# LTE3311 Series

LTE Indoor IAD

Version 1.00
Edition 1, 02/2016

# User's Guide

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

Copyright © 2016 ZyXEL Communications Corporation

**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. Every effort has been made to ensure that the information in this manual is accurate.

## Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the LTE3311 and access the Web Configurator wizards. It contains information on setting up your network and configuring for Internet access.

- More Information

  Go to **support.zyxel.com** to find other information on the LTE3311.

# Contents Overview

# Table of Contents

# PART I
# User's Guide

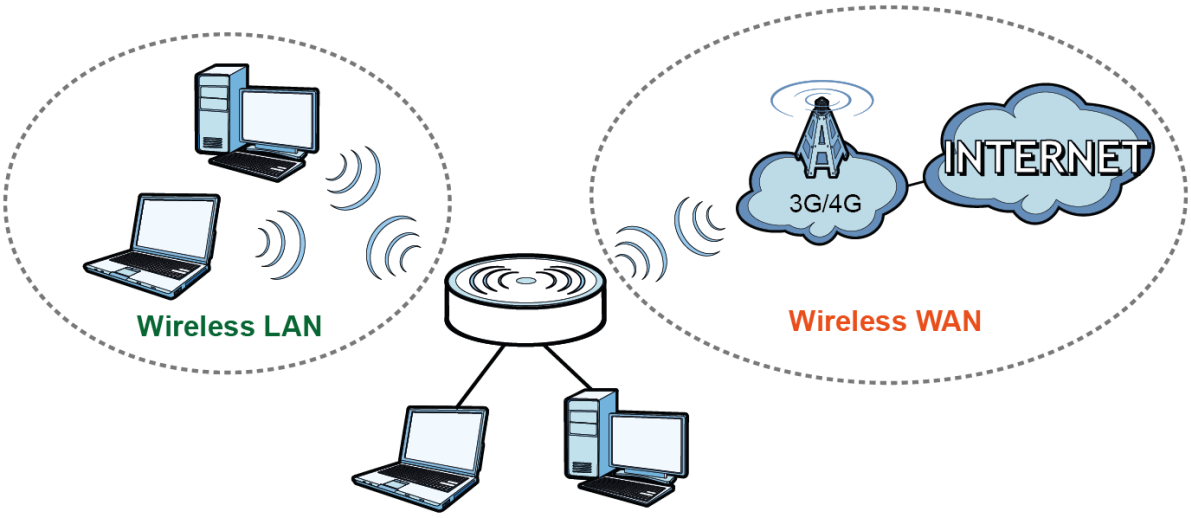
# 1

# Introduction

## 1.1 Overview

This chapter introduces the main features and applications of the LTE3311.

The LTE3311 is a wireless router, which can connect to a mobile network and the Internet through a wireless WAN connection and provide easy network access to mobile users without additional wiring. You can set up a wireless network with other IEEE 802.11b/g/n compatible devices.




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

## 1.2 Applications

Your can have the following networks with the LTE3311:

- **Wired**. You can connect network devices via the Ethernet ports of the LTE3311 so that they can communicate with each other and access the Internet.
- **Wireless LAN**. Wireless clients can wirelessly connect to the LTE3311 to access network resources. You can use WPS (Wi-Fi Protected Setup) to create an instant network connection with another WPS-compatible device.
- **Wireless WAN**. Insert a 3G/4G SIM card into the SIM card slot to connect to a mobile network for Internet access.

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

The LTE3311 comes with a built-in 3G/4G module for 3G/4G connections. To set up a 3G/4G connection using the built-in 3G/4G module, just insert a 3G/4G SIM card into the SIM card slot at the back of the LTE3311.

Note: You must insert the 3G/4G SIM card into the card slot before turning on the LTE3311.

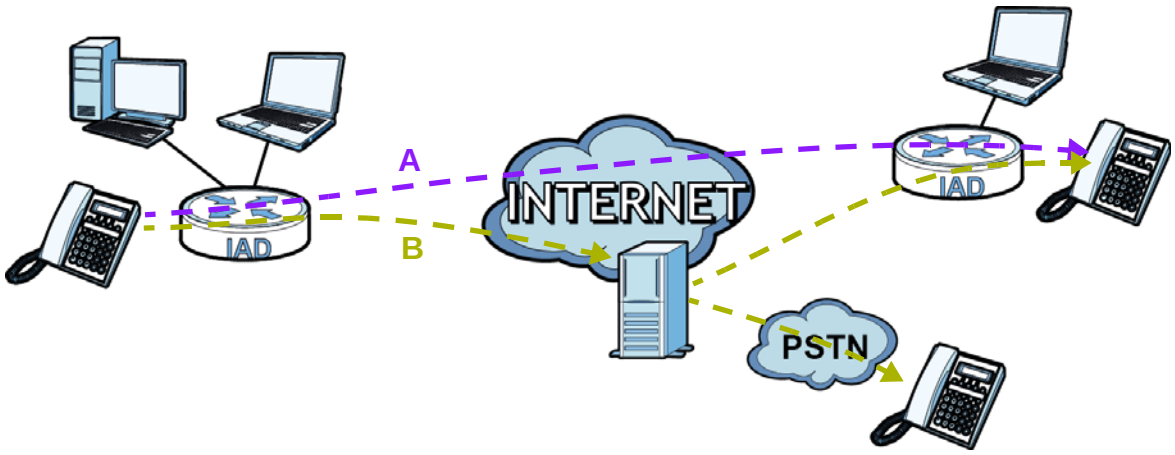
## 1.2.2 Wireless LAN (Wi-Fi) Connection

The LTE3311 is a wireless Access Point (AP) for wireless clients, such as notebook computers or PDAs and iPads. It allows them to connect to the Internet without having to rely on inconvenient Ethernet cables. By default, the wireless LAN (WLAN) is enabled on the LTE3311.

## 1.2.3 Internet Call (VoIP)

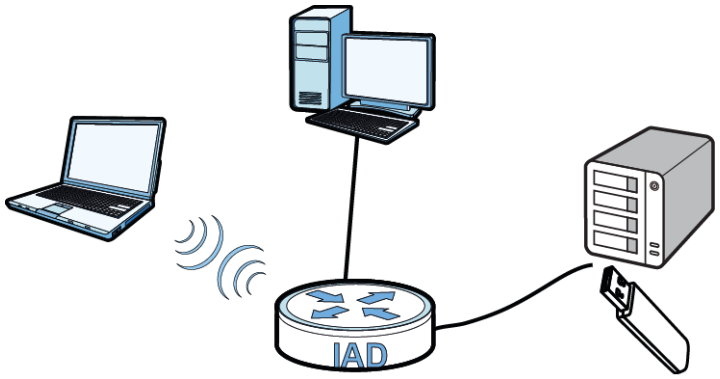
You can register a SIP (Session Initiation Protocol) account and use the LTE3311 and a connected analog telephone to make and receive VoIP telephone calls.

- Peer-to-peer calls (**A**): Use the LTE3311 to make a call to the recipient's IP address without using a SIP proxy server.
- Calls via a VoIP service provider (**B**): The LTE3311 sends your call to a VoIP service provider's SIP server which forwards your calls to either VoIP or PSTN phones.




## 1.2.4 File Sharing

Use the built-in USB 2.0 port to share files on a USB memory stick or a USB hard drive (B). You can connect one USB hard drive to the LTE3311 at a time. Use FTP to access the files on the USB device.




# 1.3 Ways to Manage the LTE3311

Use any of the following methods to manage the LTE3311.

- WPS (Wi-Fi Protected Setup). You can use the WPS button or the WPS section of the Web Configurator to set up a wireless network with your LTE3311.
- Web Configurator. This is recommended for everyday management of the LTE3311 using a (supported) web browser.

# 1.4 Good Habits for Managing the LTE3311

Do the following things regularly to make the LTE3311 more secure and to manage the LTE3311 more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). See Section 24.7 on page 167. 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 LTE3311 to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the LTE3311. You could simply restore your last configuration.

# 1.5 Resetting the LTE3311

If you forget your password or IP address, or you cannot access the Web Configurator, you will need to use the **RESET** button at the back of the LTE3311 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" (see Section 24.4 on page 163) and the IP address will be reset to "192.168.1.1".

### 1.5.1 How to Use the RESET Button

1. Make sure the power LED is on.
2. Press the **RESET** button for one to four seconds to restart/reboot the LTE3311.
3. Press the **RESET** button for longer than ten seconds to set the LTE3311 back to its factory-default configurations.

## 1.6 The WPS Button

Your LTE3311 supports Wi-Fi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the Wi-Fi Alliance.

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

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

You can use the WPS button (  ) on the top panel of the LTE3311 to activate WPS in order to quickly set up a wireless network with strong security.

1. Make sure the power LED is on (not blinking).
2. Press the WPS button for more than three seconds and release it. Press the WPS button on another WPS-enabled device within range of the LTE3311.

Note: You must activate WPS in the LTE3311 and in another wireless device within two minutes of each other.

For more information on using WPS, see Section 4.2 on page 34.

