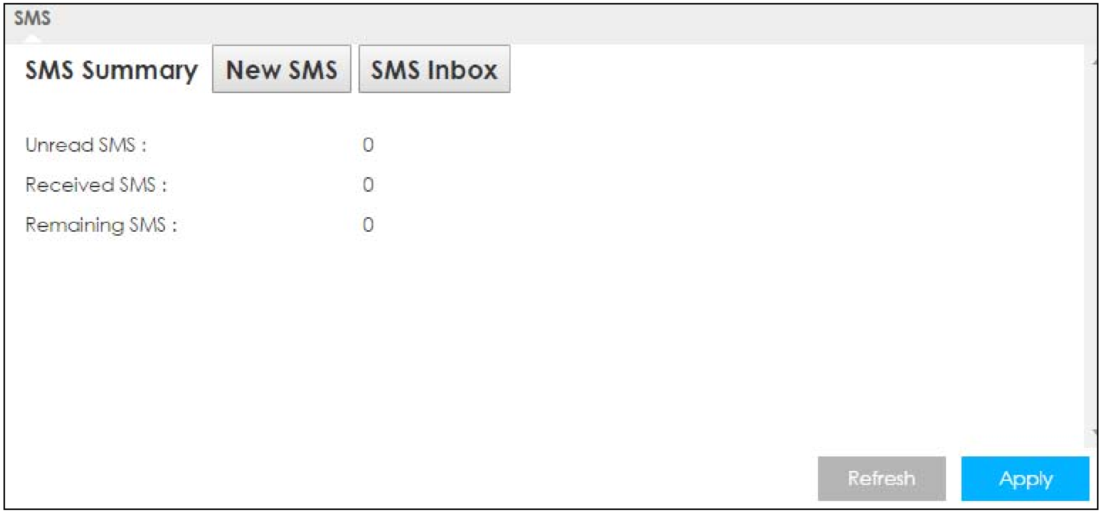
17.1.1 What You Can Do in this Chapter

- Use the **SMS** screen to send new messages and view messages received on the LTE Device (Section 17.2 on page 121).

17.2 SMS Screen

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

Figure 82 Configuration > Application > SMS



Unread SMS : 0
Received SMS : 0
Remaining SMS : 0

The following table describes the labels in this screen.

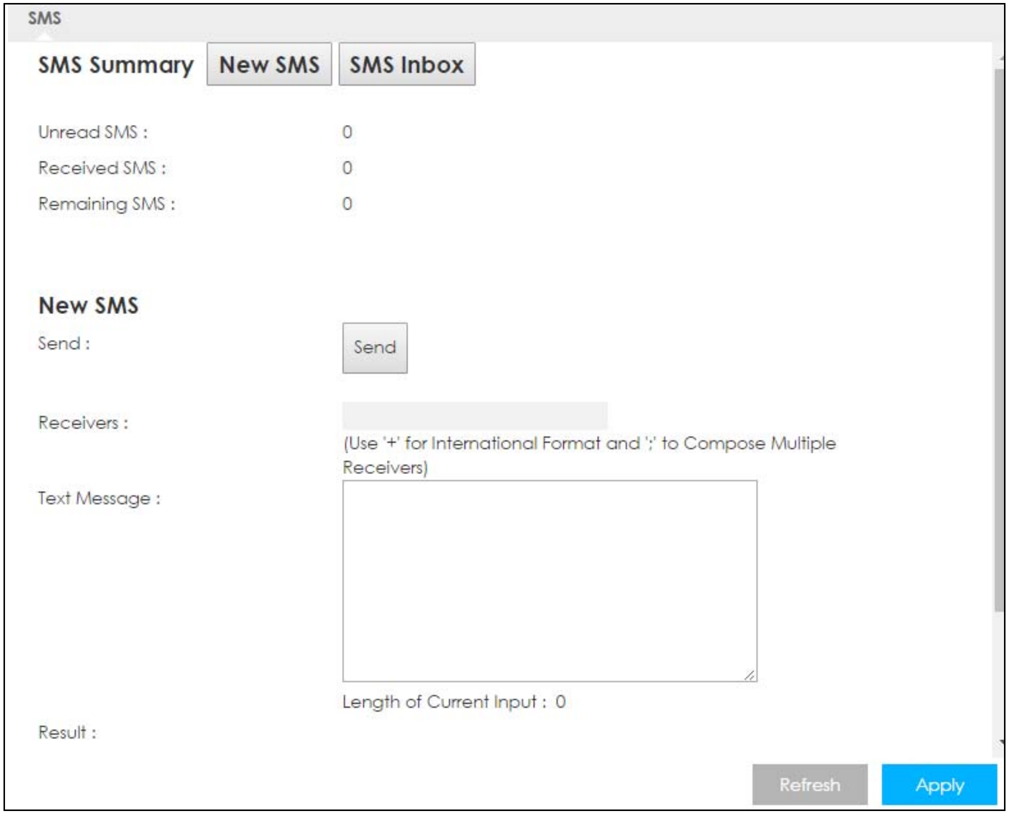
Table 54 Configuration > Application > SMS

LABEL	DESCRIPTION
SMS Summary	Click **New SMS** to display the **New SMS** section. Click **SMS Inbox** to display only the **SMS Inbox List**.
Unread SMS	This shows the number of unread SMS text messages in the SMS in-box.
Received SMS	This shows the number of SMS text messages that the LTE Device received.
Remaining SMS	This shows the number of SMS text messages that are to be sent.

17.2.1 SMS > New SMS

Click the **New SMS** button in the **SMS** screen to open the following screen. Use this screen to create a new SMS text message.

Figure 83 Configuration > Application > SMS > New SMS



SMS

SMS Summary

Unread SMS : 0

Received SMS : 0

Remaining SMS : 0

New SMS

Send :

Receivers :

(Use '+' for International Format and ';' to Compose Multiple Receivers)

Text Message :

Length of Current Input : 0

Result :

The following table describes the labels in this screen.

Table 55 Configuration > Application > SMS > New SMS

LABEL	DESCRIPTION
New SMS	
Send	Click this button to send the new message.
Receivers	Enter the phone number to which you want to send a SMS text message.

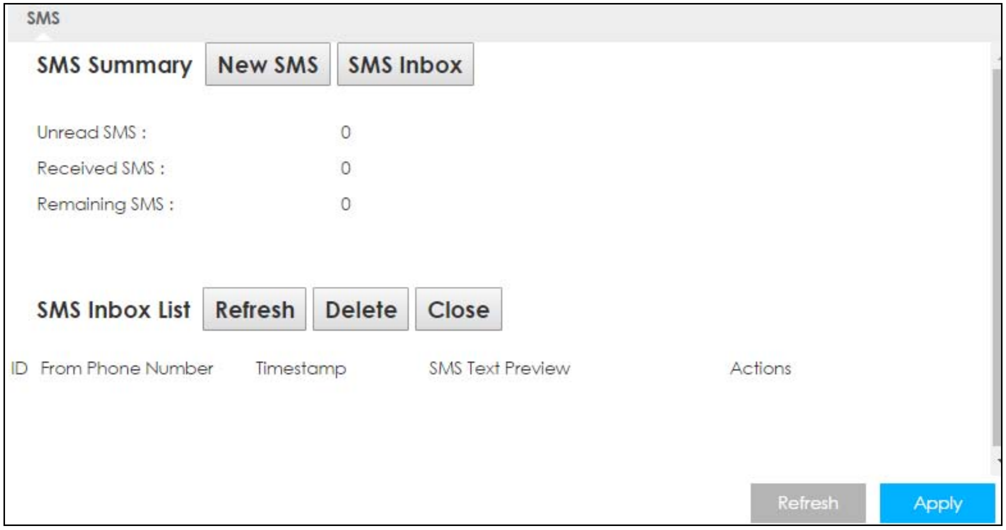
Table 55 Configuration > Application > SMS > New SMS (continued)

LABEL	DESCRIPTION
Text Message	Enter the message content. You can type up to 160 characters in one message. If the message exceeds 160 characters, more than one SMS will be sent. The maximum number of SMS that can be sent is 20 (1400 characters total).
Result	This shows whether the message is sent successfully.
Refresh	Click this button to update the screen.
Apply	Click this button to save your changes to the LTE Device.

17.2.2 SMS > SMS Inbox

Click the **SMS Inbox** button in the **SMS** screen to open the following screen. Use this screen to see the log of the SMS text messages sent.

Figure 84 Configuration > Application > SMS > SMS Inbox



Unread SMS : 0
Received SMS : 0
Remaining SMS : 0

ID From Phone Number Timestamp SMS Text Preview Actions

The following table describes the labels in this screen.

Table 56 Configuration > Application > SMS > SMS Inbox

LABEL	DESCRIPTION
SMS Inbox List	
Refresh	Click this button to update the list.
Delete	Click this button to delete an entry.
Close	Click this button to hide the **SMS Inbox List**.
ID	This field displays the index number of the message.
From Phone Number	This field displays the mobile phone number from which the message is sent.
Timestamp	This field displays the date and time the message was received.
SMS Text Preview	This field displays the content of the message.
Actions	Click the delete icon to remove the message record.
Refresh	Click this button to update the screen.
Apply	Click this button to save your changes to the LTE Device.

CHAPTER 18 Voice over 3G

18.1 Overview

4G only supports all-IP-based packet-switched telephony services. When Voice over 3G (Vo3G) is enabled, the LTE Device supports Circuit Switched FallBack (CSFB) to deliver/receive circuit-switched voice calls and SMS text messages via a 2G/3G mobile network and then goes back to the 4G LTE network to transmit data packets.

With Vo3G, users do not need a SIP account and SIP server to make phone calls over the Internet.

Note: You can enable either VoIP or Vo3G on the LTE Device, but not both at the same time.

Note: Vo3G is only available on the LTE3312-M432.

18.1.1 What You Can Do in this Chapter

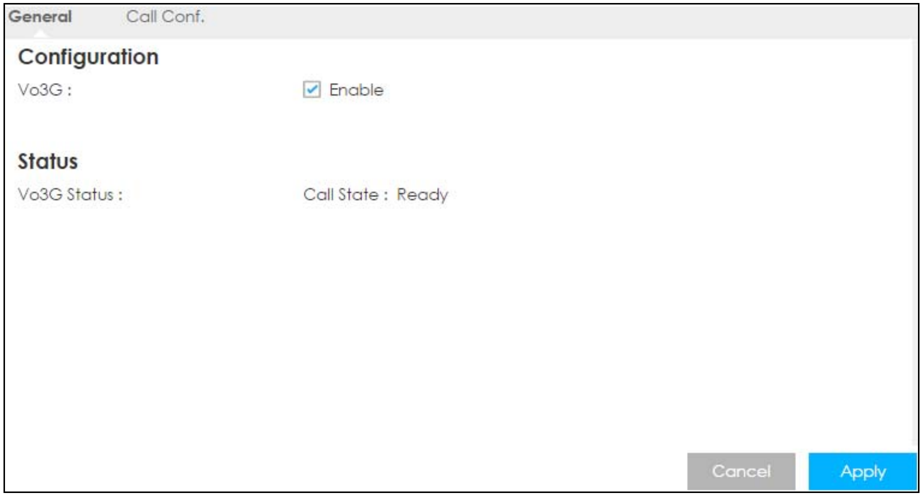
These screens allow you to configure your LTE Device to make phone calls over the Internet and your regular phone line, and to set up the phone you connect to the LTE Device.

- Use the **General** screen to enable Vo3G on the LTE Device (Section 18.2 on page 124).
- Use the **Call Conf.** screen to maintain rules for handling incoming calls (Section 18.3 on page 125).

18.2 Vo3G General Screen

Use this screen to enable Vo3G on the LTE Device. To access this screen, click **Application > Voice over 3G > General**.

Figure 85 Application > Voice over 3G > General



Configuration

Vo3G : ☑ Enable

Status

Vo3G Status : Call State : Ready

The following table describes the labels in this screen.

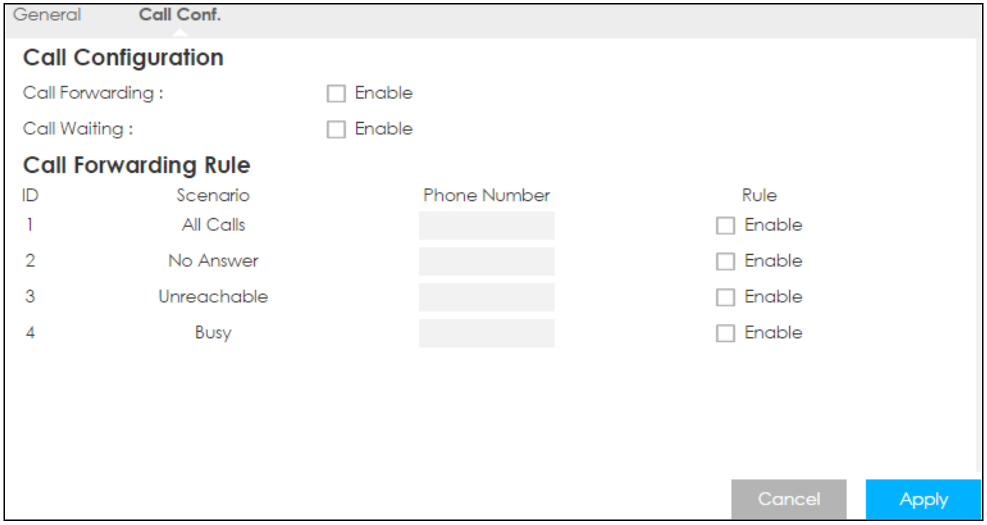
Table 57 Application > Voice over 3G > General

LABEL	DESCRIPTION
Vo3G	Select **Enable** to activate Vo3G on the LTE Device.
Vo3G Status	This shows the current state of the phone call. • **ready**: Voice over 3G (Vo3G) is enabled and the 3G connection is up. • **not ready**: Voice over 3G (Vo3G) is disabled and the 3G connection is down. • **busy**: There is a Vo3G call in progress or the callee's line is busy. • **ringing**: The phone is ringing for an incoming Vo3G call. • **dialing**: The callee's phone is ringing. • **off hook**: The callee hung up or your phone was left off the hook. **N/A** means Voice over 3G (Vo3G) is disabled.
Cancel	Click **Cancel** to start configuring this screen again.
Apply	Click **Apply** to save the settings.

18.3 Call Configuration Screen

Use this screen to maintain rules for handling incoming calls. To access this screen, click **Application > Voice over 3G > Call Conf**.

Figure 86 Application > Voice over 3G > Call Conf.



Call Configuration

Call Forwarding : □ Enable

Call Waiting : □ Enable

Call Forwarding Rule

ID	Scenario	Phone Number	Rule
1	All Calls		□ Enable
2	No Answer		□ Enable
3	Unreachable		□ Enable
4	Busy		□ Enable

The following table describes the labels in this screen.

Table 58 Application > Voice over 3G > Call Conf.

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

CHAPTER 19
Remote Management

19.1 Overview

This chapter provides information on the **Remote Management** screens. Remote Management allows you to manage your LTE Device from a remote location

Remote Management allows you to manage your EMG2926-Q10A from a remote location through the following interfaces:

- LAN and WAN
- LAN only
- WAN only

Note: The LTE Device is managed using the Web Configurator.

19.2 What You Can Do

- Use the **WWW** screen to define the interface/s from which the LTE Device can be managed remotely using the web and specify a secure client that can manage the LTE Device (Section 19.4 on page 128).
- Use the **Remote Management** screen to control through which IP addresses can access the LTE Device (Section 19.5 on page 129).

19.3 What You Need to Know

Remote management over LAN or WAN will not work when:

1. The IP address in the Secured Client IP Address field (Section 19.4 on page 128) does not match the client IP address. If it does not match, the LTE Device will disconnect the session immediately.
2. There is already another remote management session. You may only have one remote management session running at one time.
3. There is a firewall rule that blocks it.

19.3.1 System Timeout

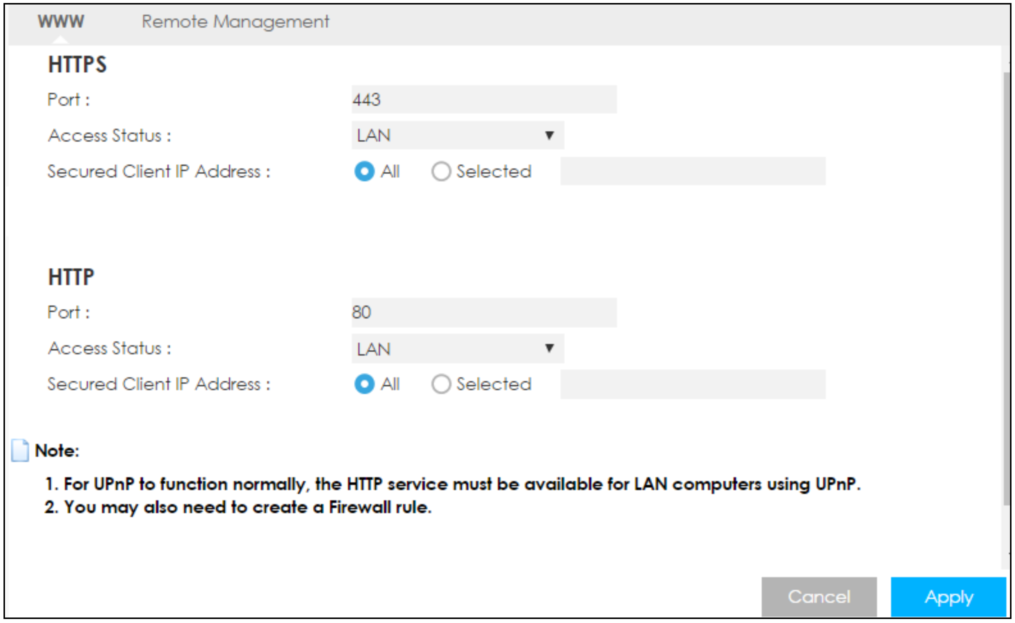
There is a default system management idle timeout of five minutes (three hundred seconds). The LTE Device automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. You can change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

19.4 WWW Screen

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

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

Figure 87 Configuration > Management > Remote MGMT > WWW



HTTPS
Port : 443
Access Status : LAN ▾
Secured Client IP Address : ● All ○ Selected

HTTP
Port : 80
Access Status : LAN ▾
Secured Client IP Address : ● All ○ Selected

Note:
1. For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.
2. You may also need to create a Firewall rule.

The following table describes the labels in this screen.

Table 59 Configuration > Management > Remote MGMT > WWW

LABEL	DESCRIPTION
HTTPS	
Port	You may change the server port number for a HTTPS service if needed. However you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the LTE Device using this HTTPS service.
Secured Client IP Address	Select **All** to allow all computers to access the LTE Device using the HTTPS service. Otherwise, check **Selected** and specify the IP address of the computer that can access the LTE Device.
HTTP	
Port	You may change the server port number for a HTTP service if needed. However you must use the same port number in order to use that service for remote management.