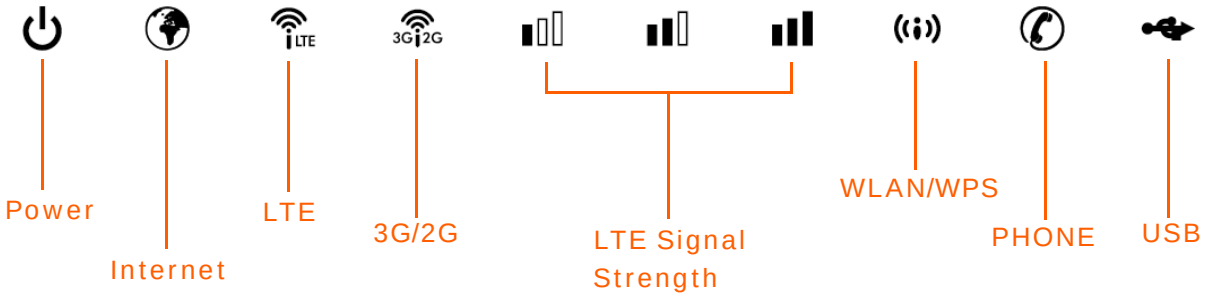
## 1.7 SIM Card Slot

The LTE3311 comes with a built-in 3G/4G module for 3G/4G connections. To set up a 3G/4G connection using the built-in 3G/4G module, just insert a 3G/4G SIM card into the SIM card slot at the back of the LTE3311.

Note: You must insert the 4G SIM card into the card slot before turning on the LTE3311.

# 1.8 LEDs

**Figure 1** Front Panel




The following table describes the LEDs.

**Table 1** Front panel LEDs

| LED | COLOR | STATUS | DESCRIPTION |
|---|---|---|---|
| Power | Green | On | The LTE3311 is receiving power and functioning properly. |
| | | Blinking | The LTE3311 is in the process of starting up or default restoring. |
| | Off | | The LTE3311 is not receiving power. |
| Internet | Green | On | The LTE3311's WAN connection is ready. |
| | | Blinking | The LTE3311 is sending/receiving data through the WAN. |
| | Off | | The WAN connection is not ready, or has failed. |
| LTE | Green | On | The LTE3311 is registered and successfully connected to a 4G network. |
| | | Blinking | The LTE3311 is looking for an available 4G network. |
| | Off | | There is no SIM card inserted, the SIM card is invalid, the PIN code is not correct or there is no service. |
| 3G/2G | Green | On | The LTE3311 is registered and successfully connected to a 3G/2G network. |
| | | Blinking | The LTE3311 is looking for an available 3G/2G network. |
| | Off | | There is no SIM card inserted, the SIM card is invalid, the PIN code is not correct or there is no service. |
| LTE Signal Strength | Green | On | A valid SIM card is inserted and the wireless WAN interface is enabled.<br>Three bars:<br>Signal strength: Excellent<br>RSRP (Reference Signal Receiving Power) >= -79 dBm<br>Two bars:<br>Signal strength: Fair<br>-81 dBm >= RSRP >= -95 dBm<br>One bar:<br>Signal strength: Poor<br>-97 dBm > RSRP |
| | Red | Blinking | There is no LTE signal because there is no valid SIM card inserted and/or the wireless WAN interface is disabled. |

**Table 1** Front panel LEDs (continued)

| LED | COLOR | STATUS | DESCRIPTION |
|---|---|---|---|
| WLAN/WPS | Green | On | The LTE3311 is ready and the 2.4GHz wireless LAN is on, but is not sending/receiving data through the wireless LAN. |
| | | Blinking (slow) | The LTE3311 is sending/receiving data through the wireless LAN. |
| | | Blinking (fast) | The LTE3311 is negotiating a WPS connection with a wireless client. |
| | Off | | The wireless LAN is not ready or has failed or WPS is disabled. |
| Phone | Green | On | A SIP account is registered for the phone port. |
| | | Blinking | A telephone connected to the phone port has its receiver off of the hook or there is an incoming call. |
| | Orange | On | A SIP account is registered for the phone port and there is a voice message in the corresponding SIP account. |
| | | Blinking | A telephone connected to the phone port has its receiver off of the hook and there is a voice message in the corresponding SIP account. |
| | Off | | The phone port does not have a SIP account registered. |
| USB | Green | On | The LTE3311 has a USB device installed and the 3G connection is up. |
| | | Blinking | The LTE3311 is sending/receiving data to/from the USB device connected to it. |
| | Off | | There is no USB device installed or the LTE3311 does not detect a USB connection. |

# 1.9 Wall Mounting

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

**Table 2** Wall Mounting Information

| | |
|---|---|
| Distance between holes | 11 cm |
| M4 Screws | Two |
| Screw anchors (optional) | Two |

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

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

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

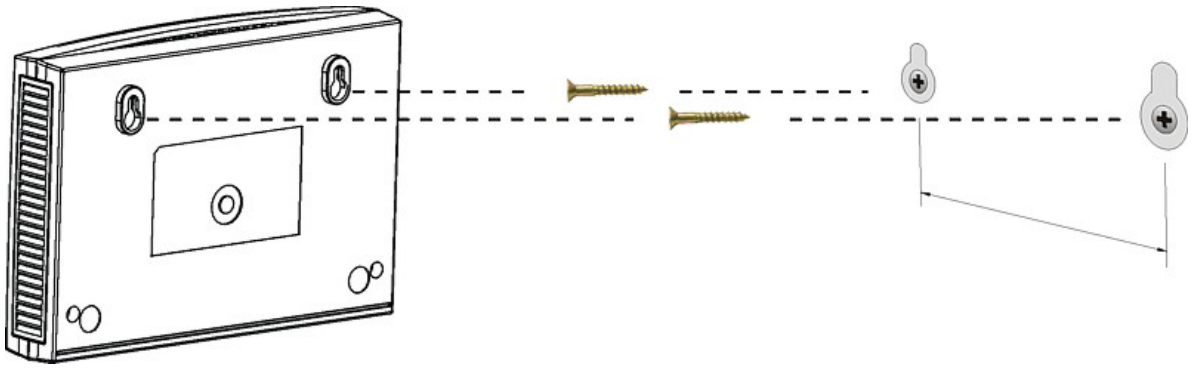
3 If using screw anchors, drill two holes for the screw anchors into the wall. Push the anchors into the full depth of the holes, then insert the screws into the anchors. Do not insert the screws all the way in - leave a small gap of about 0.5 cm.

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 LTE3311 with the connection cables.

5 Align the holes on the back of the LTE3311 with the screws on the wall. Hang the LTE3311 on the screws.

**Figure 2** Wall Mounting Example



# 2

# Introducing the Web Configurator

## 2.1 Overview

This chapter describes how to access the LTE3311 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 LTE3311 via Internet browser. Use Internet Explorer 9.0 and later versions, Mozilla Firefox 21 and later versions, Safari 6.0 and later versions or Google Chrome 26.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the Web Configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

Refer to the Troubleshooting chapter (Chapter 25 on page 170) to see how to make sure these functions are allowed in Internet Explorer.

## 2.2 Accessing the Web Configurator

1. Make sure your LTE3311 hardware is properly connected and prepare your computer or computer network to connect to the LTE3311 (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 3** Login screen


The following table describes the labels in this screen.

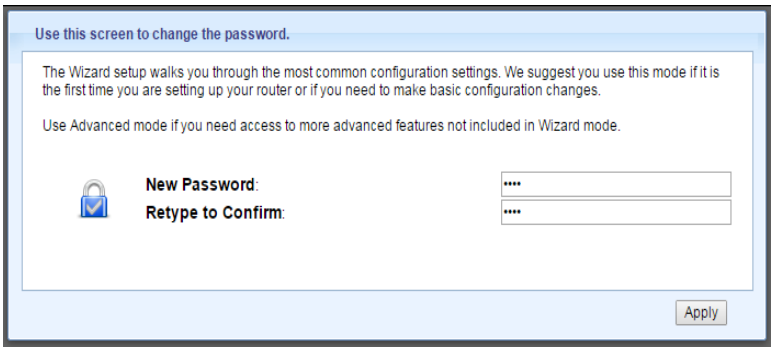
**Table 3** Login screen

| 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 4** Change Password Screen



The following table describes the labels in this screen.

**Table 4** Change Password Screen

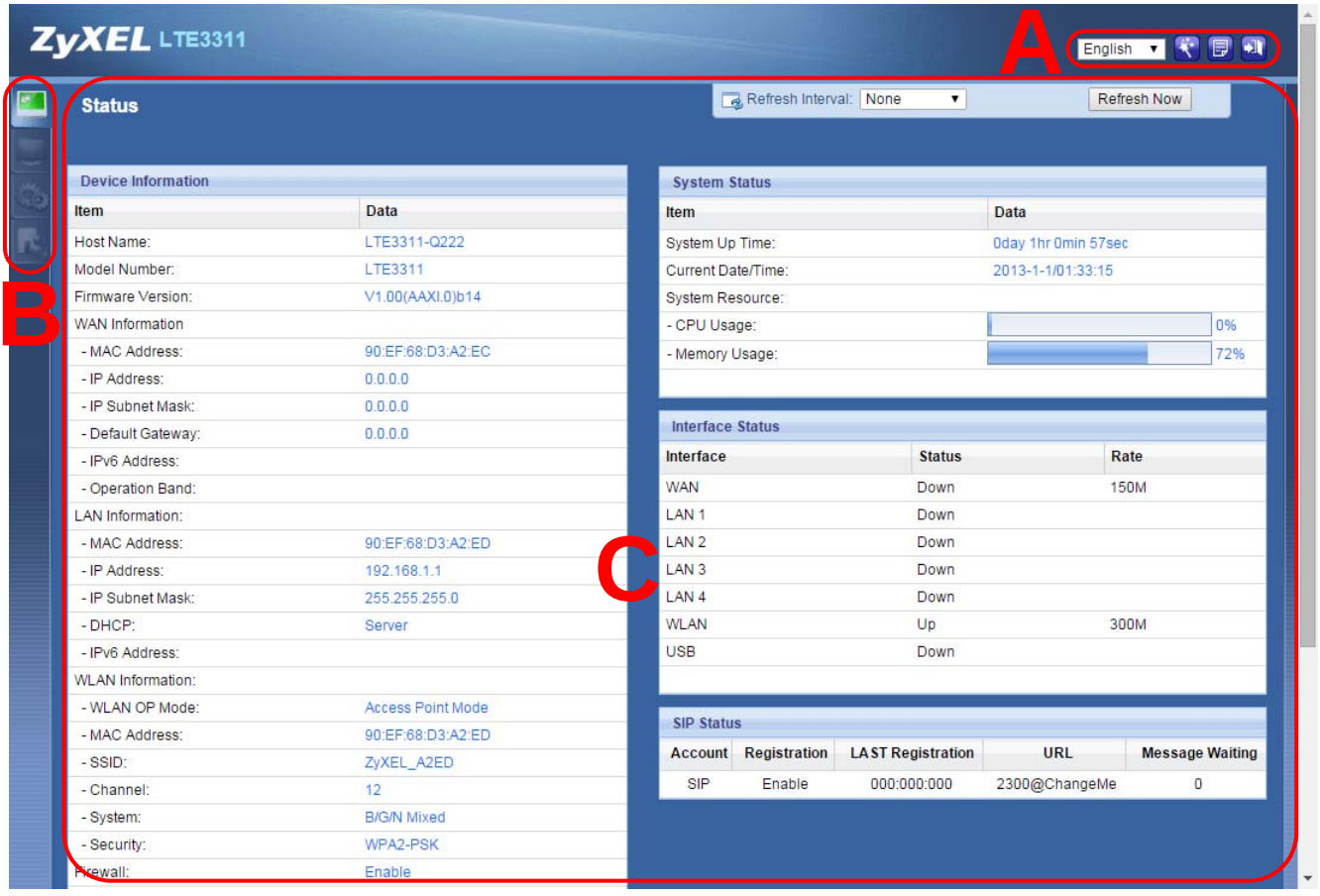
| LABEL | DESCRIPTION |
|---|---|
| New Password | Type a new password. |
| Retype to Confirm | Retype the password for confirmation. |
| Apply | Click **Apply** to save your changes back to the LTE3311. |

Note: The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes; go to Chapter 24 on page 162 to change this). Simply log back into the LTE3311 if this happens.

## 2.3 The Main Screen

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

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




- **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 6** Title Bar


The icons provide the following functions.

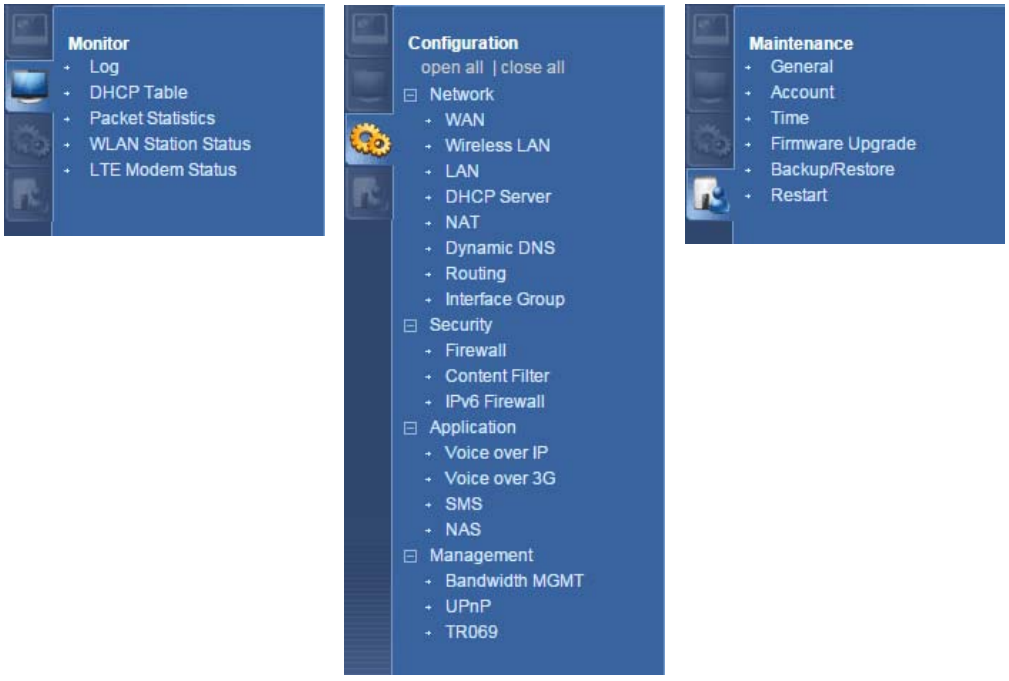
**Table 5** Title Bar: Web Configurator Icons

| LABEL | DESCRIPTION |
|---|---|
| English | Select the language you prefer. |
| Wizard | Click this icon to open the setup wizard for the LTE3311. |
| 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. |

## 2.3.2 Navigation Panel

Use the sub-menus on the navigation panel to configure LTE3311 features.

**Figure 7** Navigation Panel



The following table describes the sub-menus.

**Table 6** Navigation Panel

| LINK | TAB | FUNCTION |
|---|---|---|
| Status | | This screen shows the LTE3311's general device, system and interface status information. Use this screen to access the summary statistics tables. |
| **Monitor** | | |
| Log | View Log | Use this screen to view the list of activities recorded by your LTE3311. |
| | Log Setting | Use this screen to configure which logs to display. |
| DHCP Table | DHCP Table | Use this screen to view current DHCP client information. |
| Packet Statistics | Packet Statistics | Use this screen to view port status and packet specific statistics. |
| WLAN Station Status | Association List | Use this screen to view the wireless stations that are currently associated to the LTE3311's 2.4GHz wireless LAN. |
| LTE Modem Status | LTE Modem Status | Use this screen to view the detailed information about the LTE module, cellular interface, and SIM card. You can also view the LTE connection status. |
| **Configuration** | | |
| Network | | |
| 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 LTE3311 is connected and how you want the LTE3311 to connect to an available mobile network. |
| | IPv6 | Use this screen to configure the LTE3311's IPv6 settings. |
| | PIN Management | Use this screen to enable PIN code authentication and enter the PIN code. |
| Wireless LAN | General | Use this screen to enable the wireless LAN and configure wireless LAN and wireless security settings. |
| | More AP | Use this screen to configure multiple BSSs on the LTE3311. |
| | MAC Filter | Use the MAC filter screen to allow or deny wireless stations based on their MAC addresses from connecting to the LTE3311. |
| | 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 LTE3311'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. |

**Table 6** Navigation Panel (continued)

| LINK | TAB | FUNCTION |
|---|---|---|
| NAT | General | Use this screen to enable NAT. |
| | Port Forwarding | Use this screen to configure servers behind the LTE3311 and forward incoming service requests to the server(s) on your local network. |
| | Port Trigger | Use this screen to change your LTE3311's port triggering settings. |
| | ALG | Use this screen to enable or disable SIP (VoIP) ALG (Application Layer Gateway) in the LTE3311. |
| 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 LTE3311. |
| 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 | | |
| Voice over IP | General | Use this screen to enable VoIP, NAT traversal and dialing plan on the LTE3311. |
| | Phone Book | Use this screen to manage your VoIP contact names and phone numbers. |
| | Speed Dial | Use this screen to set up shortcuts for dialing frequently-used (VoIP) phone numbers. |
| | Phone Conf. | Use this screen to configure call features. |
| | SIP Conf. | Use this screen to set up information about your SIP account, and configure the SIP server information. |
| Voice over 3G | General | Use this screen to enable Vo3G on the LTE3311. |
| | Phone Book | Use this screen to manage your Vo3G contact names and phone numbers. |
| | Telephone Conf. | Use this screen to configure call features. |
| | Call Conf. | Use this screen to maintain rules for handling incoming calls. |
| SMS | SMS | Use this screen to send new messages and view messages received on the LTE3311. |
| NAS | File Sharing | Use this screen to allow file sharing via the LTE3311 using Windows Explorer, the workgroup name. |
| | FTP | Use this screen to allow file sharing via the LTE3311 using FTP. |
| Management | | |
| 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 LTE3311. |
| TR069 | TR069 | Use this screen to configure your LTE3311 to be managed by an ACS. |