Table 59 Configuration > Management > Remote MGMT > WWW (continued)

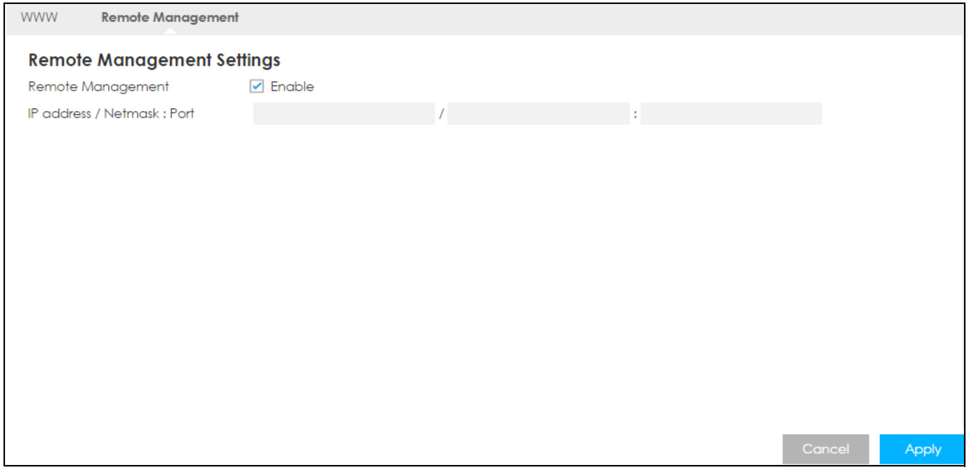
LABEL	DESCRIPTION
Access Status	Select the interface(s) through which a computer may access the LTE Device using this HTTP service. If you activated UPnP, select **WAN** to allow the UPnP traffic to come in from the WAN side successfully.
Secured Client IP Address	Select **All** to allow all computers to access the LTE Device using this HTTP service. Otherwise, check **Selected** and specify the IP address of the computer that can access the LTE Device.
Cancel	Click **Cancel** to exit this screen without saving.
Apply	Click **Apply** to save your customized settings and exit this screen.

19.5 The Remote Management Screen

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

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

Figure 88 Configuration > Management > Remote MGMT > Remote Management



Remote Management Settings

Remote Management ☑ Enable

IP address / Netmask : Port / :

The following table describes the fields in this screen.

Table 60 Configuration > Management > Remote MGMT > Remote Management

LABEL	DESCRIPTION
Remote Management	Select the **Enable** check box to allow access to the LTE Device from the IP address and activate the settings you've made in the **WWW** screen.
IP Address	This is the IP address of a computer that may use to access the LTE Device.
Netmask	This is the subnet mask identifying a computer that may access remotely to the LTE Device.

Table 60 Configuration > Management > Remote MGMT > Remote Management

LABEL	DESCRIPTION
Port	This is the port number that the computer must use to access the LTE Device. If the HTTP Port number was changed to 8080 in the **Configuration > Management > Remote MGMT > WWW** screen, then this computer should use the same number. For example http://1.1.1.1:8080 where 1.1.1.1 is the IP address of the LTE Device.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes back to the LTE Device.

CHAPTER 20 Bandwidth Management

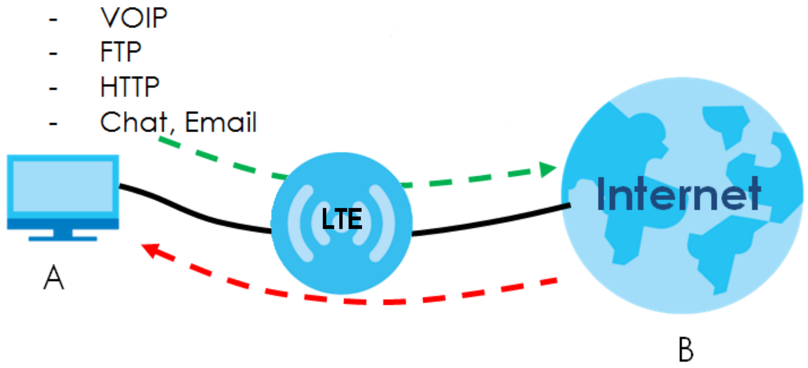
20.1 Overview

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

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

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

Figure 89 Bandwidth Management Example



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

20.2 What You Can Do

- Use the **General** screen to enable bandwidth management and assign bandwidth values (Section 20.4 on page 132).
- Use the **Advanced** screen to configure bandwidth managements rule for the services and applications (Section 20.5 on page 133).

20.3 What You Need To Know

The sum of the bandwidth allotments that apply to the WAN interface (LAN to WAN, WLAN to WAN) must be less than or equal to the upstream bandwidth that you configure in the **Bandwidth Management > General** screen (Section 20.5 on page 133).

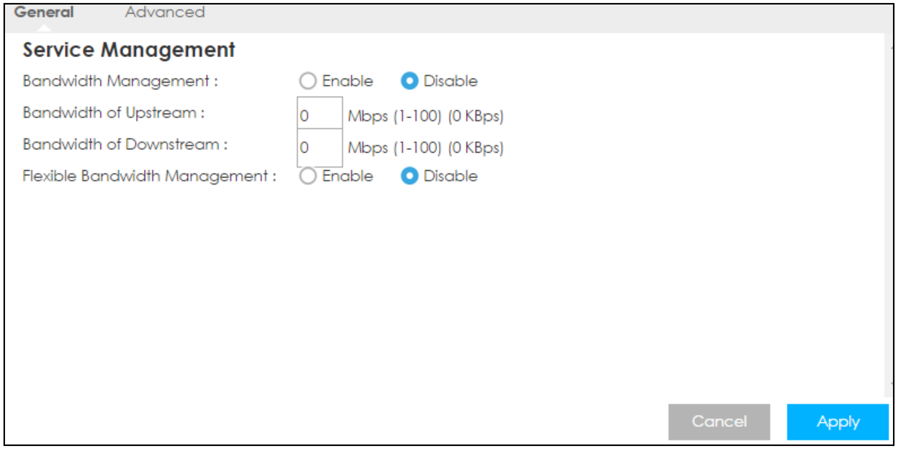
The sum of the bandwidth allotments that apply to the LAN interface (WAN to LAN, WAN to WLAN) must be less than or equal to the downstream bandwidth that you configure in the **Bandwidth Management > General** screen Section 20.5 on page 133.

20.4 General Screen

Use this screen to have the LTE Device apply bandwidth management.

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

Figure 90 Configuration > Management > Bandwidth MGMT > General



Service Management

Bandwidth Management : ○ Enable ● Disable

Bandwidth of Upstream : 0 Mbps (1-100) (0 KBps)

Bandwidth of Downstream : 0 Mbps (1-100) (0 KBps)

Flexible Bandwidth Management : ○ Enable ● Disable

The following table describes the labels in this screen.

Table 61 Configuration > Management > Bandwidth MGMT > General

LABEL	DESCRIPTION
Bandwidth Management	This field allows you to have LTE Device apply bandwidth management. Enable bandwidth management to give traffic that matches a bandwidth rule priority over traffic that does not match a bandwidth rule. Enabling bandwidth management also allows you to control the maximum or minimum amounts of bandwidth that can be used by traffic that matches a bandwidth rule.
Bandwidth of Upstream	Specify the total amount of bandwidth that you want to dedicate to uplink traffic. The recommendation is to set this to match the actual upstream data rate. This is traffic from LAN/WLAN to WAN.
Bandwidth of Downstream	Specify the total amount of bandwidth that you want to dedicate to downlink traffic. The recommendation is to set this to match the actual downstream data rate. This is traffic from WAN to LAN/WLAN.

Table 61 Configuration > Management > Bandwidth MGMT > General (continued)

LABEL	DESCRIPTION
Flexible Bandwidth Management	Select **Enable** to use up to 100% of the configured bandwidth. If you select **Disable**, you can only use up to 33% of the configured bandwidth.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Apply	Click **Apply** to save your customized settings.

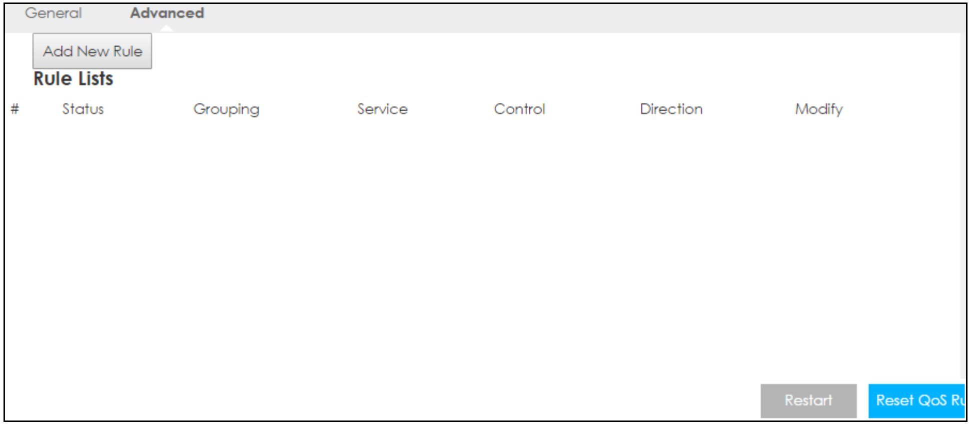
20.5 Advanced Screen

Use this screen to configure bandwidth management rules for the pre-defined services or applications.

You can also use this screen to configure bandwidth management rule for other services or applications that are not on the pre-defined list of LTE Device. Additionally, you can define the IP addresses and port for a service or application.

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

Figure 91 Management > Bandwidth Management > Advanced



The following table describes the labels in this screen.

Table 62 Management > Bandwidth Management > Advanced

LABEL	DESCRIPTION
Add New Rule	Click this to open a screen where you can create a new bandwidth management rule for a service or application.
Rule List	
#	This is the number of an individual bandwidth management rule.
Status	This field indicates whether the rule is active (yellow bulb) or not (gray bulb).
Grouping	This field displays the IP address or a range of IP addresses of the destination computer for whom this rule applies.
Service	This field displays the protocol and port used for the service.
Control	This field displays whether the maximum/minimum bandwidth allowed or a priority level is specified in the rule.
Direction	These read-only labels represent the physical interfaces. Bandwidth management applies to all traffic flowing out of the router through the interface, regardless of the traffic's source.

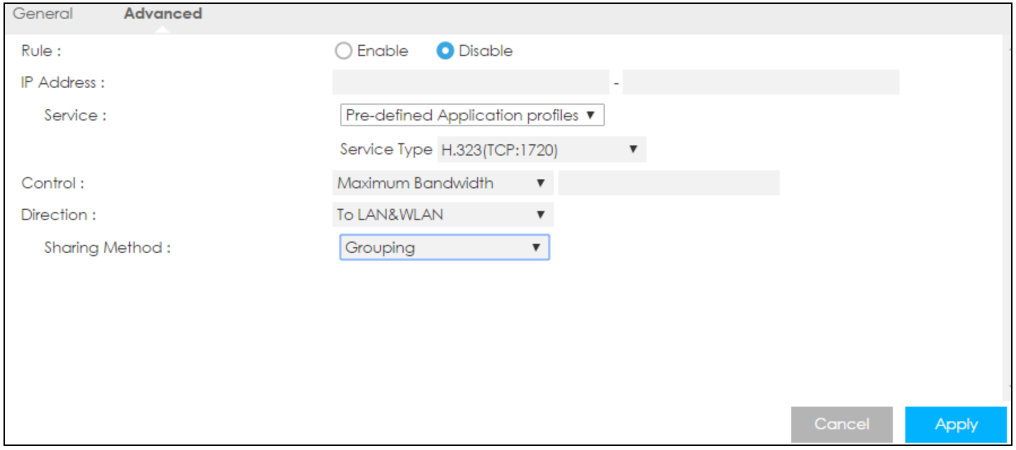
Table 62 Management > Bandwidth Management > Advanced (continued)

LABEL	DESCRIPTION
Modify	Click the remove icon to delete the rule.
Restart	Click this button to begin configuring this screen afresh.
Reset QoS Rule	Click this button to remove all bandwidth management rules.

20.5.1 Add Bandwidth management Rule

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

Figure 92 Bandwidth Management Rule Configuration: Application List



Rule : ○ Enable ● Disable

IP Address : -

Service : Pre-defined Application profiles ▼

Service Type H.323(TCP:1720) ▼

Control : Maximum Bandwidth ▼

Direction : To LAN&WLAN ▼

Sharing Method : Grouping ▼

The following table describes the labels in this screen.

Table 63 Bandwidth Management Rule Configuration: Application List

LABEL	DESCRIPTION
Rule	Select **Enable** to turn on the bandwidth management rule. Otherwise, select **Disable**.
IP Address	Enter the IP address or a range of IP addresses of the destination computer for whom this rule applies.
Service	Select **Service Port** and manually enter the port number(s) that defines the traffic type, for example TCP port 80 defines web traffic. Select **Pre-defined Application profiles** to configure a bandwidth management rule for a pre-defined service or application.
Protocol	If you set **Service** to **Service Port**, select the protocol (**TCP**, or **UDP**) used for the service.
Service Type	If you set **Service** to **Pre-defined Application profiles**, select the name of the service to which the LTE Device applies the bandwidth management rule.
Control	Select **Maximum Bandwidth** or **Minimum Bandwidth** and specify the maximum or minimum bandwidth allowed for the rule in **KBps** (kilobytes per second) or **MBps** (megabytes per second). Otherwise, select **Priority** and enter a priority level (from 1 to 7) for traffic that matches this rule.
Direction	Select **To LAN&WLAN** to apply the rule to traffic from WAN to LAN and WLAN. Select **To WAN** to apply the rule to traffic from LAN/WLAN to WAN. Select **Both** to apply the rule to traffic traveling in either direction.

Table 63   Bandwidth Management Rule Configuration: Application List (continued)

LABEL	DESCRIPTION
Sharing Method	This field is available only when you set **Control** to **Maximum Bandwidth** or **Minimum Bandwidth**. Select **Grouping** to Select **Single** to
Cancel	Click **Cancel** to exit this screen without saving.
Apply	Click **Apply** to save your customized settings.

See Appendix B on page 183 for commonly used services and port numbers.

CHAPTER 21 Universal Plug-and-Play (UPnP)

21.1 Overview

This chapter introduces the UPnP feature in the web configurator.

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

21.2 What You Need to Know

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

21.2.1 NAT Traversal

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

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

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

See the NAT chapter for more information on NAT.

21.2.2 Cautions with UPnP

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

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

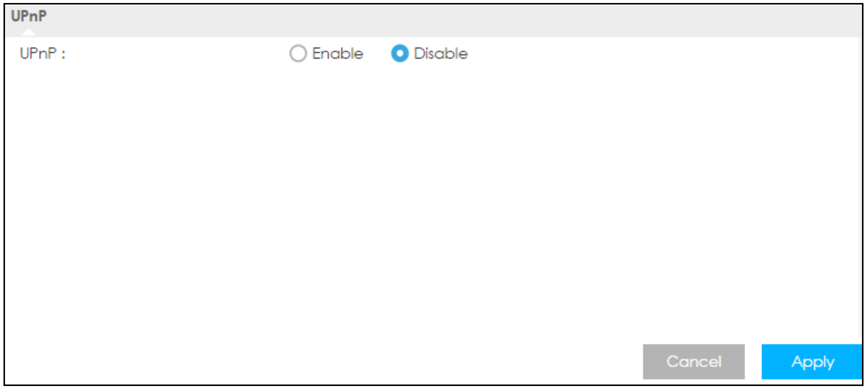
All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

21.3 UPnP Screen

Use this screen to enable UPnP on your LTE Device.

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

Figure 93 Configuration > Management > UPnP



UPnP

UPnP : ○ Enable ● Disable

The following table describes the fields in this screen.

Table 64 Configuration > Management > UPnP

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

21.4 Technical Reference

The sections show examples of using UPnP.

21.4.1 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the LTE Device.

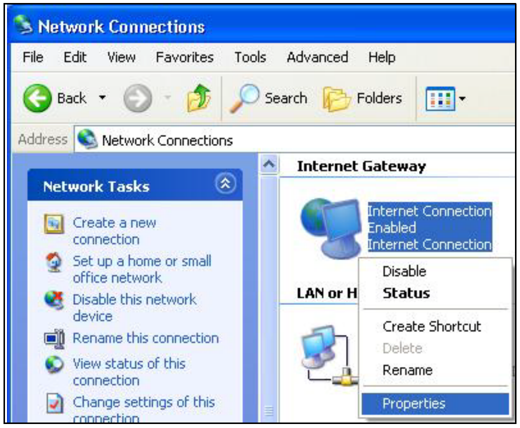
Make sure the computer is connected to a LAN port of the LTE Device. Turn on your computer and the LTE Device.

21.4.1.1 Auto-discover Your UPnP-enabled Network Device

1 Click **start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

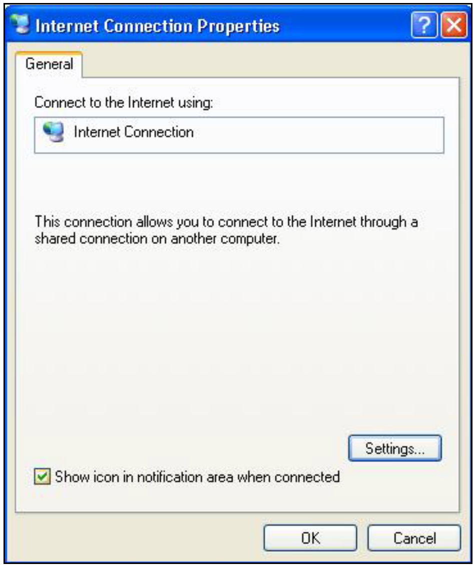
2 Right-click the icon and select **Properties**.

Figure 94 Network Connections



3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

Figure 95 Internet Connection Properties



Connect to the Internet using:

Internet Connection

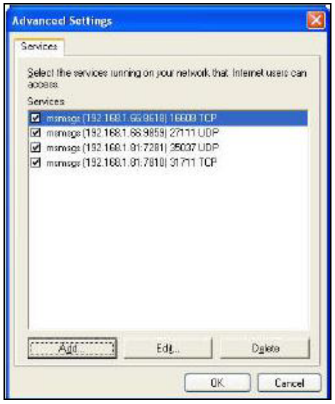
This connection allows you to connect to the Internet through a shared connection on another computer.

Settings...

☑ Show icon in notification area when connected

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

Figure 96 Internet Connection Properties: Advanced Settings

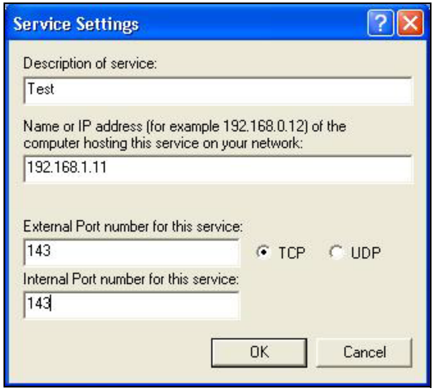


Select the services running on your network that Internet users can access.