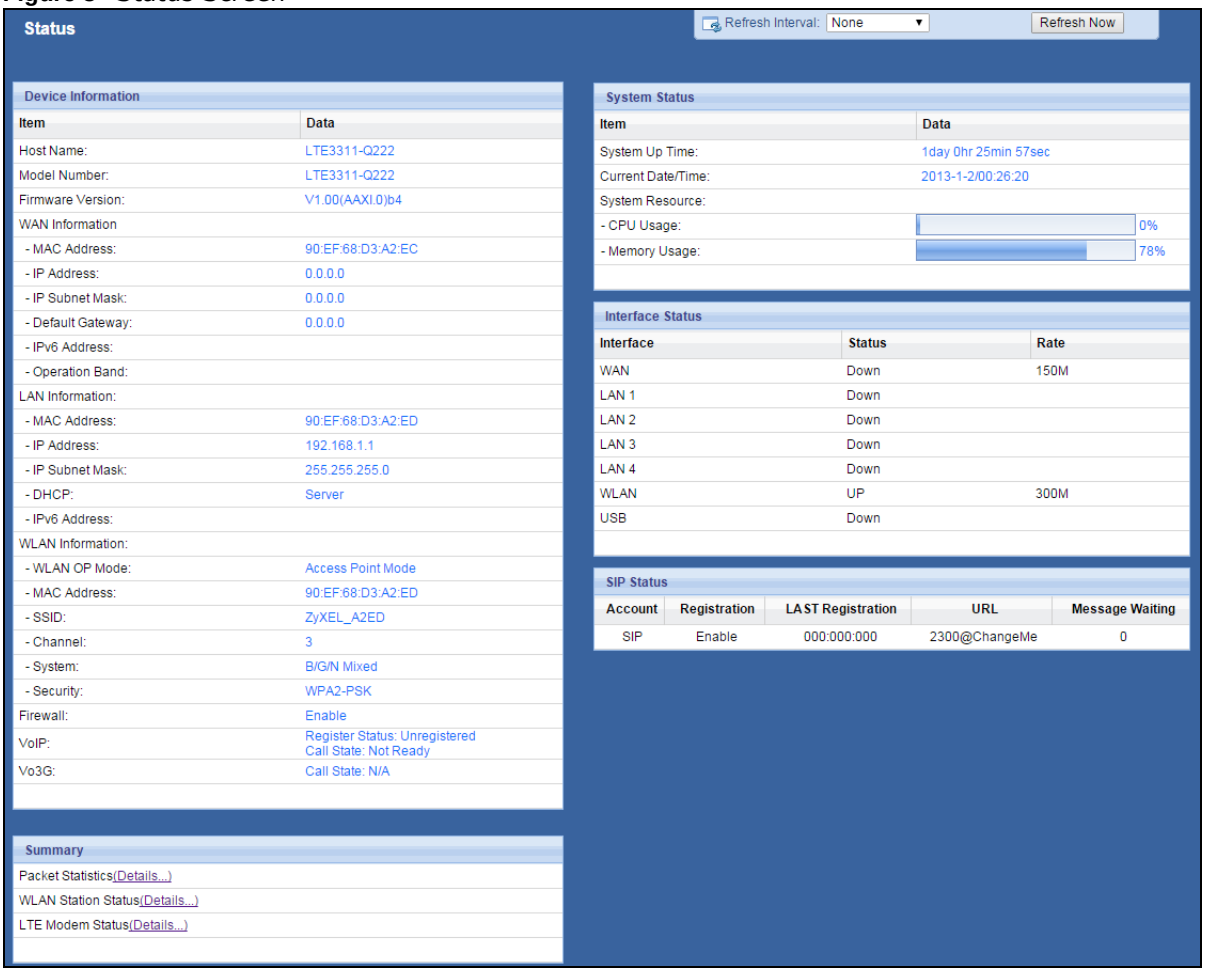
**Table 6** Navigation Panel (continued)

| LINK | TAB | FUNCTION |
|---|---|---|
| **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 LTE3311. |
| Time | Time Setting | Use this screen to change your LTE3311's time and date. |
| Firmware Upgrade | Firmware Upgrade | Use this screen to upload firmware to your LTE3311. |
| Backup/ Restore | Backup/ Restore | Use this screen to backup and restore the configuration or reset the factory defaults to your LTE3311. |
| Restart | System Restart | This screen allows you to reboot the LTE3311 without turning the power off. |

# 2.4 Status Screen

Click  to open the status screen.

**Figure 8** Status Screen



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

**Table 7** Status Screen Icon Key

| ICON | DESCRIPTION |
|---|---|
|   | 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. |
|  | Click this icon to see the **Status** page. The information in this screen depends on the device mode you select. |
|  | Click this icon to see the **Monitor** navigation menu. |
|  | Click this icon to see the **Configuration** navigation menu. |
|  | Click this icon to see the **Maintenance** navigation menu. |

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

**Table 8** 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 device. |
| IP Address | This shows the WAN port's IP address. |
| IP Subnet Mask | This shows the WAN port's subnet mask. |
| Default Gateway | This shows the WAN port's gateway IP address. |
| IPv6 Address | This shows the IPv6 address of the LTE3311 on the WAN. |
| Operation Band | This shows the network type and the frequency band used by the mobile network to which the LTE3311 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 LTE3311 on the LAN. |
| WLAN Information | |
| WLAN OP Mode | This is the device mode to which the LTE3311'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 LTE3311 in the 2.4GHz wireless LAN. |
| Channel | This shows the channel number which you select manually. |
| System | This shows the wireless standards the LTE3311 supports. |
| Security | This shows the level of wireless security the LTE3311 is using. |
| Firewall | This shows whether the firewall is enabled or not. |

**Table 8** Status Screen (continued)

| LABEL | DESCRIPTION |
|---|---|
| VoIP | This shows the current registration status of the SIP account. It also shows the current state of the phone call.<br>• **ready**: VoIP is enabled and a SIP account is registered for the phone port.<br>• **not ready**: VoIP is disabled or there is no SIP account registered for the phone port.<br>• **busy**: There is a VoIP call in progress or the callee's line is busy.<br>• **ringing**: The phone is ringing for an incoming VoIP call.<br>• **dialing**: The callee's phone is ringing.<br>• **off hook**: The callee hung up or your phone was left off the hook. |
| Vo3G | This shows the current state of the phone call.<br>• **ready**: Voice over 3G (Vo3G) is enabled and the 3G connection is up.<br>• **not ready**: Voice over 3G (Vo3G) is disabled and the 3G connection is down.<br>• **busy**: There is a Vo3G call in progress or the callee's line is busy.<br>• **ringing**: The phone is ringing for an incoming Vo3G call.<br>• **dialing**: The callee's phone is ringing.<br>• **off hook**: The callee hung up or your phone was left off the hook.<br>**N/A** means Voice over 3G (Vo3G) is disabled. |
| Summary | |
| Packet Statistics | Click **Details...** to go to the **Monitor > Packet Statistics** screen (Section 5.5 on page 48). 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 5.6 on page 49). Use this screen to view the wireless stations that are currently associated to the LTE3311's 2.4GHz wireless LAN. |
| LTE Modem Status | Click **Details...** to go to the **Monitor > LTE Modem Status** screen (Section 5.7 on page 50). 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. |
| System Status | |
| Item | This column shows the type of data the LTE3311 is recording. |
| Data | This column shows the actual data recorded by the LTE3311. |
| System Up Time | This is the total time the LTE3311 has been on. |
| Current Date/Time | This field displays your LTE3311's present date and time. |
| System Resource | |
| - CPU Usage | This displays what percentage of the LTE3311's processing ability is currently used. When this percentage is close to 100%, the LTE3311 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 LTE3311 is using. |
| Interface Status | |
| Interface | This displays the LTE3311 port types. The port types are: **WAN**, **LAN** and **WLAN**. |
| Status | For the LAN and WAN ports, this field displays **Down** (line is down) or **Up** (line is up or connected).<br>For the 2.4GHz WLAN, it displays **Up** when the 2.4GHz WLAN is enabled or **Down** when the 2.4G WLAN is disabled.<br>For the USB port, it displays **Up** when the LTE3311 detects a USB connection or **Down** when there is no USB device attached or the LTE3311 does not detect a USB connection. |

**Table 8** Status Screen (continued)

| LABEL | DESCRIPTION |
|---|---|
| Rate | For the LAN ports, this displays the port speed or is left blank when the line is disconnected.<br>For the WAN port, it always displays the maximum transmission rate.<br>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.<br>For the USB port, it displays the port speed or is left blank when the line is disconnected. |
| SIP Status | |
| Account | This displays each SIP account in the LTE3311. |
| Registration | This displays whether the SIP account is enabled or not. |
| LAST Registration | This field displays the last time you successfully registered the SIP account. |
| URL | This displays the account number and service domain of the SIP account. You can change these in the **Application > Voice over IP > SIP Conf. > Service Domain Conf.** screens. |
| Message Waiting | This field indicates whether or not there are any messages waiting for the SIP account. |

# 3

# Setup Wizard

## 3.1 Overview

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

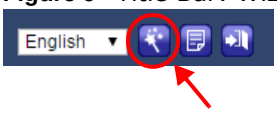
The Web Configurator's wizard helps you configure your device to access the Internet and change the wireless LAN settings. Refer to your ISP for your Internet account information. Leave a field blank if you don't have that information.

## 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.

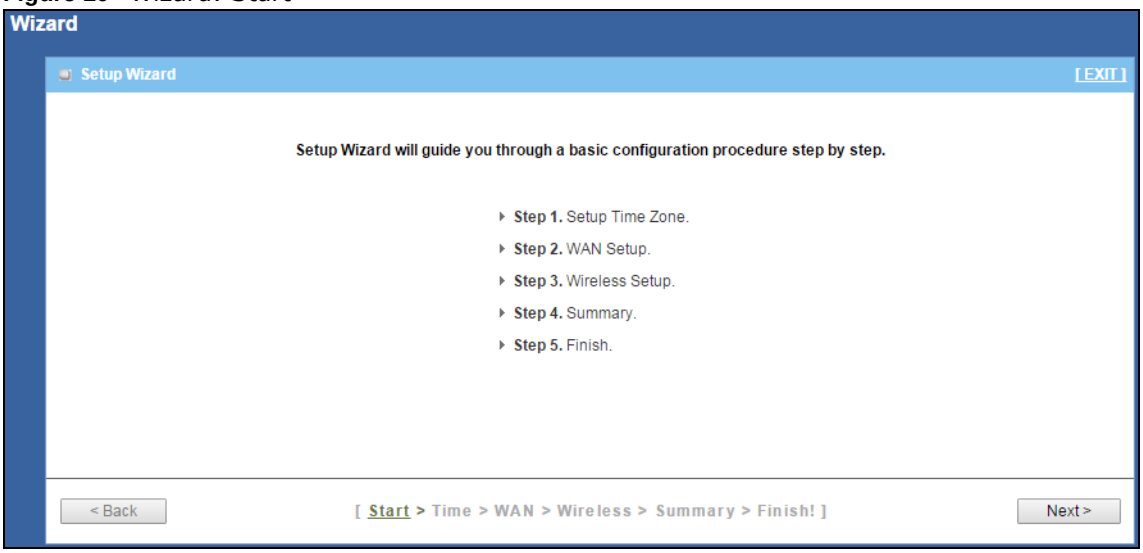
**Figure 9** Title Bar: Wizard icon




## 3.3 Wizard Setup

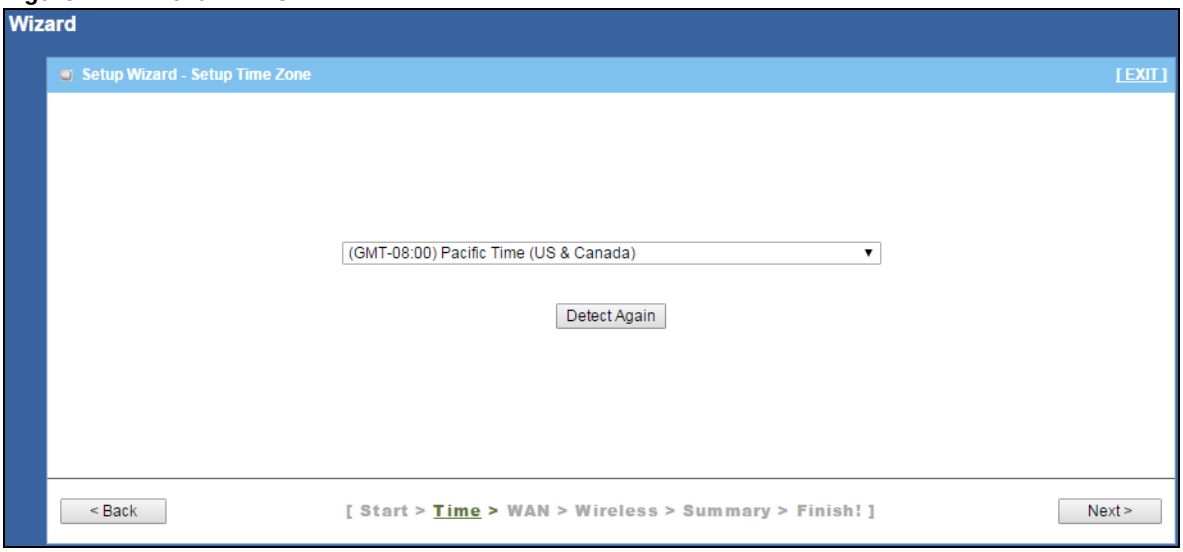
1 The first wizard screen displays showing the main steps in the wizard setup. Click **Next** to proceed with the time zone setup screen.

**Figure 10** Wizard: Start




2 The LTE3311 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 LTE3311's location and click **Next**.

**Figure 11** Wizard: Time

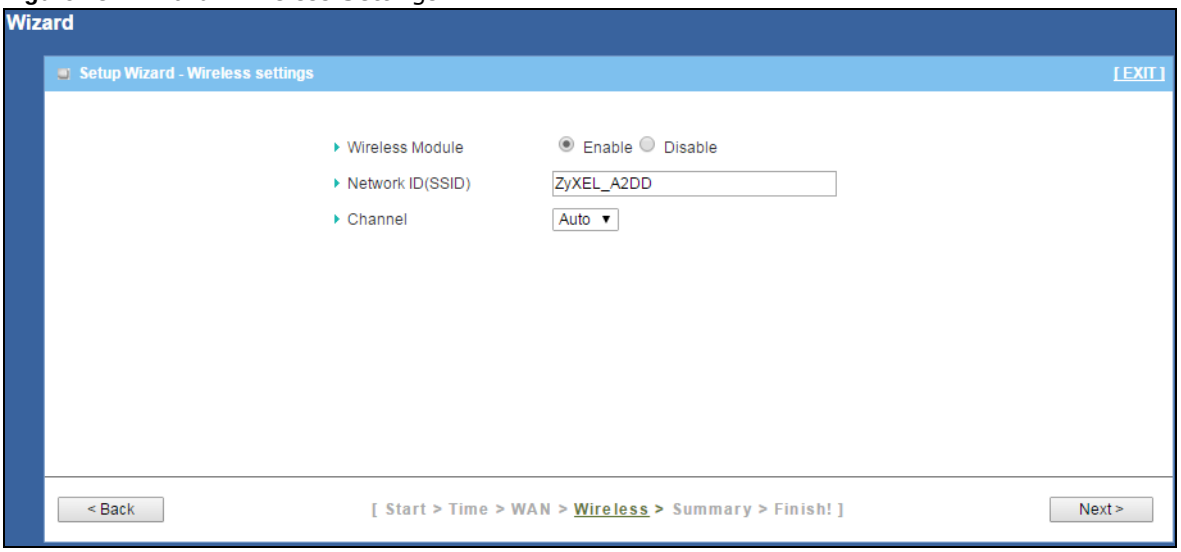



3 Enter your APN (Access Point Name) provided by your service provider. Select the country where the LTE3311 is located and your service provider name. Click **Next**.

**Figure 12** Wizard: WAN

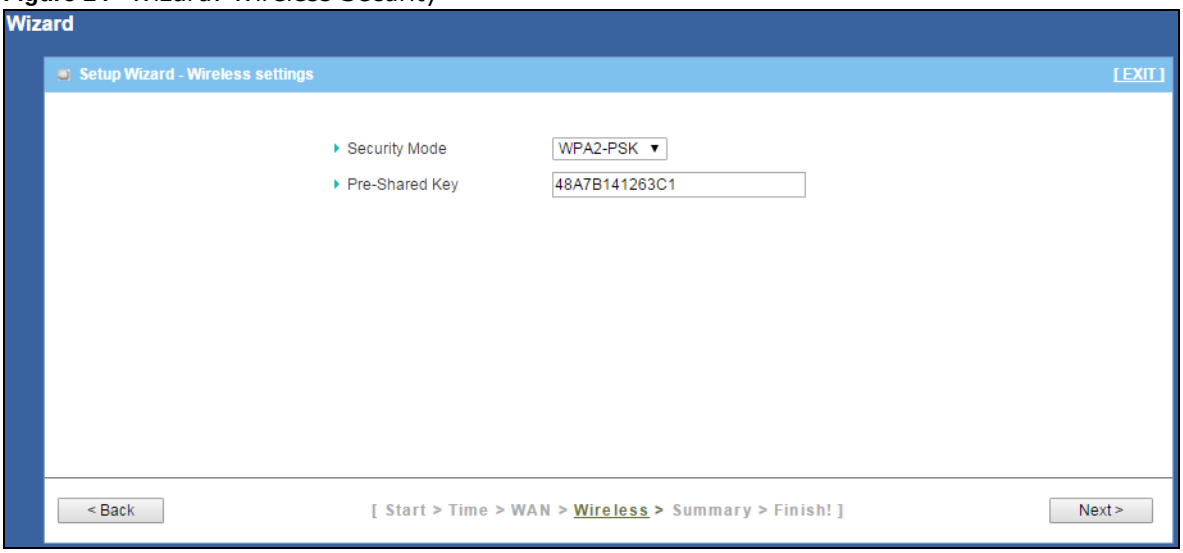

4 Use this screen to enable or disable the LTE3311's wireless LAN, and enter the wireless network name (SSID). Select a channel or use **Auto** to have the LTE3311 automatically determine a channel to use. Click **Next**.