Services

- ☑ msmsgs (192.168.1.66:8618) 16608 TCP
- ☑ msmsgs (192.168.1.66:9859) 27111 UDP
- ☑ msmsgs (192.168.1.81:7281) 35037 UDP
- ☑ msmsgs (192.168.1.81:7810) 31711 TCP

Figure 97 Internet Connection Properties: Advanced Settings: Add



Description of service: Test

Name or IP address (for example 192.168.0.12) of the computer hosting this service on your network: 192.168.1.11

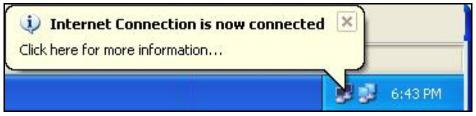
External Port number for this service: 143 ● TCP ○ UDP

Internal Port number for this service: 143

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

5 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

Figure 98 System Tray Icon

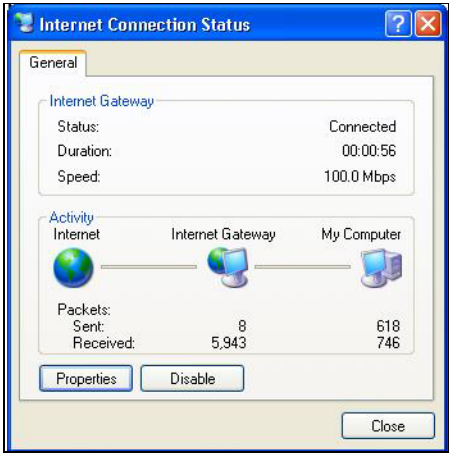


Internet Connection is now connected

Click here for more information...

6 Double-click on the icon to display your current Internet connection status.

Figure 99 Internet Connection Status



Internet Gateway

Status: Connected

Duration: 00:00:56

Speed: 100.0 Mbps

Activity

	Internet	Internet Gateway	My Computer
Packets:			
Sent:		8	618
Received:		5,943	746

21.4.2 Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the LTE Device without finding out the IP address of the LTE Device first. This comes helpful if you do not know the IP address of the LTE Device.

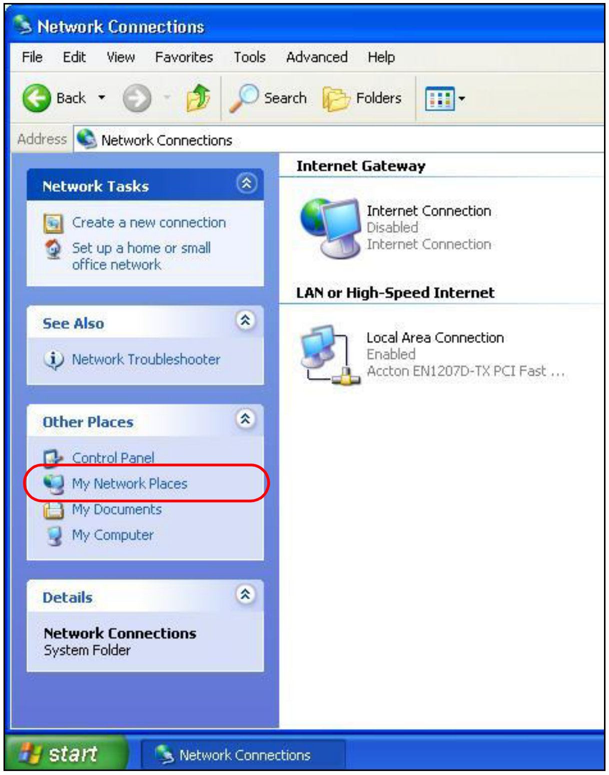
Follow the steps below to access the web configurator.

1 Click **Start** and then **Control Panel**.

2 Double-click **Network Connections**.

3 Select **My Network Places** under **Other Places**.

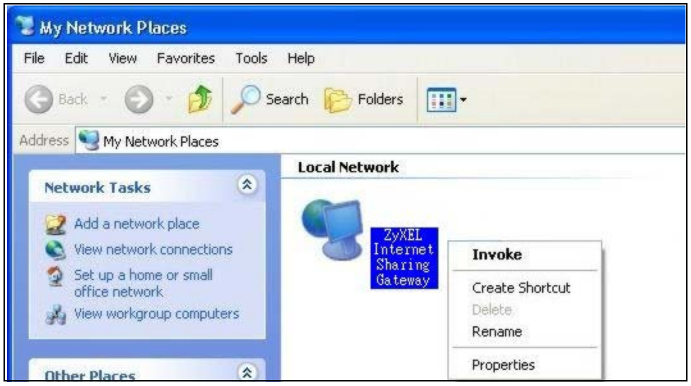
Figure 100 Network Connections



4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

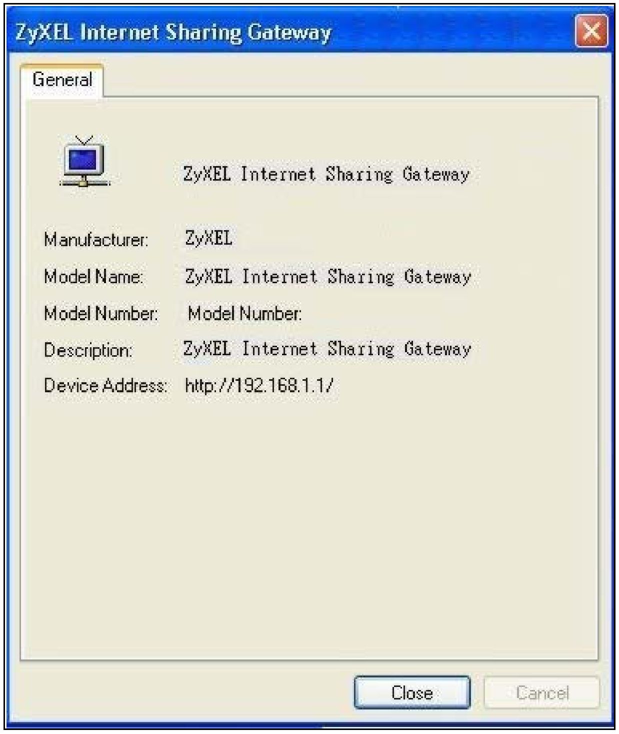
5 Right-click on the icon for your LTE Device and select **Invoke**. The web configurator login screen displays.

Figure 101 Network Connections: My Network Places



6 Right-click on the icon for your LTE Device and select **Properties**. A properties window displays with basic information about the LTE Device.

Figure 102 Network Connections: My Network Places: Properties: Example



ZyXEL Internet Sharing Gateway

ZyXEL Internet Sharing Gateway

Manufacturer: ZyXEL

Model Name: ZyXEL Internet Sharing Gateway

Model Number: Model Number:

Description: ZyXEL Internet Sharing Gateway

Device Address: http://192.168.1.1/

CHAPTER 22
TR-069

22.1 Overview

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

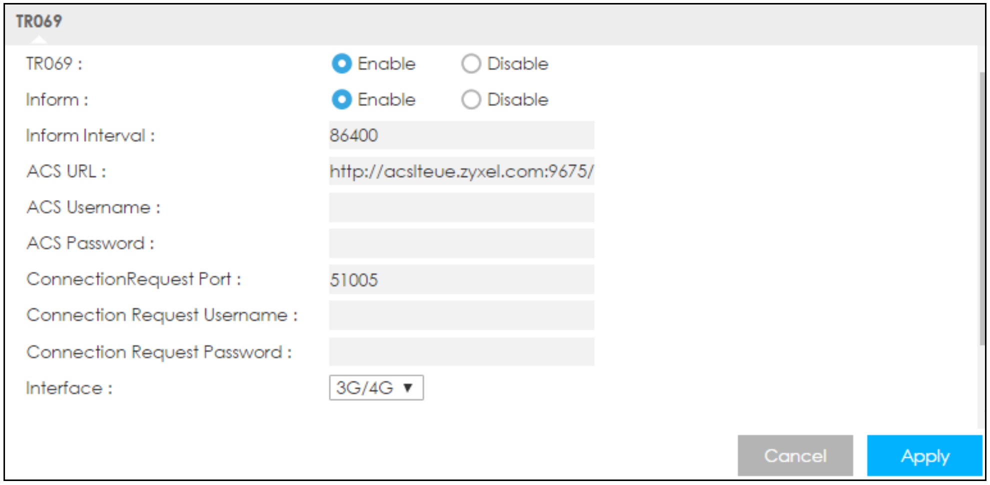
22.2 TR-069 Screen

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

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

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

Figure 103 Management > TR-069



TR069

TR069 :	● Enable ○ Disable
Inform :	● Enable ○ Disable
Inform Interval :	86400
ACS URL :	http://acslteue.zyxel.com:9675/
ACS Username :	
ACS Password :	
ConnectionRequest Port :	51005
Connection Request Username :	
Connection Request Password :	
Interface :	3G/4G ▼

The following table describes the fields in this screen.

Table 65 Maintenance > TR-069 Client

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

CHAPTER 23 Maintenance

23.1 Overview

This chapter provides information on the **Maintenance** screens.

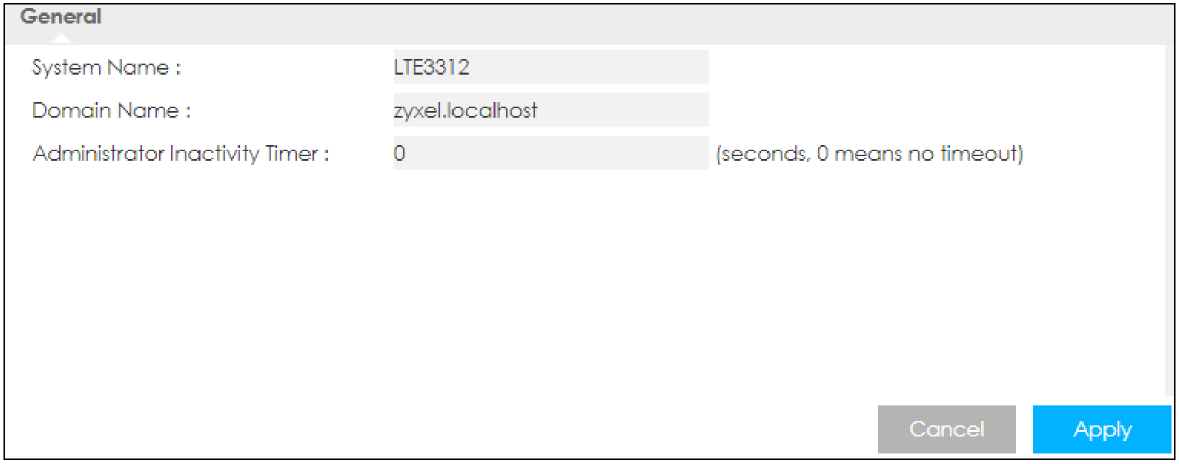
23.2 What You Can Do

- Use the **General** screen to set the timeout period of the management session (Section 23.3 on page 145).
- Use the **Account** screen to change your LTE Device's system password (Section 23.4 on page 146).
- Use the **Time** screen to change your LTE Device's time and date (Section 23.5 on page 147).
- Use the **Firmware Upgrade** screen to upload firmware to your LTE Device (Section 23.6 on page 149).
- Use the **Module Upgrade** screen to upload firmware to your LTE module (Section 23.7 on page 150).
- Use the **Backup/Restore** screen to view information related to factory defaults, backup configuration, and restoring configuration (Section 23.8 on page 151).
- Use the **Restart** screen to reboot the LTE Device without turning the power off (Section 23.9 on page 152).

23.3 General Screen

Use this screen to set the management session timeout period. Click **Maintenance** > **General**. The following screen displays.

Figure 104 Maintenance > General



General

System Name :	LTE3312
Domain Name :	zyxel.localhost
Administrator Inactivity Timer :	0 (seconds, 0 means no timeout)

The following table describes the labels in this screen.

Table 66 Maintenance > General

LABEL	DESCRIPTION
System Name	System Name is a unique name to identify the LTE Device in an Ethernet network.
Domain Name	Enter the domain name you want to give to the LTE Device.
Administrator Inactivity Timer	Type how many minutes a management session can be left idle before the session times out. The default is 300 seconds. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Cancel	Click **Cancel** to begin configuring this screen afresh.
Apply	Click **Apply** to save your changes back to the LTE Device.

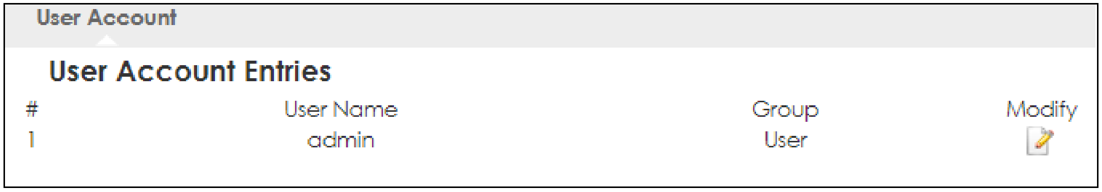
23.4 Account Screen

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

If you forget your LTE Device's password (or IP address), you will need to reset the device. See Section 23.9 on page 152 for details.

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

Figure 105 Maintenance > Account



User Account Entries

#	User Name	Group	Modify
1	admin	User	✎

The following table describes the labels in this screen.

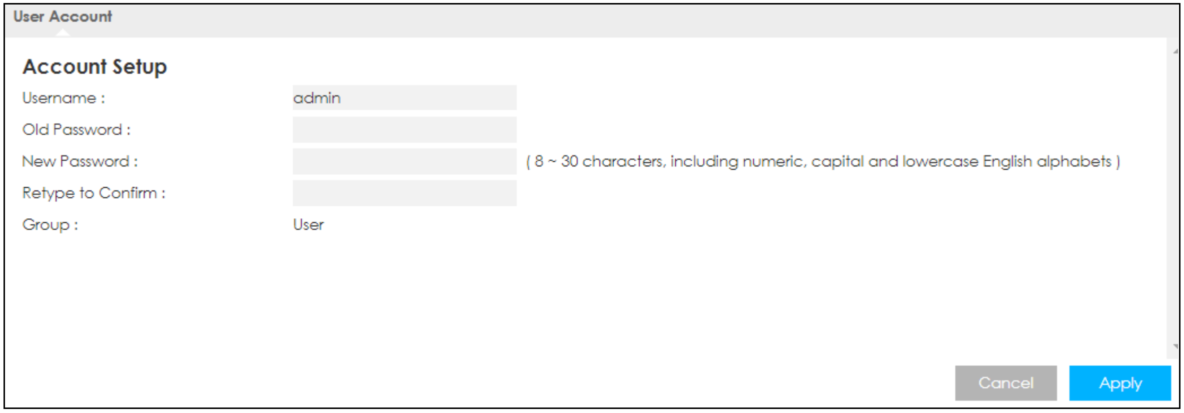
Table 67 Maintenance > Account

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

23.4.1 Edit a User Account

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

Figure 106 Maintenance > Account > Edit



User Account

Account Setup

Username : admin

Old Password :

New Password : (8 ~ 30 characters, including numeric, capital and lowercase English alphabets)

Retype to Confirm :

Group : User

The following table describes the labels in this screen.

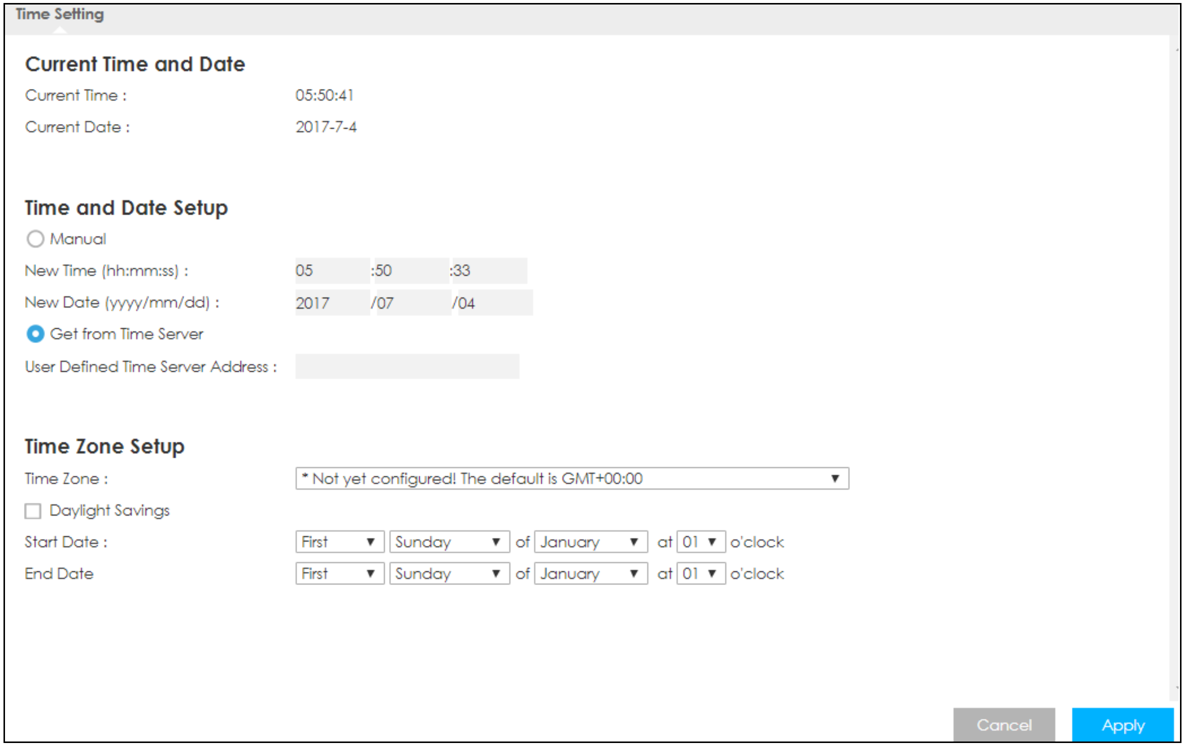
Table 68 Maintenance > Account > Edit

LABEL	DESCRIPTION
Username	Enter a descriptive name for the user account. The user name can be up to 15 alphanumeric characters (0-9, A-Z, a-z, -, _ with no spaces).
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password from 8 to 30 case-sensitive keyboard characters. Make sure you include a number, lowercase, and uppercase English letter. Also, these special characters "/*.,)" are not allowed in a password. Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Type the new password again in this field.
Group	This shows the type of login account.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Apply	Click **Apply** to save your changes back to the LTE Device.

23.5 Time Setting Screen

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

Figure 107 Maintenance > Time



Time Setting

Current Time and Date

Current Time : 05:50:41

Current Date : 2017-7-4

Time and Date Setup

○ Manual

New Time (hh:mm:ss) : 05 :50 :33

New Date (yyyy/mm/dd) : 2017 /07 /04

● Get from Time Server

User Defined Time Server Address :

Time Zone Setup

Time Zone : * Not yet configured! The default is GMT+00:00 ▼

□ Daylight Savings

Start Date : First ▼ Sunday ▼ of January ▼ at 01 ▼ o'clock

End Date First ▼ Sunday ▼ of January ▼ at 01 ▼ o'clock

The following table describes the labels in this screen.

Table 69 Maintenance > Time

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

Table 69 Maintenance > Time (continued)

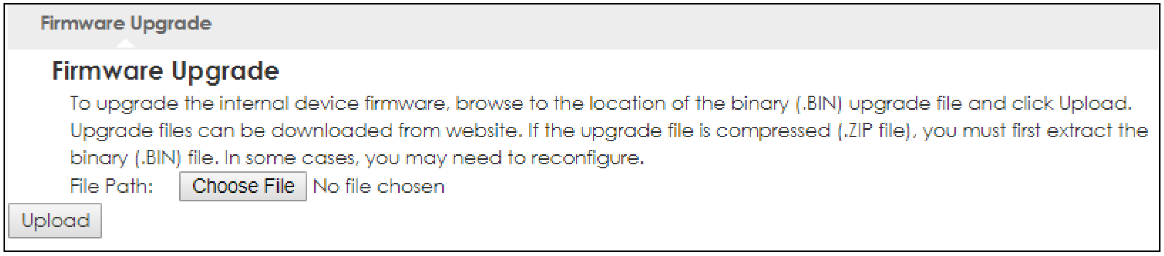
LABEL	DESCRIPTION
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Daylight Savings**. The **at** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and select **2** in the **at** 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 **at** field depends on your time zone. In Germany for instance, you would select 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Daylight Savings**. The **at** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and select 2 in the **at** 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 **at** field depends on your time zone. In Germany for instance, you would select 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Cancel	Click **Cancel** to begin configuring this screen afresh.
Apply	Click **Apply** to save your changes back to the LTE Device.