**Figure 13** Wizard: Wireless Settings



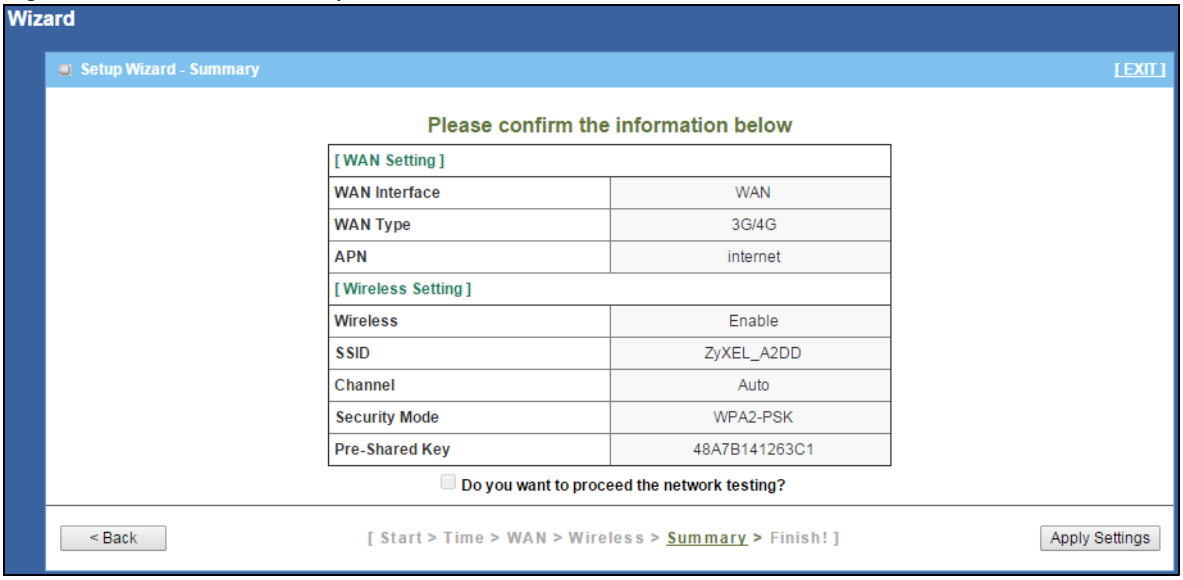

5 Select **WPA2-PSK** and enter a pre-shared key from 8 to 63 case-sensitive characters for data encryption. The wireless clients which want to associate with this wireless network must have the same wireless security settings. Otherwise, select **No Security** to allow any client to associate with this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

**Figure 14** Wizard: Wireless Security



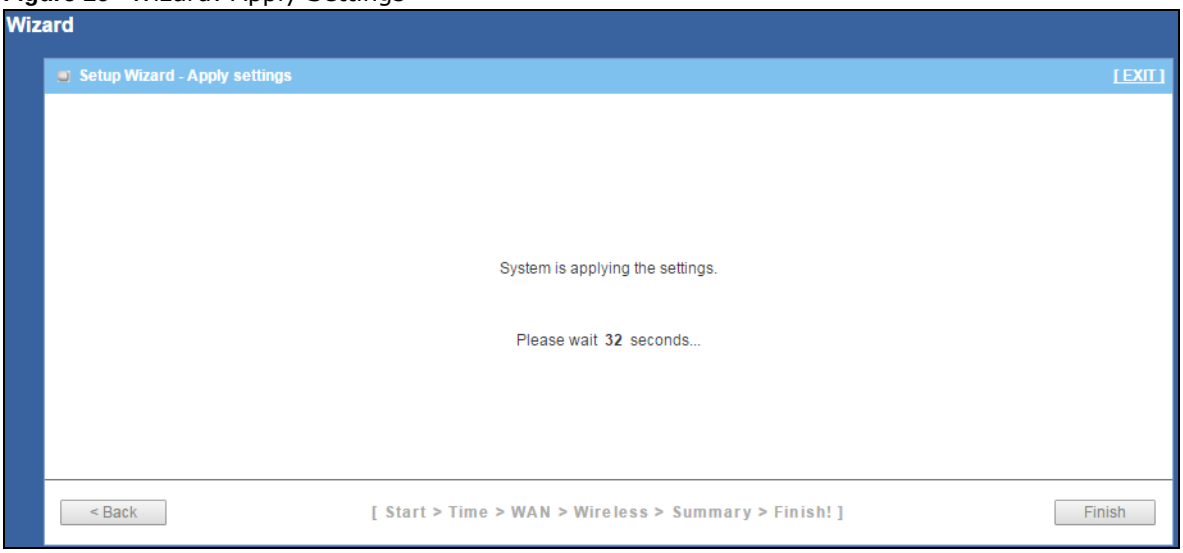

6 Use the read-only summary table to check whether what you have configured is correct. Click **Apply Settings** to save your settings. Otherwise, click **Back** to go back to the previous screens.

**Figure 15** Wizard: Summary



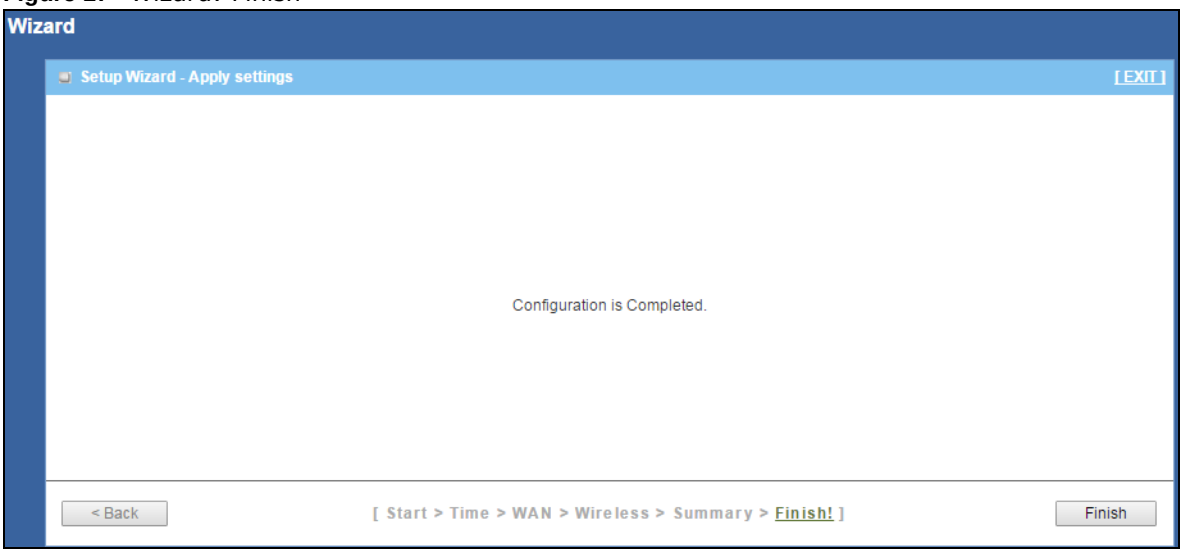

7 The system takes about 35 seconds to apply settings.

**Figure 16** Wizard: Apply Settings




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

**Figure 17** Wizard: Finish




You are now ready to connect wirelessly to your LTE3311 and access the Internet.

# 4

# Tutorials

## 4.1 Overview

This chapter provides tutorials for setting up your LTE3311.

- Set Up a Wireless Network Using WPS
- Connect to LTE3311 Wireless Network without WPS
- Using Multiple SSIDs on the LTE3311

## 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 LTE3311 as the AP and NWD210N as the wireless client which connects to a notebook.

Note: The wireless client must be a WPS-aware device (for example, a WPS USB adapter or PCI card).

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 LTE3311'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 LTE3311 is turned on. Make sure the **WIFI** button (at the back panel of the LTE3311) is pushed in, and that the device is placed within range of your notebook.
2. Make sure that you have installed the wireless client (this example uses the NWD210N) driver and utility in your notebook.
3. In the wireless client utility, find the WPS settings. Enable WPS and press the WPS button (**Start** or **WPS** button).
4. Log into LTE3311's Web Configurator and press the **Push Button** in the **Configuration > Network > Wireless LAN 2.4G > WPS Station** screen.