23.6 Firmware Upgrade Screen

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

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

Figure 108 Maintenance > Firmware Upgrade



Firmware Upgrade

Firmware Upgrade

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

File Path: Choose File No file chosen

Upload

The following table describes the labels in this screen.

Table 70 Maintenance > Firmware Upgrade

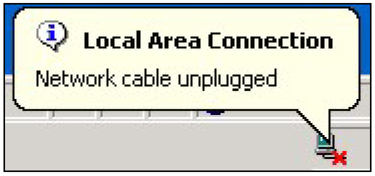
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Choose File** to find it.
Choose File	Click **Choose File** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click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

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

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

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

Figure 109 Network Temporarily Disconnected



Local Area Connection

Network cable unplugged

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

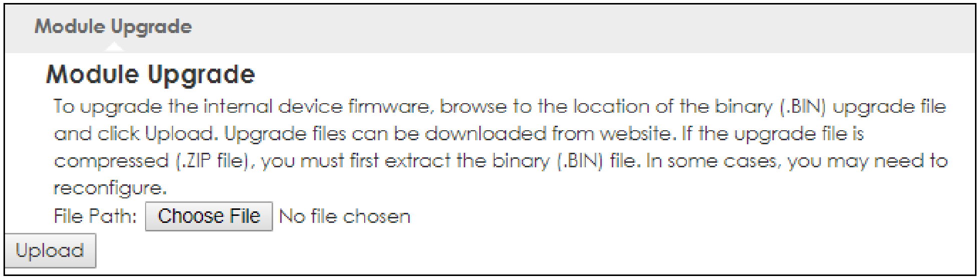
If the upload was not successful, an error message appears. Click **Return** to go back to the **Firmware Upgrade** screen.

23.7 Module Upgrade Screen

You only need to upgrade firmware to the LTE module for LTE enhancements when a notice is released on the Zyxel website. If you see a notice, download the file to your computer and unzip it if necessary.

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

Figure 110 Maintenance > Module Upgrade



Module Upgrade

Module Upgrade

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

File Path: Choose File No file chosen

The following table describes the labels in this screen.

Table 71 Maintenance > Module Upgrade

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

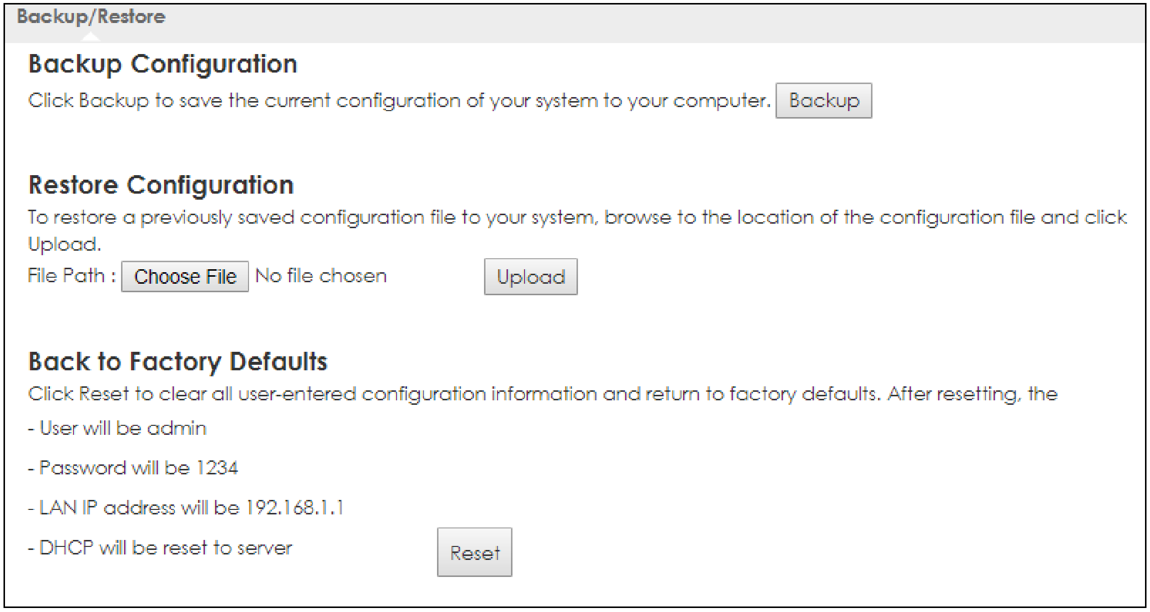
23.8 Configuration Backup/Restore Screen

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

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

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

Figure 111 Maintenance > Backup/Restore



Backup/Restore

Backup Configuration

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

Restore Configuration

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.

File Path :

Back to Factory Defaults

Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the

- User will be admin
- Password will be 1234
- LAN IP address will be 192.168.1.1
- DHCP will be reset to server

The following table describes the labels in this screen.

Table 72 Maintenance > Backup/Restore

LABEL	DESCRIPTION
Backup	Click **Backup** to save the LTE Device's current configuration to your computer.
File Path	Type in the location of the file you want to upload in this field or click **Choose File** to find it.
Choose File	Click **Choose File** to find the file you want to upload.

Table 72 Maintenance > Backup/Restore (continued)

LABEL	DESCRIPTION
Upload	Click **Upload** to begin the upload process. Note: Do not turn off the LTE Device while configuration file upload is in progress. After you see a "configuration upload successful" screen, you must then wait one minute before logging into the LTE Device again. The LTE Device automatically restarts in this time causing a temporary network disconnect. If you see an error screen, click Back to return to the Backup/Restore screen.
Reset	Pressing the **Reset** button in this section clears all user-entered configuration information and returns the LTE Device to its factory defaults. You can also press the **RESET** button on the rear panel to reset the factory defaults of your LTE Device. Refer to the chapter about introducing the Web Configurator for more information on the **RESET** button.

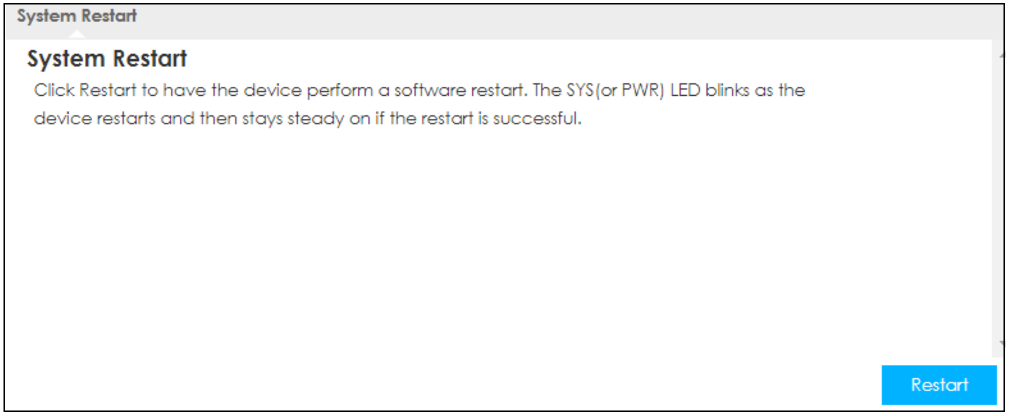
Note: If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default LTE Device IP address (192.168.1.1). See Appendix A on page 158 for details on how to set up your computer's IP address.

23.9 Restart Screen

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

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

Figure 112 Maintenance > Restart



System Restart

Click Restart to have the device perform a software restart. The SYS(or PWR) LED blinks as the device restarts and then stays steady on if the restart is successful.

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

CHAPTER 24
Troubleshooting

24.1 Overview

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

- Power, Hardware Connections, and LEDs
- LTE Device Access and Login
- Internet Access
- WiFi Connections

24.2 Power, Hardware Connections, and LEDs

The LTE Device does not turn on. None of the LEDs turn on.

1. Make sure you are using the power adaptor or cord included with the LTE Device.
2. Make sure the power adaptor or cord is connected to the LTE Device and plugged in to an appropriate power source. Make sure the power source is turned on.
3. Disconnect and re-connect the power adaptor or cord to the LTE Device.
4. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.3.2 on page 16.
2. Check the hardware connections. See the Quick Start Guide.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Disconnect and re-connect the power adaptor to the LTE Device.
5. If the problem continues, contact the vendor.

The **Battery** LED is alternating between green and amber.

If the **Battery** LED is alternating between green and amber, the battery installed in the LTE Device has one of the following problems. If they are not solved, the LTE Device and other devices connected to it could be damaged. See the LED section for more information.

A wrong type of battery is being used or the battery is damaged.

1 Make sure you're using the correct type of battery.

2 Inspect your battery for damage. Contact the vendor to replace the damaged battery.

The battery was removed while charging.

Install the battery back to the LTE Device to charge. If you remove the charging battery, its battery life could be shortened.

The battery temperature is too high or too low.

1 Remove the battery from the LTE Device, and wait for it cool down or warm up.

2 If the battery is overheated, make sure the LTE Device is not placed in an enclosed space, nor on a very soft surface, such as a bed or sofa. Insufficient airflow could cause ventilation problems to the LTE Device.

3 Make sure your operating environment of the LTE Device is within the recommended ambient temperature range. If not, relocate the LTE Device to a cooler or warmer place.

I don't know how to charge the battery.

1 Insert the battery in the LTE Device.

2 Use the included power adaptor to connect the LTE Device to an appropriate power outlet.

1 Check the Battery LED. If it's blinking amber, it means the battery is charging. See the LED section for more information.

24.3 LTE Device Access and Login

I don't know the IP address of my LTE Device.

1 The default IP address of the LTE Device is **192.168.1.1**.

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

3 Reset your LTE Device to change all settings back to their default.

I forgot the password.

1 If you forget your password or IP address, or you cannot access the Web Configurator, you can use the **RESET** button at the back of the LTE Device 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".

2 Make sure the POWER LED is on.

3 Press the **RESET** button for five seconds to set the LTE Device back to its factory-default configurations.

4 Press the **RESET** button for two seconds to restart the LTE Device.

I cannot see or access the **Login** screen in the Web Configurator.

1 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled. See your browser help.

2 Make sure you log into the Web Configurator from the LAN and that your computer is in the same subnet as the LTE Device when remote management service is disabled. If remote management is enabled, make sure you log in from the WAN with a specific IP address.

3 Reset the device to its factory defaults, and try to access the LTE Device with the default IP address. See the Troubleshooting chapter for more information.

4 If the problem continues, contact the network administrator or vendor.

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

1 Make sure you have entered the user name and password correctly. The default user name is **admin** and the default password is **1234**. This field is 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 5 minutes.

3 Disconnect and re-connect the power adaptor or cord to the LTE Device.

4 If this does not work, you have to reset the device to its factory defaults. See the Troubleshooting chapter for more information.

24.4 Internet Access

I cannot access the Internet.

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

2 Make sure your mobile access information (such as APN) is entered correctly in the wizard or the WAN screen. These fields are case-sensitive, so make sure [Caps Lock] is not on.

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 the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1 There might be a lot of traffic on the network. If the LTE Device 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. Look at the LEDs, and check the LED section for more information. If the signal strength is low, try moving the LTE Device 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 Connect two external antennas to improve the wireless WAN signal strength. Point the antennas to the base stations directions if you know where they are, or try pointing the antennas in different directions and check which provides the strongest signal to the LTE Device. See the Introduction chapter for more information.

4 Reboot the LTE Device.

5 If the problem continues, contact the network administrator or vendor.

24.5 WiFi Connections

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

1. Make sure the wireless LAN is enabled on the LTE Device.
2. Make sure the wireless adapter on your computer is working properly.
3. Make sure the wireless adapter installed on your computer is IEEE 802.11 compatible and supports the same wireless standard as the LTE Device.
4. Make sure your computer (with a wireless adapter installed) is within the transmission range of the LTE Device.
5. Check that both the LTE Device and the wireless adapter on your computer are using the same WiFi and WiFi security settings.

I set up URL keyword blocking, but I can still access a website that should be blocked.

Make sure that the keywords are listed in the rule's **Keyword List**.

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

The following factors may cause interference:

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

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

- Move your wireless device closer to the AP if the signal strength is low.
- Reduce wireless interference that may be caused by other wireless networks or surrounding wireless electronics such as cordless phones.
- Place the AP where there are minimum obstacles (such as walls and ceilings) between the AP and the wireless client.
- Reduce the number of wireless clients connecting to the same AP simultaneously, or add additional APs if necessary.

Try closing some programs that use the Internet, especially peer-to-peer applications. If the wireless client is sending or receiving a lot of information, it may have too many programs open that use the Internet.

APPENDIX A
Setting Up Your Computer's IP Address

Note: Your specific LTE Device may not support all of the operating systems described in this appendix. See the product specifications for more information about which operating systems are supported.

This appendix shows you how to configure the IP settings on your computer in order for it to be able to communicate with the other devices on your network. Windows Vista/XP/2000, Mac OS 9/OS X, and all versions of UNIX/LINUX include the software components you need to use TCP/IP on your computer.

If you manually assign IP information instead of using a dynamic IP, make sure that your network's computers have IP addresses that place them in the same subnet.

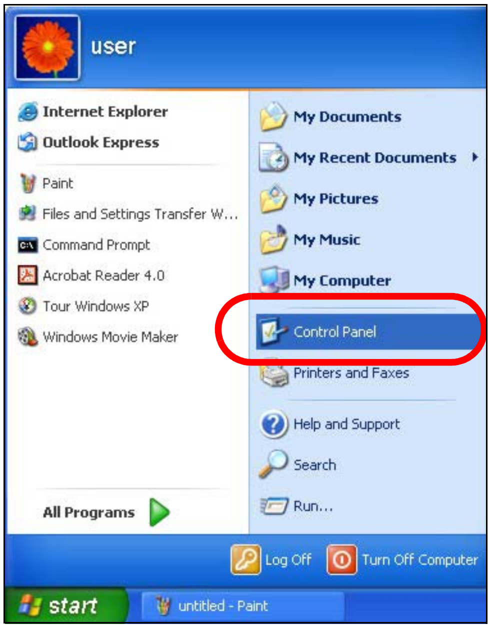
In this appendix, you can set up an IP address for:

- Windows XP/NT/2000 on page 158
- Windows Vista on page 161
- Windows 7 on page 164
- Mac OS X: 10.3 and 10.4 on page 167
- Mac OS X: 10.5 and 10.6 on page 170
- Linux: Ubuntu 8 (GNOME) on page 174
- Linux: openSUSE 10.3 (KDE) on page 177

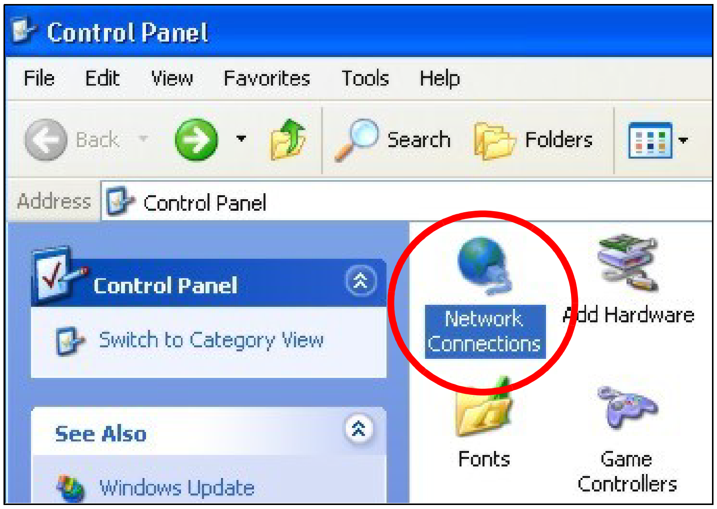
Windows XP/NT/2000

The following example uses the default Windows XP display theme but can also apply to Windows 2000 and Windows NT.

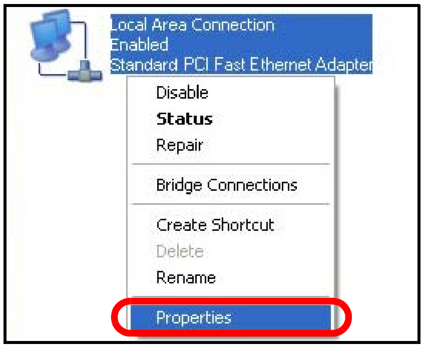
1 Click **Start** > **Control Panel**.



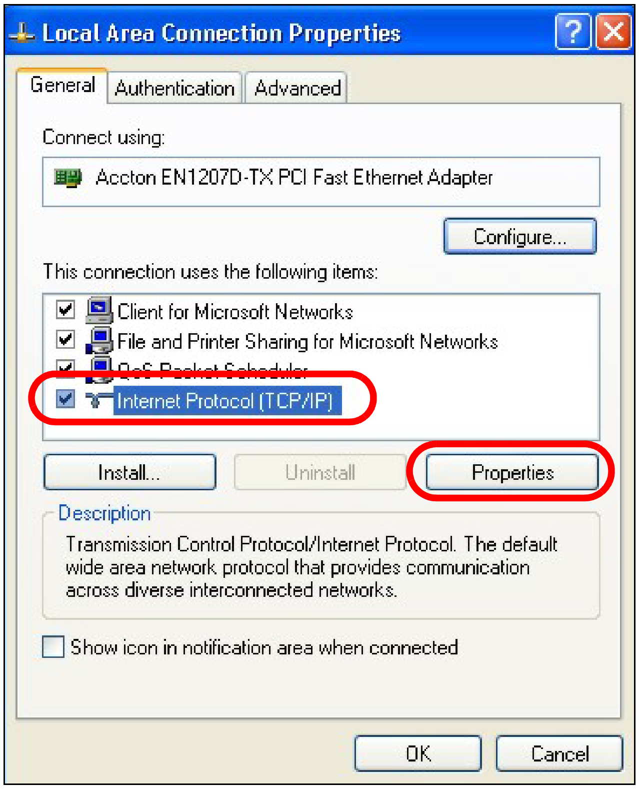
2 In the **Control Panel**, click the **Network Connections** icon.



3 Right-click **Local Area Connection** and then select **Properties**.



4 On the **General** tab, select **Internet Protocol (TCP/IP)** and then click **Properties**.



Connect using:

Accton EN1207D-TX PCI Fast Ethernet Adapter

This connection uses the following items:

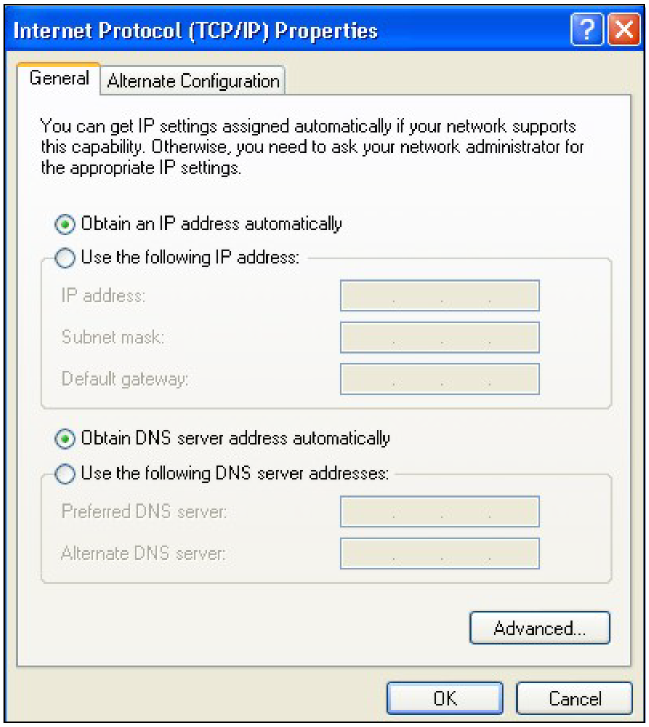
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

□ Show icon in notification area when connected

5 The **Internet Protocol TCP/IP Properties** window opens.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

6 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.

7 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

8 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

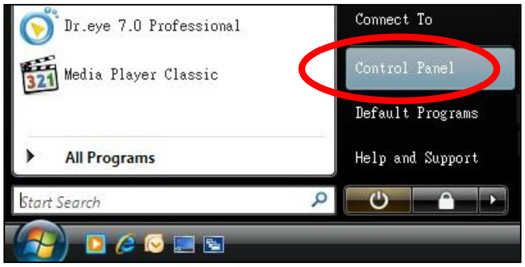
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

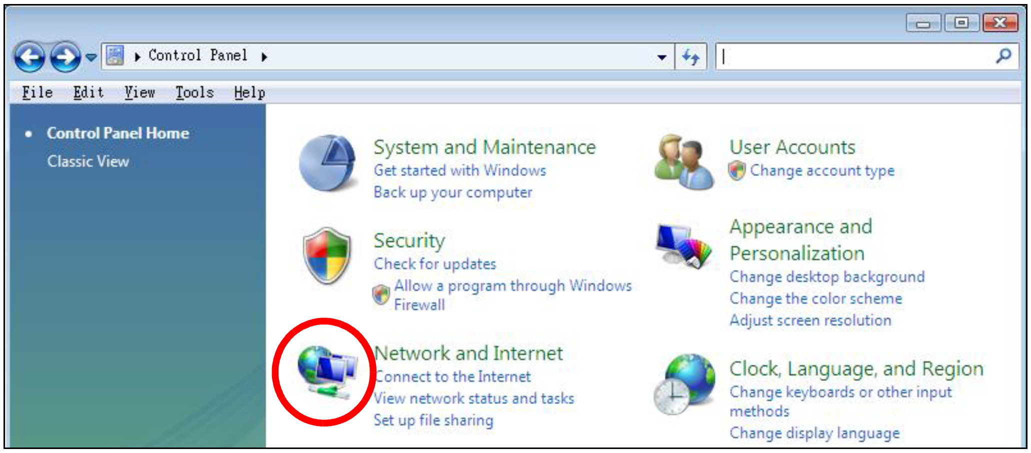
Windows Vista

This section shows screens from Windows Vista Professional.

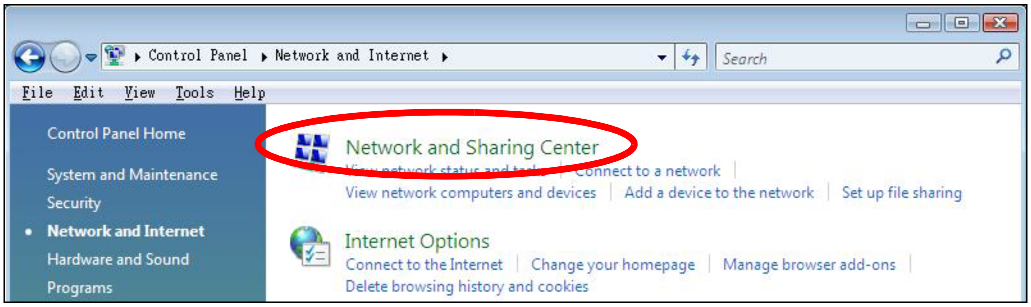
1 Click **Start** > **Control Panel**.



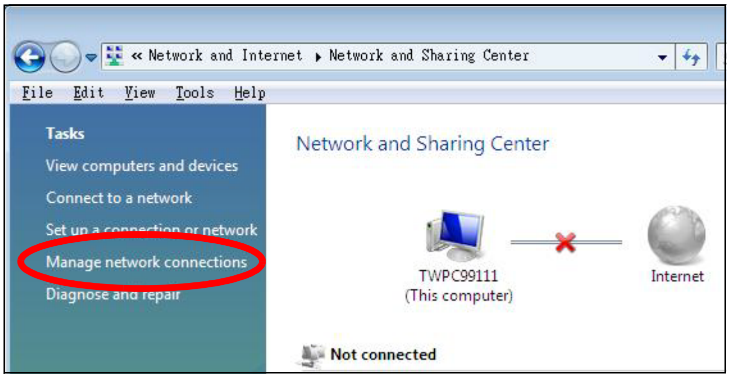
2 In the **Control Panel**, click the **Network and Internet** icon.



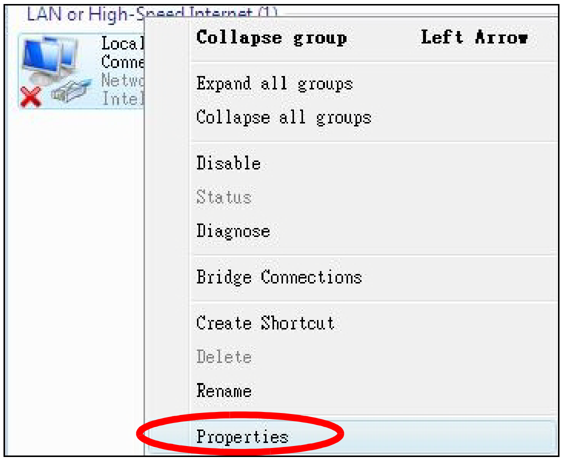
3 Click the **Network and Sharing Center** icon.


Control Panel ▸ Network and Internet ▸
Search
File Edit View Tools Help
Control Panel Home
System and Maintenance
Security
Network and Internet
Hardware and Sound
Programs
Network and Sharing Center
View network status and tasks | Connect to a network
View network computers and devices | Add a device to the network | Set up file sharing
Internet Options
Connect to the Internet | Change your homepage | Manage browser add-ons
Delete browsing history and cookies

4 Click **Manage network connections**.

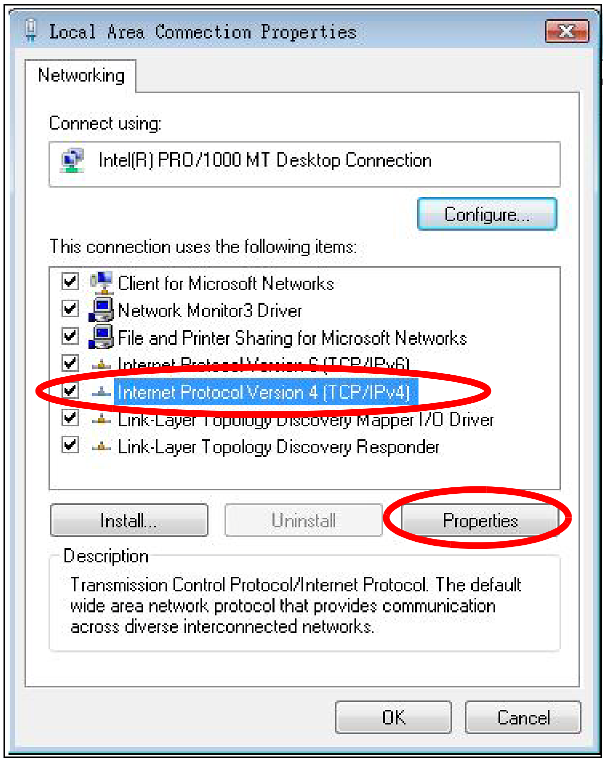

« Network and Internet ▸ Network and Sharing Center
File Edit View Tools Help
Tasks
View computers and devices
Connect to a network
Set up a connection or network
Manage network connections
Diagnose and repair
Network and Sharing Center
TWPC99111
(This computer)
Internet
Not connected

5 Right-click **Local Area Connection** and then select **Properties**.



Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

6 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.



Local Area Connection Properties

Networking

Connect using:

Intel(R) PRO/1000 MT Desktop Connection

Configure...

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ Network Monitor3 Driver
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

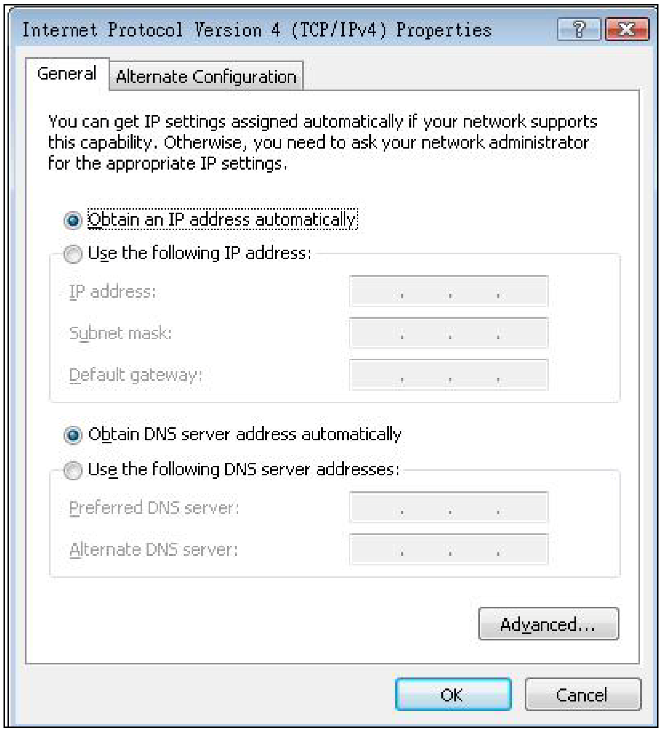
Install... Uninstall Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK Cancel

7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Advanced...

OK Cancel

8 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.Click **Advanced**.

9 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

10 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

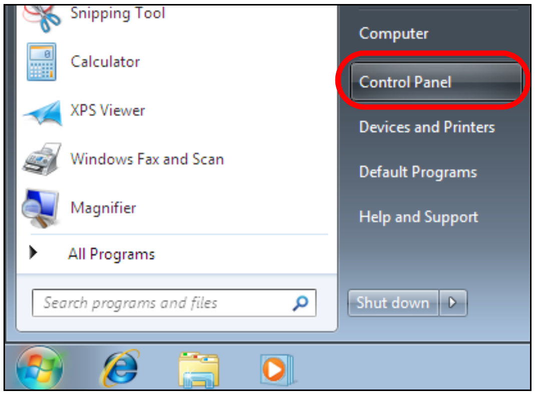
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

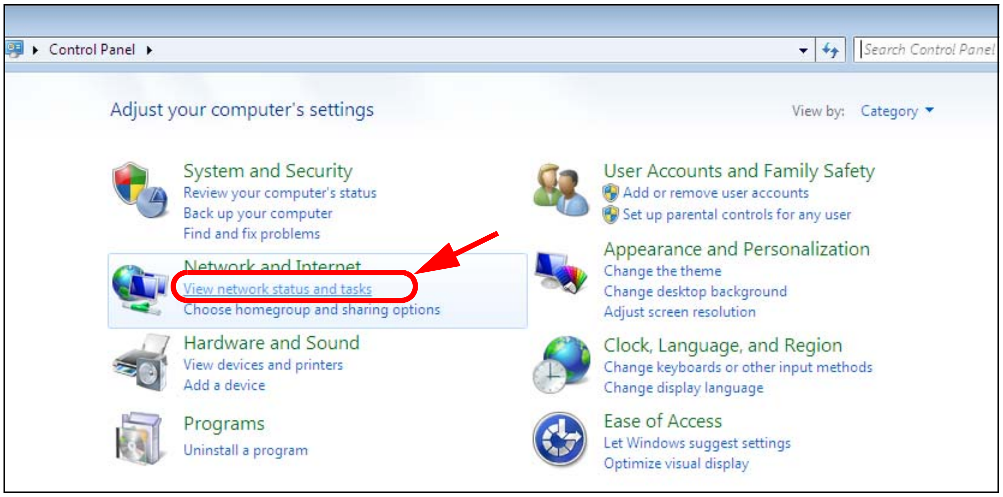
Windows 7

This section shows screens from Windows 7 Enterprise.

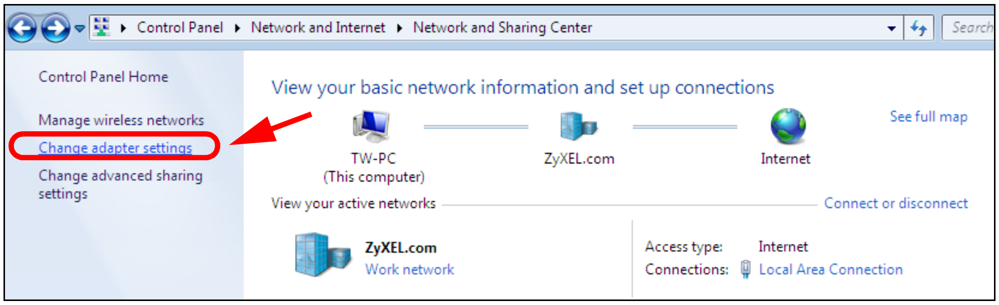
1 Click **Start** > **Control Panel**.



2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.

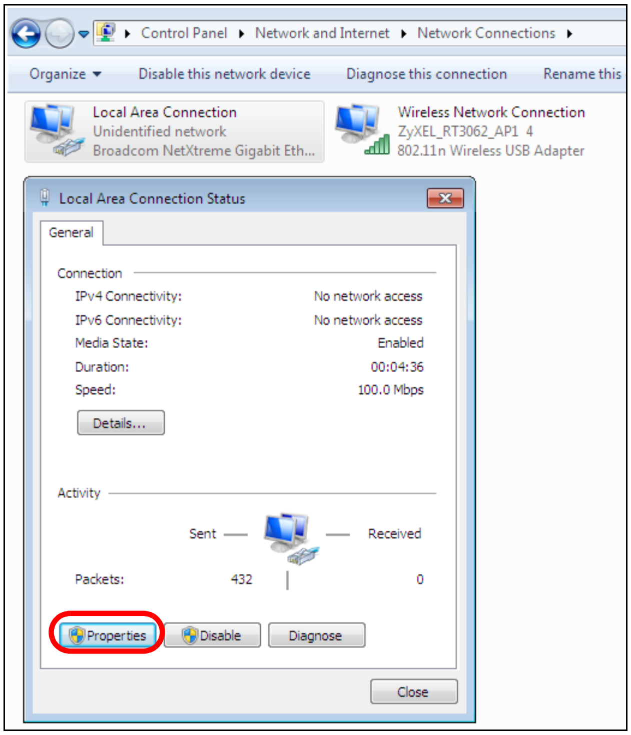

Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Back up your computer
Find and fix problems
Network and Internet
View network status and tasks
Choose homegroup and sharing options
Hardware and Sound
View devices and printers
Add a device
Programs
Uninstall a program
User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user
Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution
Clock, Language, and Region
Change keyboards or other input methods
Change display language
Ease of Access
Let Windows suggest settings
Optimize visual display

3 Click **Change adapter settings**.


Control Panel ▸ Network and Internet ▸ Network and Sharing Center
Search
Control Panel Home
Manage wireless networks
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
TW-PC
(This computer)
ZyXEL.com
Internet
View your active networks
Connect or disconnect
ZyXEL.com
Work network

Access type: Internet
Connections: Local Area Connection

4 Double click **Local Area Connection** and then select **Properties**.


Control Panel ▸ Network and Internet ▸ Network Connections ▸
Organize ▾
Disable this network device
Diagnose this connection
Rename this
Local Area Connection
Unidentified network
Broadcom NetXtreme Gigabit Eth...
Wireless Network Connection
ZyXEL_RT3062_AP1 4
802.11n Wireless USB Adapter
Local Area Connection Status
General
Details...
Activity
Sent
Received
Properties
Disable
Diagnose
Close

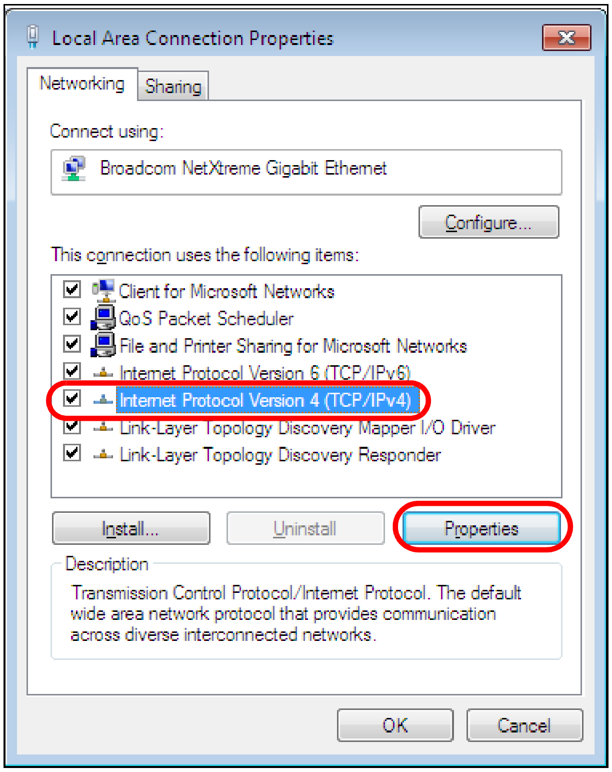
Connection

IPv4 Connectivity: No network access
IPv6 Connectivity: No network access
Media State: Enabled
Duration: 00:04:36
Speed: 100.0 Mbps

Packets: Sent 432, Received 0

Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

5 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.



Local Area Connection Properties

Networking | Sharing

Connect using:

Broadcom NetXtreme Gigabit Ethernet

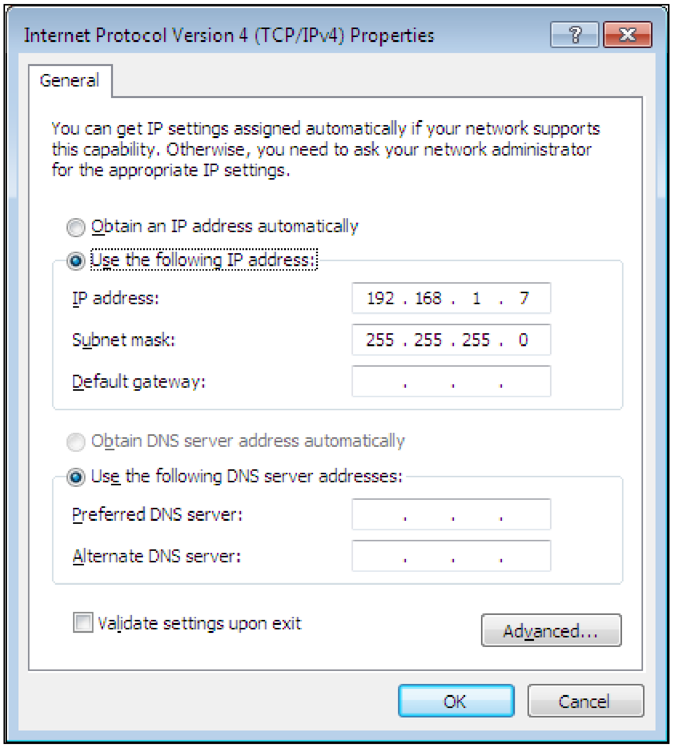
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

6 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 7

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

7 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided. Click **Advanced** if you want to configure advanced settings for IP, DNS and WINS.