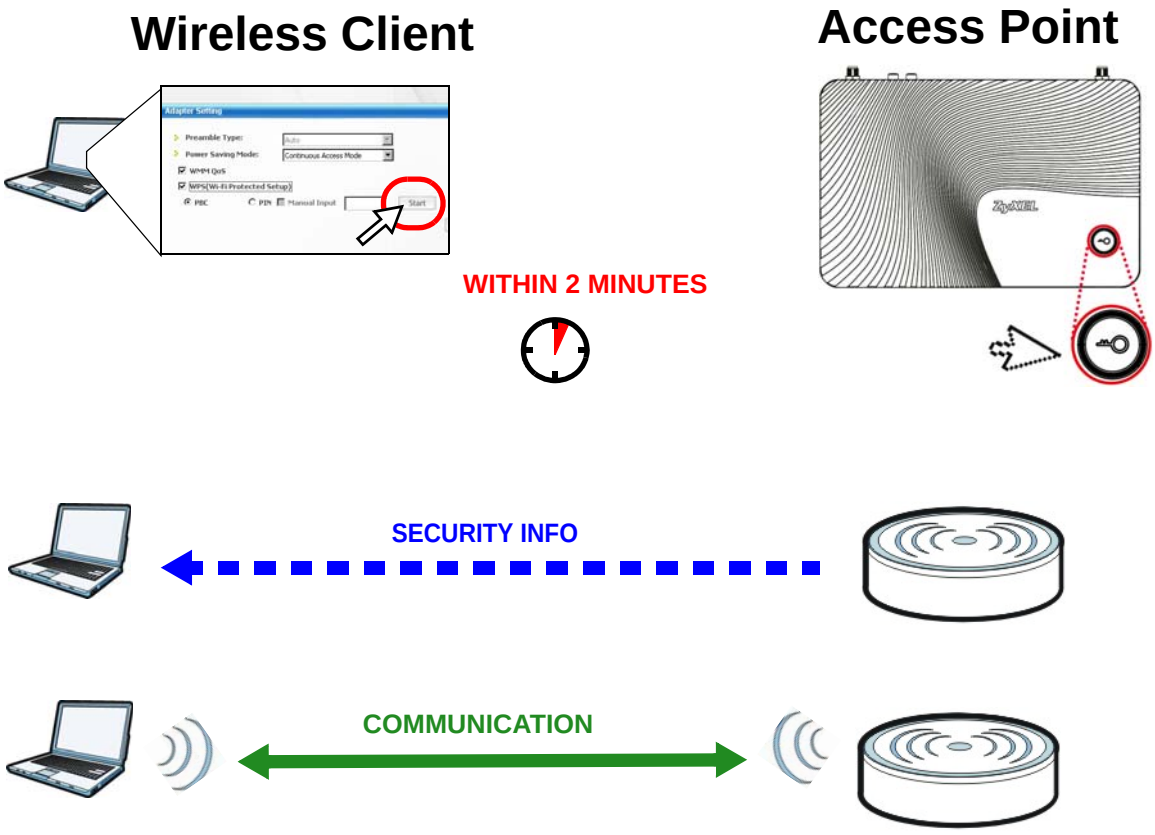
Note: Your LTE3311 has a WPS button located on its panel, as well as a WPS button in its configuration utility. Both buttons have exactly the same function; you can use one or the other.

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 LTE3311 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 LTE3311 securely.

The following figure shows you an example to set up wireless network and security by pressing a button on both LTE3311 and wireless client (the NWD210N in this example).

**Figure 18** Example WPS Process: PBC Method




## 4.2.2 PIN Configuration

When you use the PIN configuration method, you need to use both LTE3311's configuration interface and the client's utilities.

1 Launch your wireless client's configuration utility. Go to the WPS settings and select the PIN method to get a PIN number.

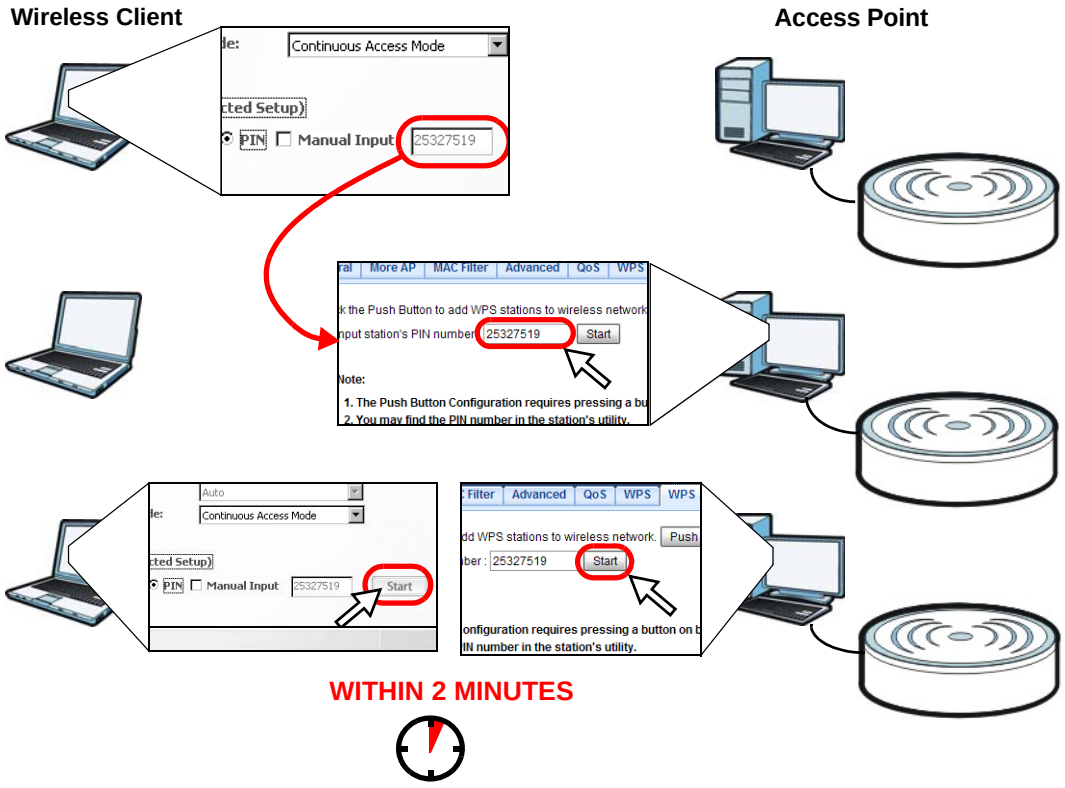
2 Enter the PIN number to the **PIN** field in the **Configuration > Network > Wireless LAN > WPS Station** screen on the LTE3311.

3 Click **Start** buttons (or button next to the PIN field) on both the wireless client utility screen and the LTE3311's **WPS Station** screen within two minutes.

The LTE3311 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 LTE3311 securely.

The following figure shows you the example to set up wireless network and security on LTE3311 and wireless client (ex. NWD210N in this example) by using PIN method.

**Figure 19** Example WPS Process: PIN Method




# 4.3 Connect to LTE3311 Wireless Network without WPS

This example shows you how to configure wireless security settings with the following parameters on your LTE3311 and connect your computer to the LTE3311 wireless network.

| | |
|---|---|
| **SSID** | SSID_Example3 |
| **Channel** | 6 |
| **Security** | WPA2-PSK<br>(Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey) |

Follow the steps below to configure the wireless settings on your LTE3311.

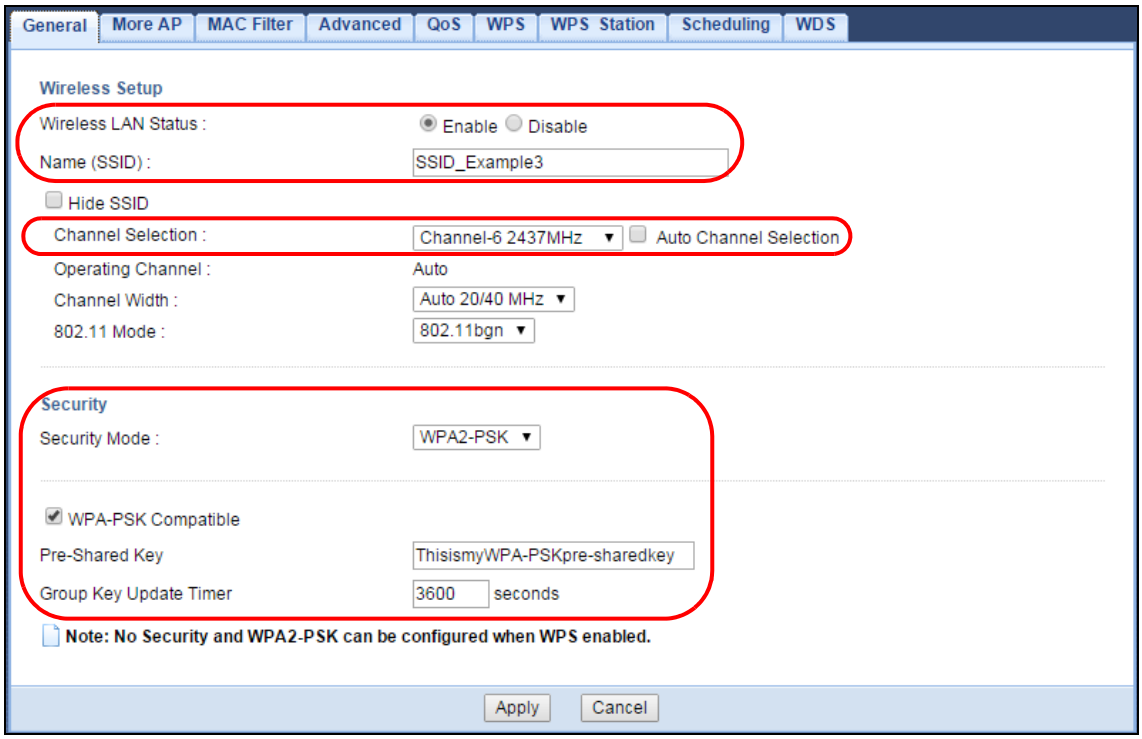
The instructions require that your hardware is connected (see the Quick Start Guide) and you are logged into the Web Configurator through your LAN connection (see Section 2.2 on page 19).