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

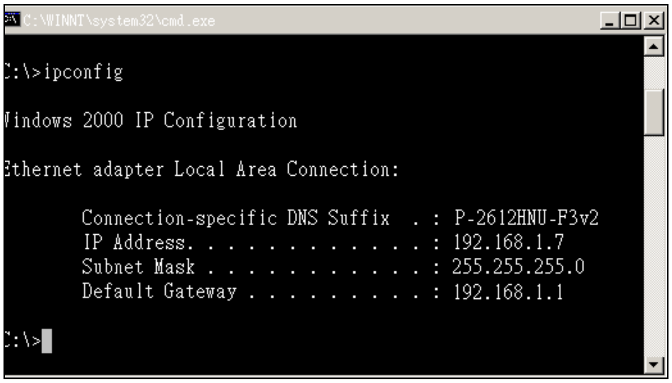
9 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

3 The IP settings are displayed as follows.

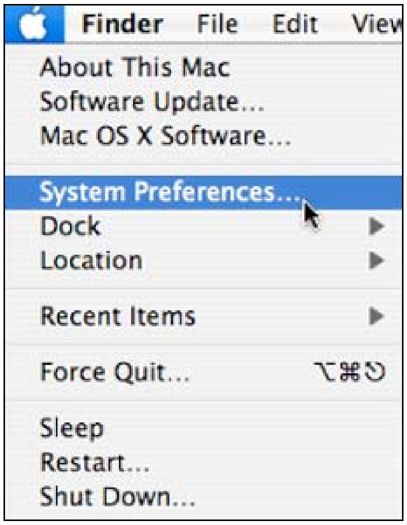


```
:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

       Connection-specific DNS Suffix  . : P-2612HNU-F3v2
       IP Address. . . . . . . . . . . . : 192.168.1.7
       Subnet Mask . . . . . . . . . . . : 255.255.255.0
       Default Gateway . . . . . . . . . : 192.168.1.1

:\>
```

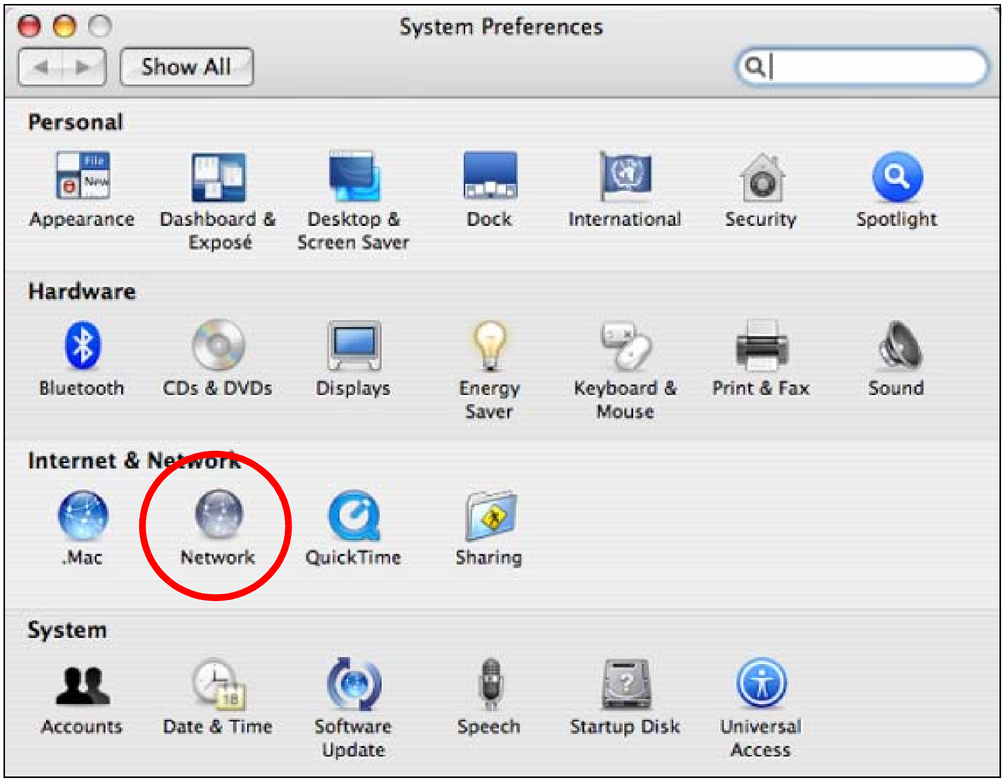
Mac OS X: 10.3 and 10.4

The screens in this section are from Mac OS X 10.4 but can also apply to 10.3.

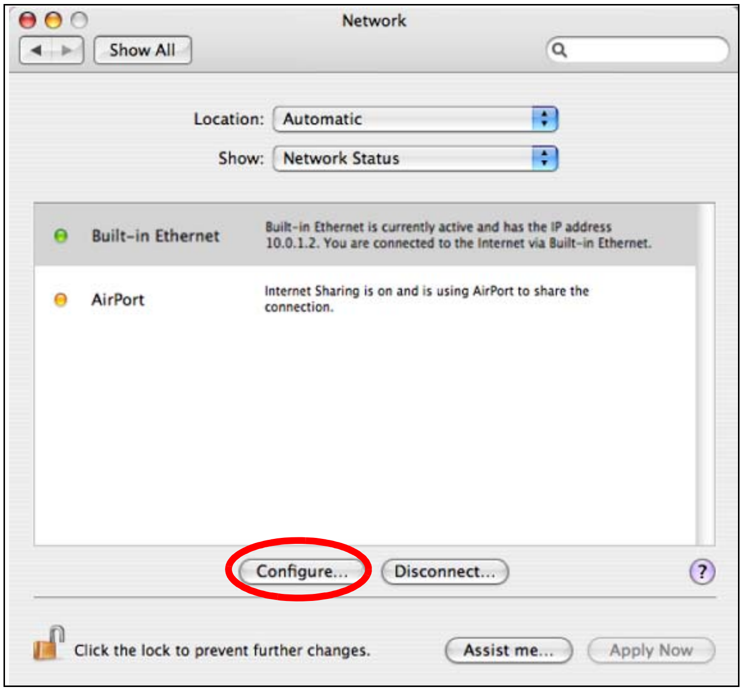
1 Click **Apple** > **System Preferences**.



2 In the **System Preferences** window, click the **Network** icon.



3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure.**



Location: Automatic

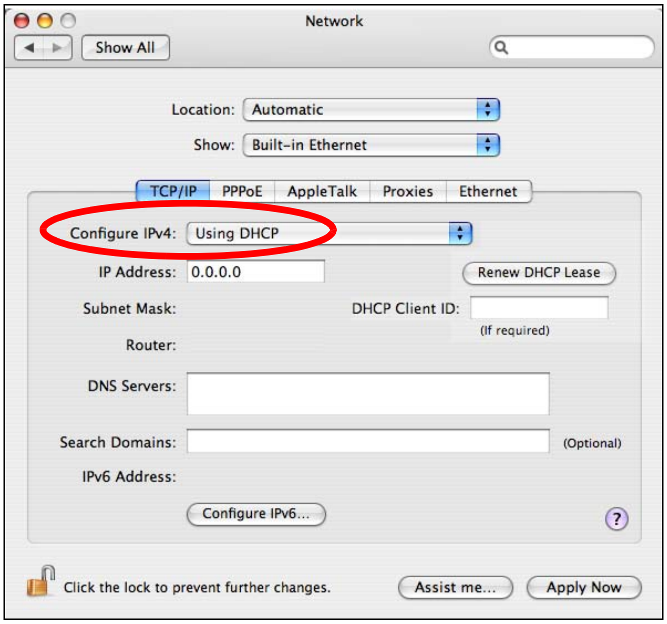
Show: Network Status

Built-in Ethernet — Built-in Ethernet is currently active and has the IP address 10.0.1.2. You are connected to the Internet via Built-in Ethernet.

AirPort — Internet Sharing is on and is using AirPort to share the connection.

Click the lock to prevent further changes.

4 For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.



Location: Automatic

Show: Built-in Ethernet

Configure IPv4: Using DHCP

IP Address: 0.0.0.0

Subnet Mask:

DHCP Client ID: (If required)

Router:

DNS Servers:

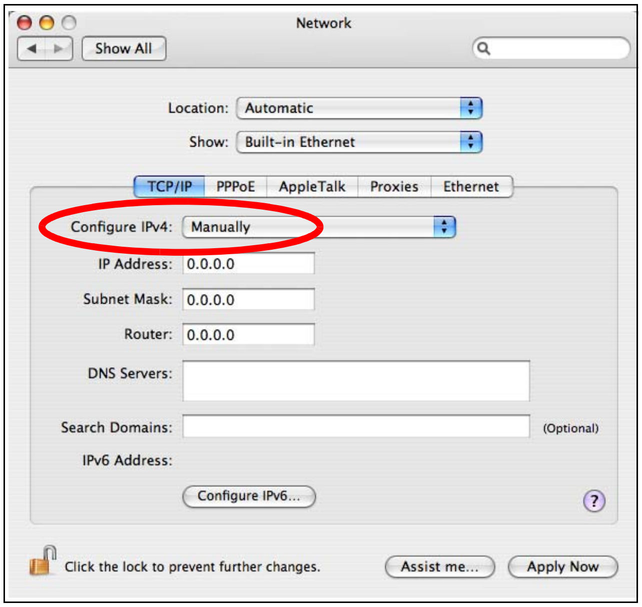
Search Domains: (Optional)

IPv6 Address:

Click the lock to prevent further changes.

5 For statically assigned settings, do the following:

- From the **Configure IPv4** list, select **Manually**.
- In the **IP Address** field, type your IP address.
- In the **Subnet Mask** field, type your subnet mask.
- In the **Router** field, type the IP address of your device.



Location: Automatic
Show: Built-in Ethernet

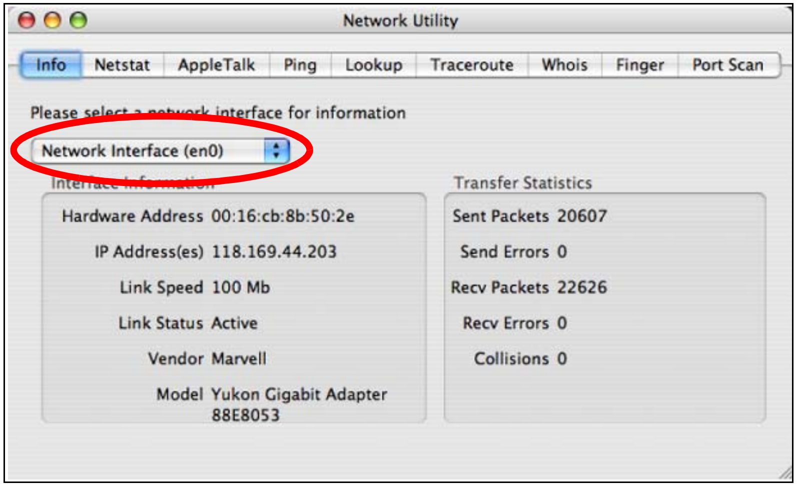
Configure IPv4: Manually
IP Address: 0.0.0.0
Subnet Mask: 0.0.0.0
Router: 0.0.0.0
DNS Servers:
Search Domains: (Optional)
IPv6 Address:

6 Click **Apply Now** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network Interface** from the **Info** tab.

Figure 113 Mac OS X 10.4: Network Utility



Please select a network interface for information
Network Interface (en0)

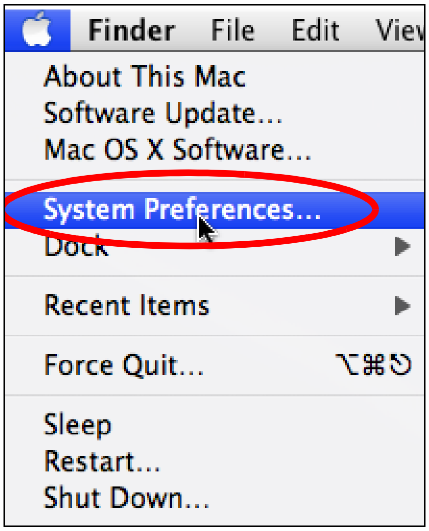
Interface Information
Hardware Address 00:16:cb:8b:50:2e
IP Address(es) 118.169.44.203
Link Speed 100 Mb
Link Status Active
Vendor Marvell
Model Yukon Gigabit Adapter 88E8053

Transfer Statistics
Sent Packets 20607
Send Errors 0
Recv Packets 22626
Recv Errors 0
Collisions 0

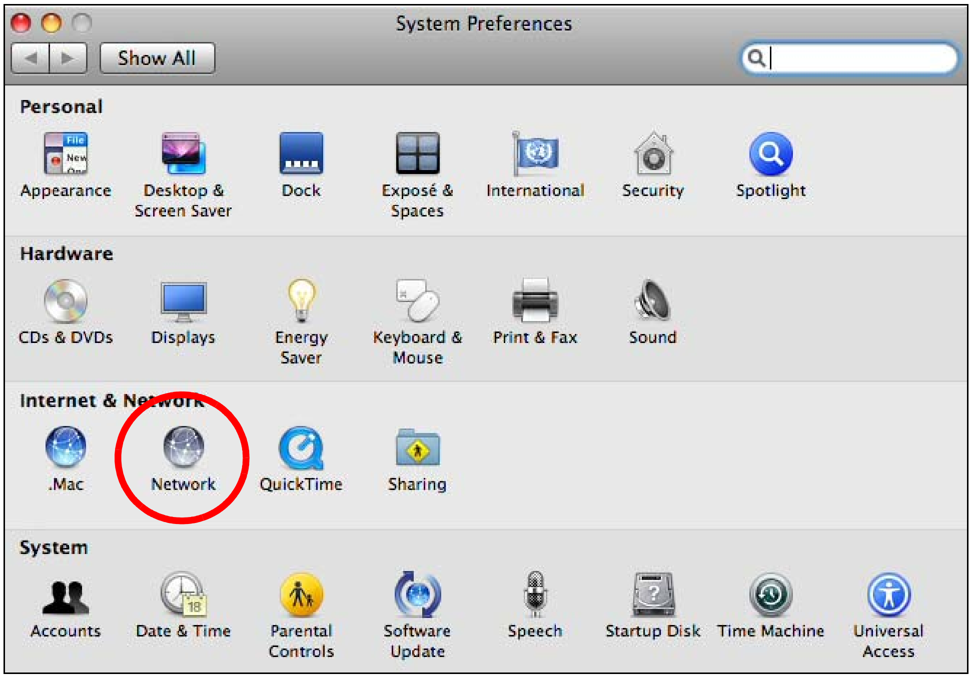
Mac OS X: 10.5 and 10.6

The screens in this section are from Mac OS X 10.5 but can also apply to 10.6.

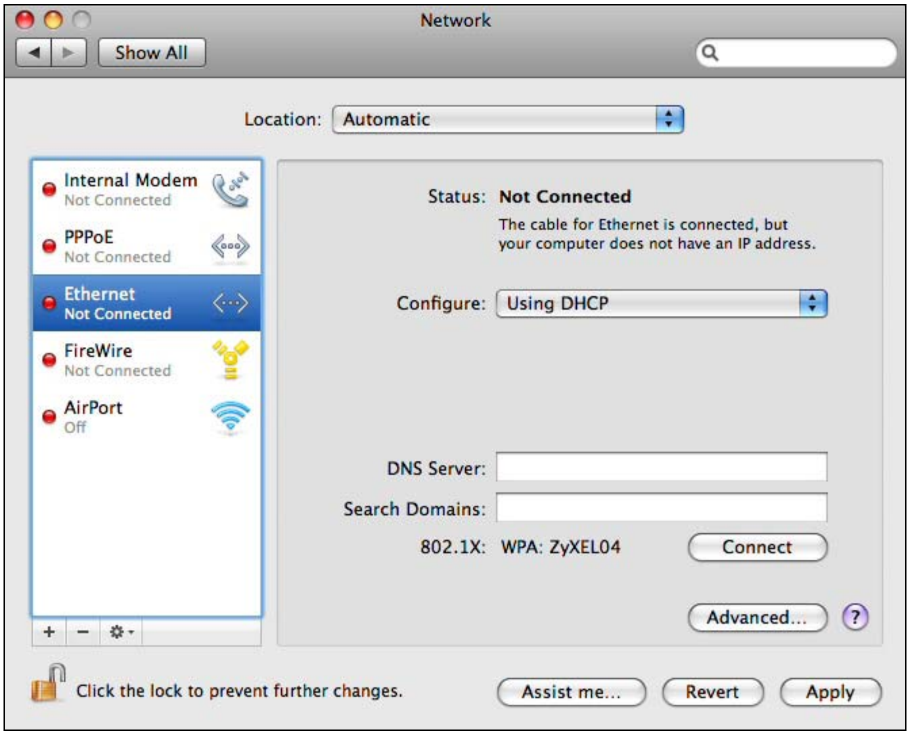
1 Click **Apple** > **System Preferences**.



2 In **System Preferences**, click the **Network** icon.



3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.



Network

Location: Automatic

Internal Modem
Not Connected

PPPoE
Not Connected

Ethernet
Not Connected

FireWire
Not Connected

AirPort
Off

Status: **Not Connected**

The cable for Ethernet is connected, but your computer does not have an IP address.

Configure: Using DHCP

DNS Server:

Search Domains:

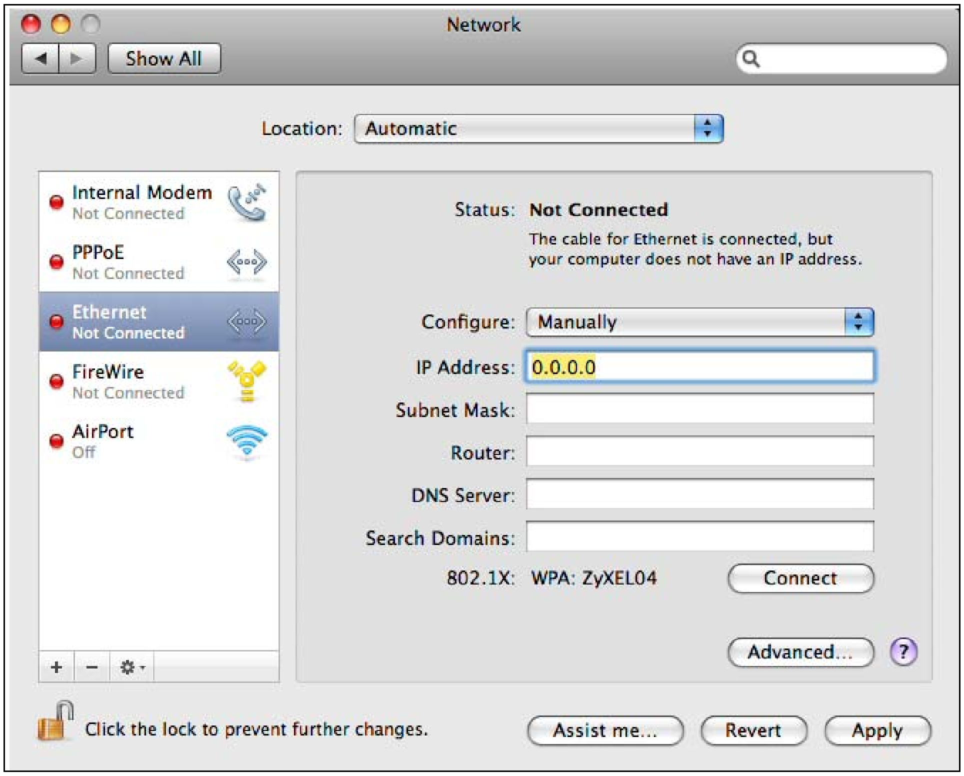
802.1X: WPA: ZyXEL04

Click the lock to prevent further changes.

4 From the **Configure** list, select **Using DHCP** for dynamically assigned settings.

5 For statically assigned settings, do the following:

- From the **Configure** list, select **Manually**.
- In the **IP Address** field, enter your IP address.
- In the **Subnet Mask** field, enter your subnet mask.
- In the **Router** field, enter the IP address of your LTE Device.



Location: Automatic

Status: **Not Connected**

The cable for Ethernet is connected, but your computer does not have an IP address.

Configure: Manually

IP Address: 0.0.0.0

Subnet Mask:

Router:

DNS Server:

Search Domains:

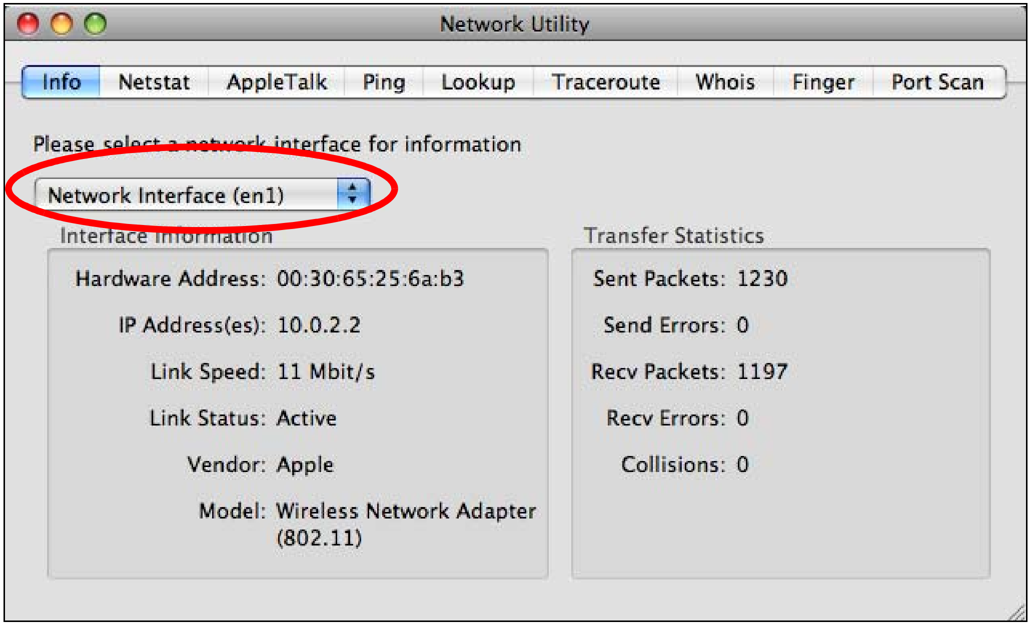
802.1X: WPA: ZyXEL04

6 Click **Apply** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network interface** from the **Info** tab.

Figure 114 Mac OS X 10.5: Network Utility



Please select a network interface for information

Network Interface (en1)

Interface Information

Hardware Address: 00:30:65:25:6a:b3

IP Address(es): 10.0.2.2

Link Speed: 11 Mbit/s

Link Status: Active

Vendor: Apple

Model: Wireless Network Adapter (802.11)

Transfer Statistics

Sent Packets: 1230

Send Errors: 0

Recv Packets: 1197

Recv Errors: 0

Collisions: 0

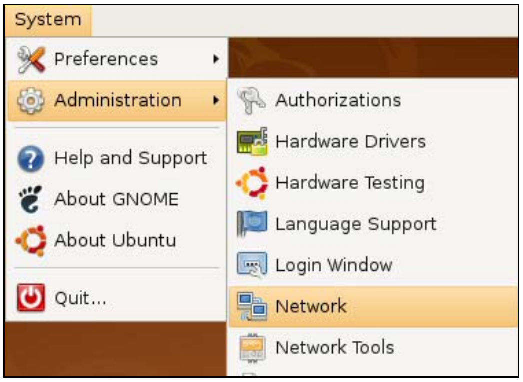
Linux: Ubuntu 8 (GNOME)

This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default Ubuntu 8 installation.

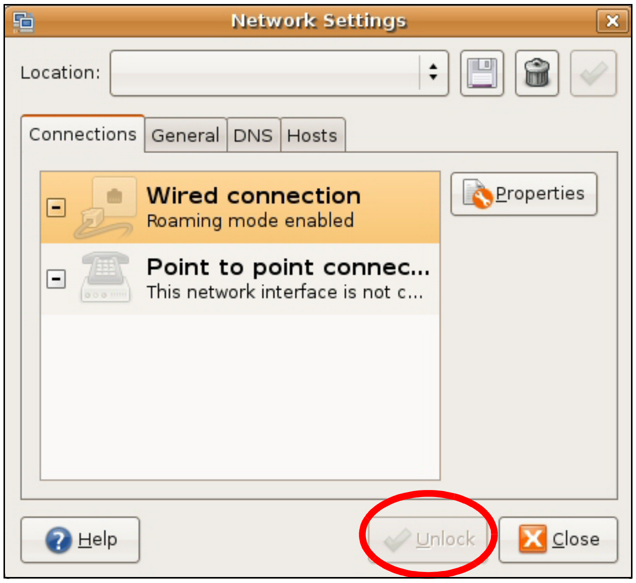
Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in GNOME:

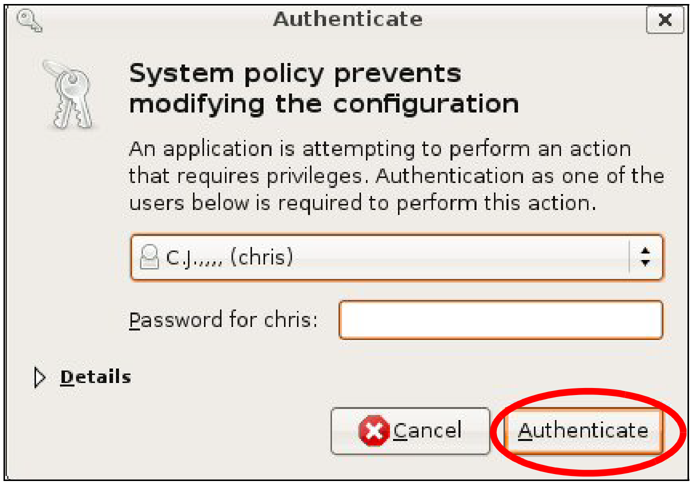
1 Click **System > Administration > Network**.



2 When the **Network Settings** window opens, click **Unlock** to open the **Authenticate** window. (By default, the **Unlock** button is greyed out until clicked.) You cannot make changes to your configuration unless you first enter your admin password.



3 In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.



Authenticate

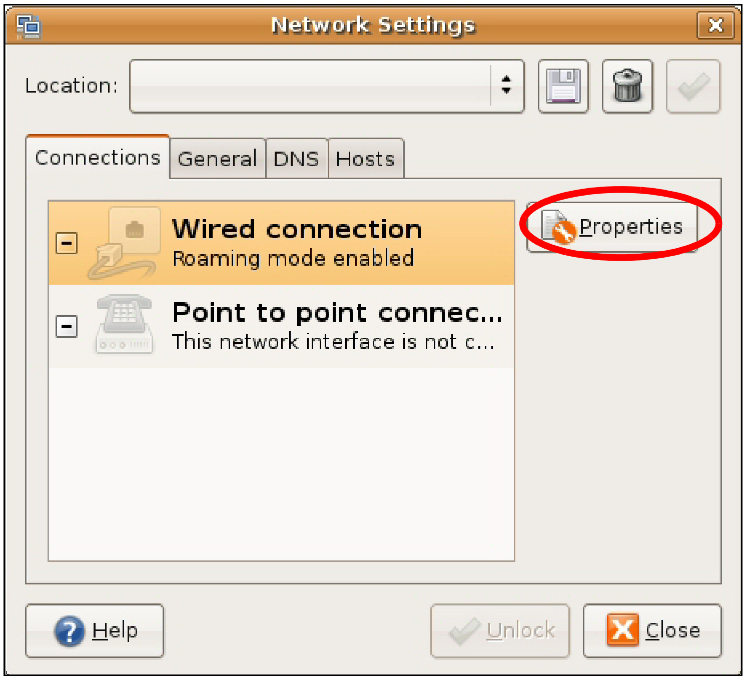
System policy prevents modifying the configuration

An application is attempting to perform an action that requires privileges. Authentication as one of the users below is required to perform this action.

C.J.,,,, (chris)

Password for chris:

4 In the **Network Settings** window, select the connection that you want to configure, then click **Properties**.



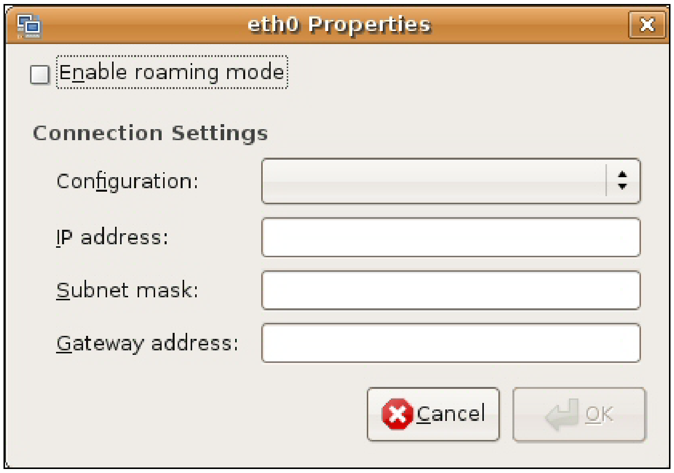
Network Settings

Location:

Wired connection
Roaming mode enabled

Point to point connec...
This network interface is not c...

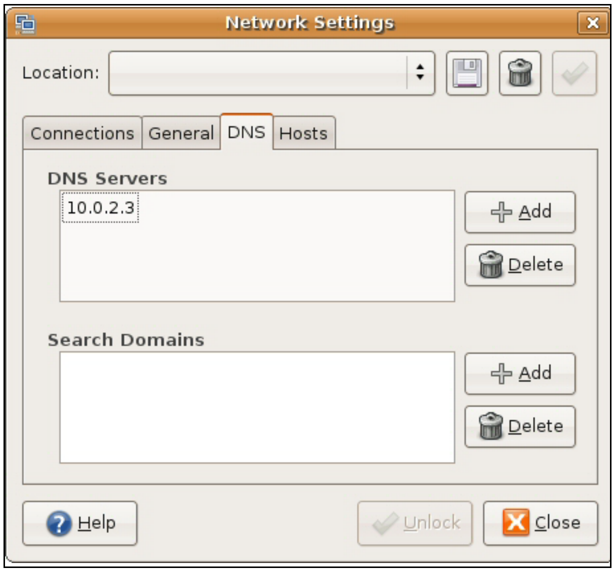
5 The **Properties** dialog box opens.



- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
- In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.

6 Click **OK** to save the changes and close the **Properties** dialog box and return to the **Network Settings** screen.

7 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Settings** window and then enter the DNS server information in the fields provided.



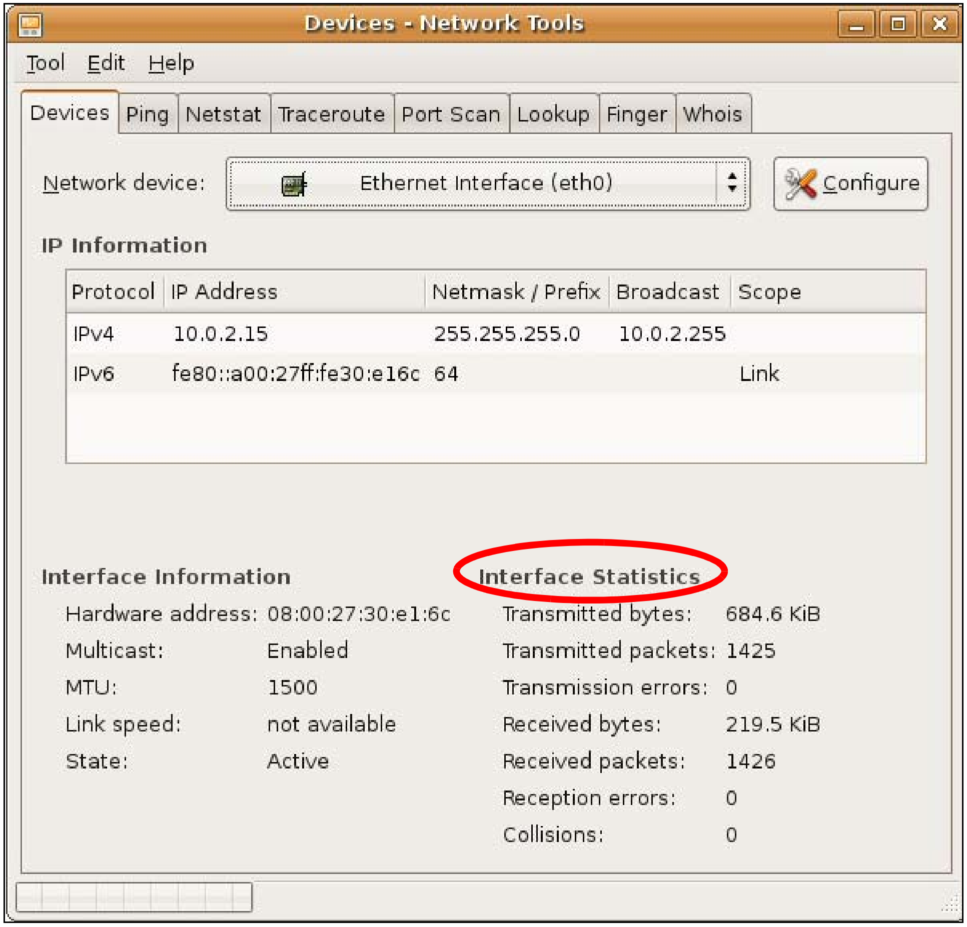
DNS Servers: 10.0.2.3

8 Click the **Close** button to apply the changes.

Verifying Settings

Check your TCP/IP properties by clicking **System > Administration > Network Tools**, and then selecting the appropriate **Network device** from the **Devices** tab. The **Interface Statistics** column shows data if your connection is working properly.

Figure 115 Ubuntu 8: Network Tools



Network device: Ethernet Interface (eth0)

IP Information

Protocol	IP Address	Netmask / Prefix	Broadcast	Scope
IPv4	10.0.2.15	255.255.255.0	10.0.2.255	
IPv6	fe80::a00:27ff:fe30:e16c	64		Link

Interface Information

Hardware address:	08:00:27:30:e1:6c
Multicast:	Enabled
MTU:	1500
Link speed:	not available
State:	Active

Interface Statistics

Transmitted bytes:	684.6 KiB
Transmitted packets:	1425
Transmission errors:	0
Received bytes:	219.5 KiB
Received packets:	1426
Reception errors:	0
Collisions:	0

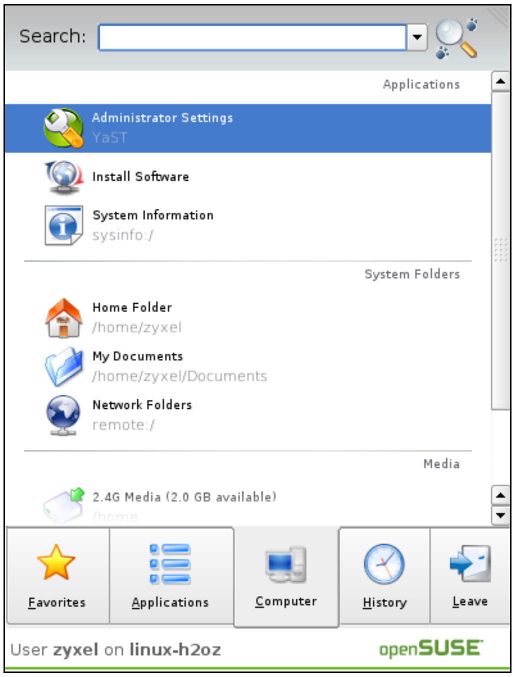
Linux: openSUSE 10.3 (KDE)

This section shows you how to configure your computer's TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default openSUSE 10.3 installation.

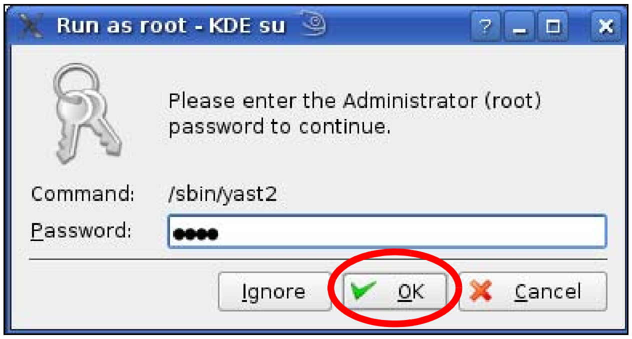
Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in the KDE:

1 Click **K Menu > Computer > Administrator Settings (YaST)**.



2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.

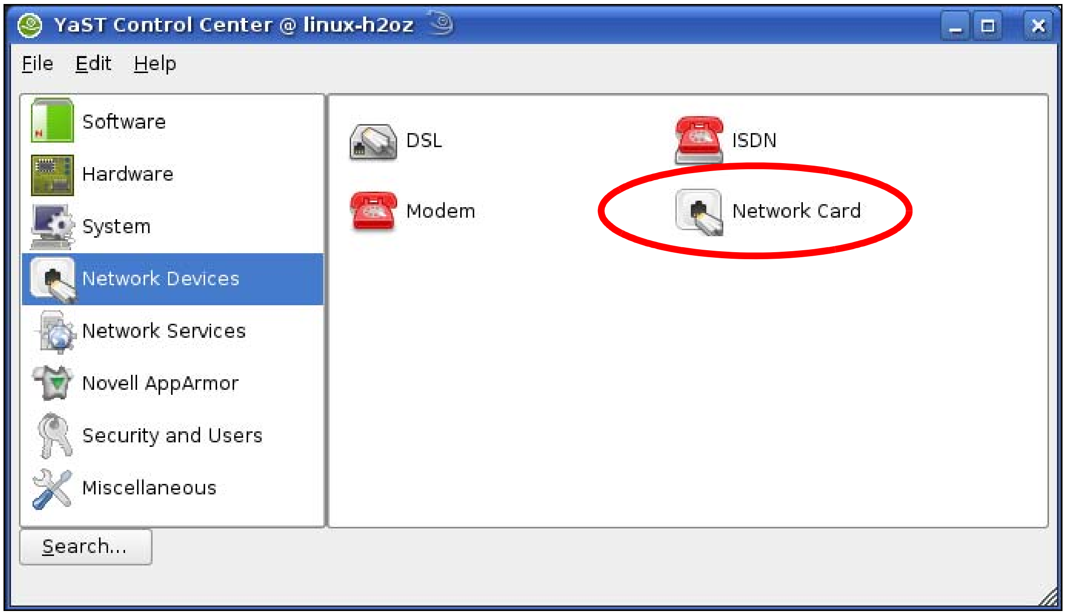


Please enter the Administrator (root) password to continue.

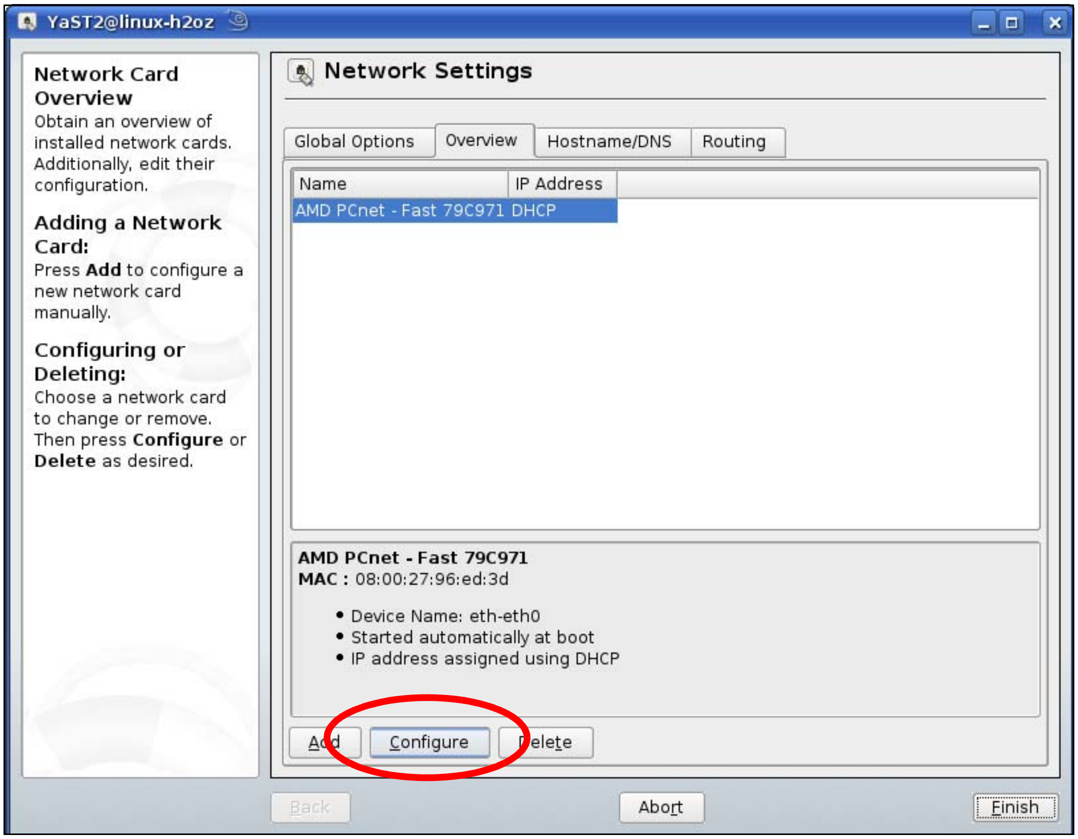
Command: /sbin/yast2

Password: ●●●●

3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.



4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.



Network Card Overview
Obtain an overview of installed network cards. Additionally, edit their configuration.

Adding a Network Card:
Press **Add** to configure a new network card manually.

Configuring or Deleting:
Choose a network card to change or remove. Then press **Configure** or **Delete** as desired.

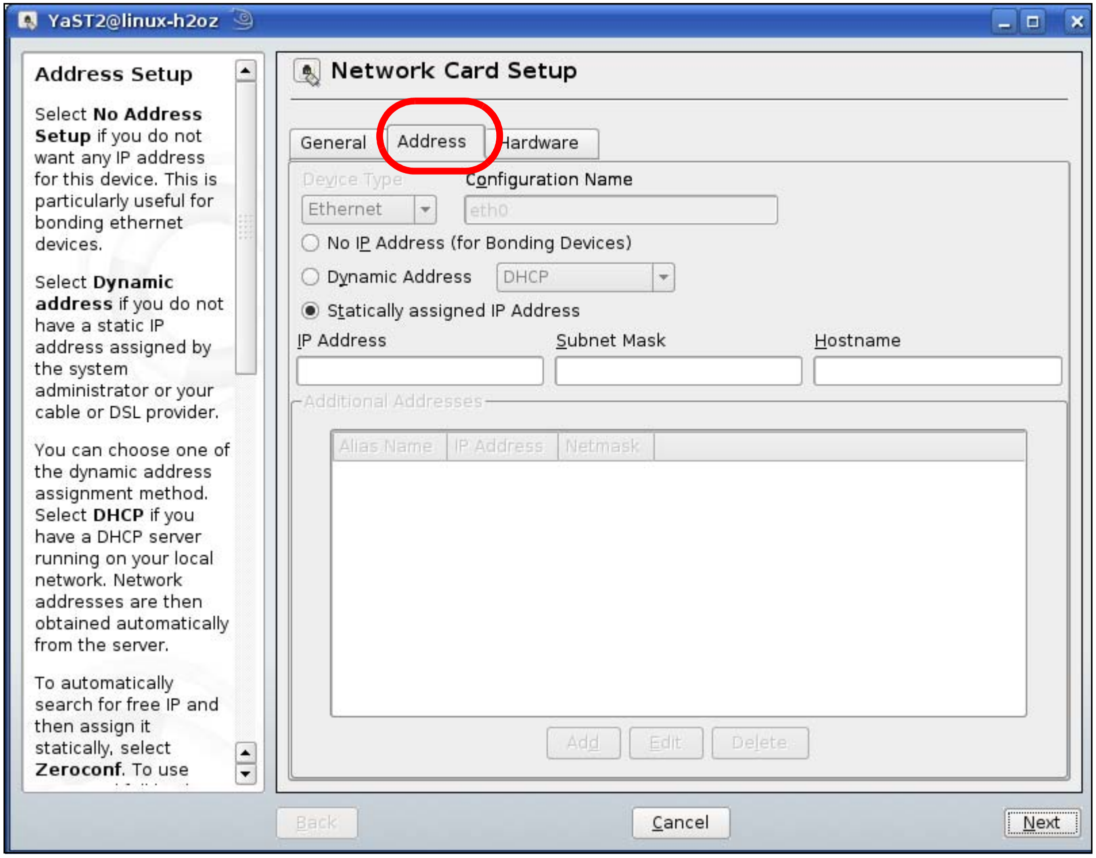
Name	IP Address
AMD PCnet - Fast 79C971	DHCP

AMD PCnet - Fast 79C971
MAC : 08:00:27:96:ed:3d

- Device Name: eth-eth0
- Started automatically at boot
- IP address assigned using DHCP

5 When the **Network Card Setup** window opens, click the **Address** tab

Figure 116 openSUSE 10.3: Network Card Setup



Address Setup

Select **No Address Setup** if you do not want any IP address for this device. This is particularly useful for bonding ethernet devices.

Select **Dynamic address** if you do not have a static IP address assigned by the system administrator or your cable or DSL provider.

You can choose one of the dynamic address assignment method. Select **DHCP** if you have a DHCP server running on your local network. Network addresses are then obtained automatically from the server.

To automatically search for free IP and then assign it statically, select **Zeroconf**. To use

Device Type: Ethernet

Configuration Name: eth0

○ No IP Address (for Bonding Devices)

○ Dynamic Address DHCP

● Statically assigned IP Address

IP Address	Subnet Mask	Hostname

Additional Addresses

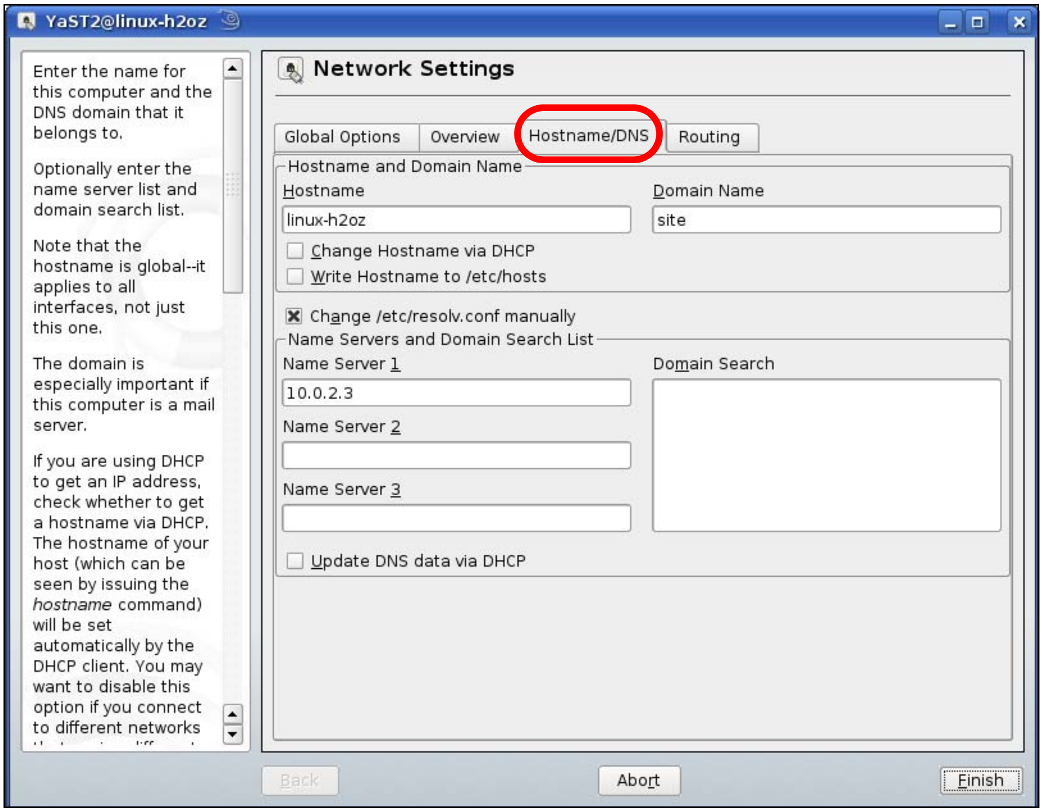
Alias Name	IP Address	Netmask

6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.

Select **Statically assigned IP Address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Hostname** fields.

7 Click **Next** to save the changes and close the **Network Card Setup** window.

8 If you know your DNS server IP address(es), click the **Hostname/DNS** tab in **Network Settings** and then enter the DNS server information in the fields provided.



Enter the name for this computer and the DNS domain that it belongs to.

Optionally enter the name server list and domain search list.

Note that the hostname is global--it applies to all interfaces, not just this one.

The domain is especially important if this computer is a mail server.

If you are using DHCP to get an IP address, check whether to get a hostname via DHCP. The hostname of your host (which can be seen by issuing the *hostname* command) will be set automatically by the DHCP client. You may want to disable this option if you connect to different networks

Hostname and Domain Name

Hostname: linux-h2oz

Domain Name: site

□ Change Hostname via DHCP

□ Write Hostname to /etc/hosts

☒ Change /etc/resolv.conf manually

Name Servers and Domain Search List

Name Server 1: 10.0.2.3

Name Server 2:

Name Server 3:

Domain Search:

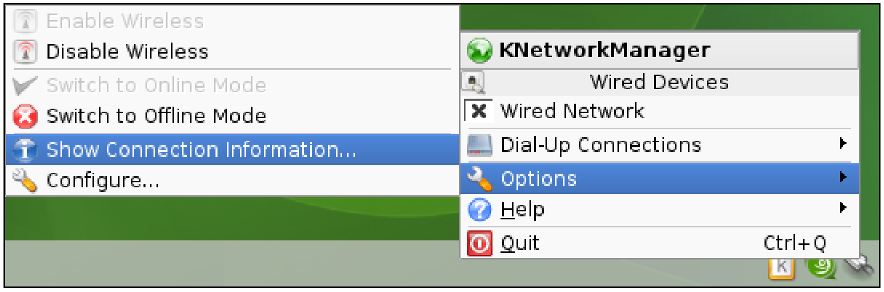
□ Update DNS data via DHCP

9 Click **Finish** to save your settings and close the window.

Verifying Settings

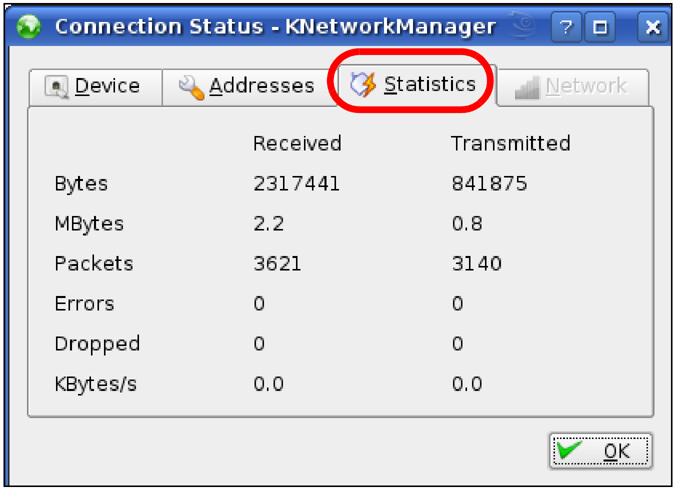
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 117 openSUSE 10.3: KNetwork Manager



When the **Connection Status - KNetwork Manager** window opens, click the **Statistics tab** to see if your connection is working properly.

Figure 118 openSUSE: Connection Status - KNetwork Manager



	Received	Transmitted
Bytes	2317441	841875
MBytes	2.2	0.8
Packets	3621	3140
Errors	0	0
Dropped	0	0
KBytes/s	0.0	0.0

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 73 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 73 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.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.

Table 73 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
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
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 D
Legal Information

Copyright

Copyright © 2017 by Zyxel Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of Zyxel Communications Corporation.

Published by Zyxel Communications Corporation. All rights reserved.

Disclaimer

Zyxel does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Zyxel further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Regulatory Notice and Statement

UNITED STATES of AMERICA

The following information applies if you use the product within USA area.

FCC EMC Statement

- The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

  (1) This device may not cause harmful interference, and

  (2) This device must accept any interference received, including interference that may cause undesired operation.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the device.
- This product has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
- If this device does cause harmful interference to radio or television reception, which is found by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
  - Reorient or relocate the receiving antenna
  - Increase the separation between the devices
  - Connect the equipment to an outlet other than the receiver's
  - Consult a dealer or an experienced radio/TV technician for assistance

The following information applies if you use the product with RF function within USA area.

FCC Radiation Exposure Statement

- This device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must be at least 20 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.

CANADA

The following information applies if you use the product within Canada area.

Industry Canada ICES Statement

CAN ICES-3 (B)/NMB-3(B)

Industry Canada RSS-GEN & RSS-247 statement

- This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

- This radio transmitter has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

If the product with 5G wireless function operating in 5150-5250 MHz and 5725-5850 MHz, the following attention must be paid,

- The device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.
- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-to-point operation as appropriate; and
- The worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in Section 6.2.2(3) of RSS 247 shall be clearly indicated.

If the product with 5G wireless function operating in 5250-5350 MHz and 5470-5725 MHz , the following attention must be paid.

- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit.
- Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.
- Le présent émetteur radio de modèle s'il fait partie du matériel de catégoriel) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Lorsque la fonction sans fil 5G fonctionnant en 5150-5250 MHz and 5725-5850 MHz est activée pour ce produit , il est nécessaire de porter une attention particulière aux choses suivantes

- Les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5 725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée pour l'exploitation point à point et l'exploitation non point à point, selon le cas;
- Les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élévation, et énoncée à la section 6.2.2 3) du CNR-247, doivent être clairement indiqués.

Lorsque la fonction sans fil 5G fonctionnant en 5250-5350 MHz et 5470-5725 MHz est activée pour ce produit , il est nécessaire de porter une attention particulière aux choses suivantes.

- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis pour les dispositifs utilisant les bandes de 5 250 à 5 350 MHz et de 5 470 à 5 725 MHz doit être conforme à la limite de la p.i.r.e.

Industry Canada radiation exposure statement

This device complies with IC radiation exposure limits set forth for an uncontrolled environment. This device should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

EUROPEAN UNION

The following information applies if you use the product within the European Union.

Declaration of Conformity with Regard to EU Directive 2014/53/EU (Radio Equipment Directive, RED)

- Compliance information for 2.4GHz and/or 5GHz 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 minimum distance 20cm between the radiator and your body.

Български (Bulgarian)	С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/EC. **National Restrictions** • 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)	Undertegnede Zyxel erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU. **National Restrictions** • 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/EU põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Zyxel ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/EU.
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/EU.
Hrvatski (Croatian)	Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 2014/53/EU.
Íslenska (Icelandic)	Hér með lýsir, Zyxel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53/EU.
Italiano (Italian)	Con la presente Zyxel dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/EU. **National Restrictions** • 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)	Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 2014/53/EU būtiskajām prasībām un citiem ar to saistītajiem noteikumiem. **National Restrictions** • 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 frekvenèu joslas izmantoðanai ârpus telpâm nepiecieðama atïauja no Elektronisko sakaru direkcijas. Vairâk informâcijas: http://www.esd.lv.
Lietuvių kalba (Lithuanian)	Šiuo Zyxel deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/EU Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, Zyxel nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvetõ követelményeknek és az 2014/53/EU irányelv egyéb elõírásainak.
Malti (Maltese)	Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/53/EU.
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/EU.
Português (Portuguese)	Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/EU.

Română (Romanian)	Prin prezenta, Zyxel declară că acest echipament este în conformitate cu cerințele esențiale şi alte prevederi relevante ale Directivei 2014/53/EU.
Slovenčina (Slovak)	Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EU.
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.

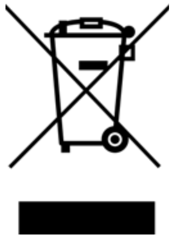
Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung 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.

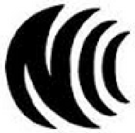
Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit 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

以下訊息僅適用於產品操作於 5.25-5.35 秭赫頻帶內並銷售至台灣地區

- 在 5.25-5.35 秭赫頻帶內操作之無線資訊傳輸設備，限於室內使用。

以下訊息僅適用於產品屬於專業安裝並銷售至台灣地區

- 本器材須經專業工程人員安裝及設定，始得設置使用，且不得直接販售給一般消費者。

安全警告 - 為了您的安全，請先閱讀以下警告及指示：

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸：
  - 任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
  - 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 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 if 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