1 Make sure the **WIFI** switch (at the back panel of the LTE3311) is set to **ON**.

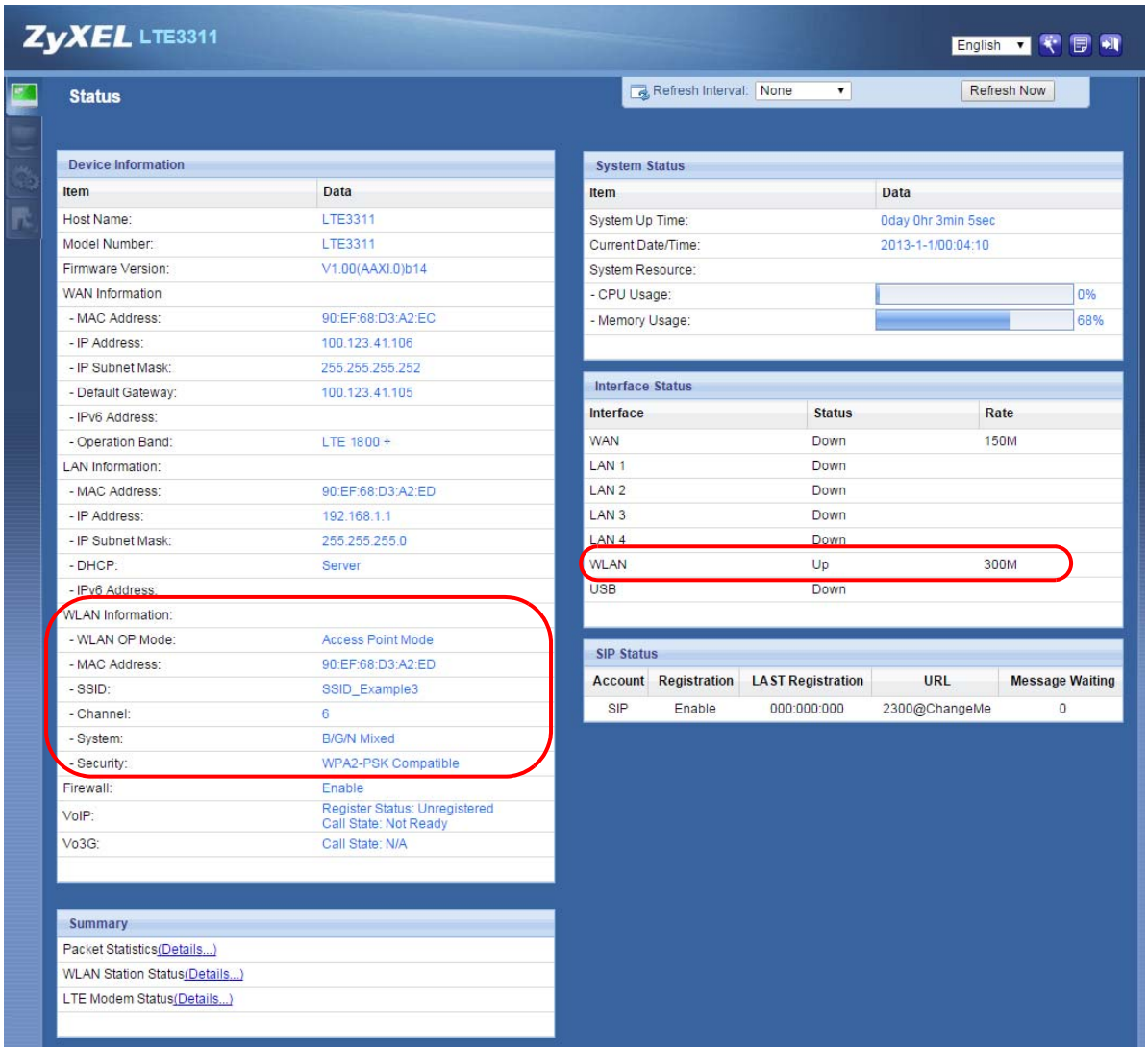
2 Open the **Configuration > Network** > **Wireless LAN > General** screen in the AP's Web Configurator.

3 Confirm that the wireless LAN is enabled on the LTE3311.

4 Enter **SSID_Example3** as the SSID and select **Channel-06** as the channel. Set security mode to **WPA2-PSK** and enter **ThisismyWPA-PSKpre-sharedkey** in the **Pre-Shared Key** field. Click **Apply**.



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




## 4.3.1 Configure Your Notebook

Note: In this example, we use the ZyXEL NWD6505 wireless adapter as the wireless client and use the Windows built-in utility (Windows Zero Configuration (WZC)) to connect to the wireless network.

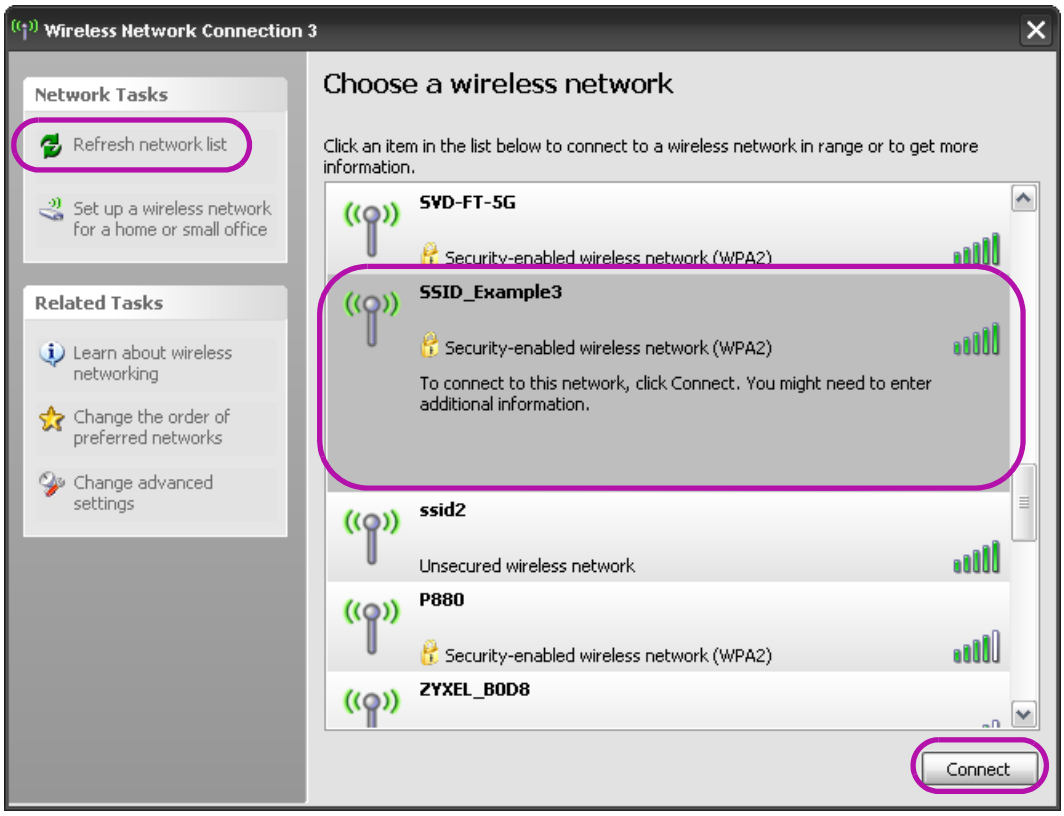
1 The LTE3311 supports IEEE 802.11b, IEEE 802.11g, and IEEE 802.11n wireless clients. Make sure that your notebook or computer's wireless adapter supports one of these standards.

2 Wireless adapters come with software sometimes called a "utility" that you install on your computer. See your wireless adapter's User's Guide for information on how to do that.

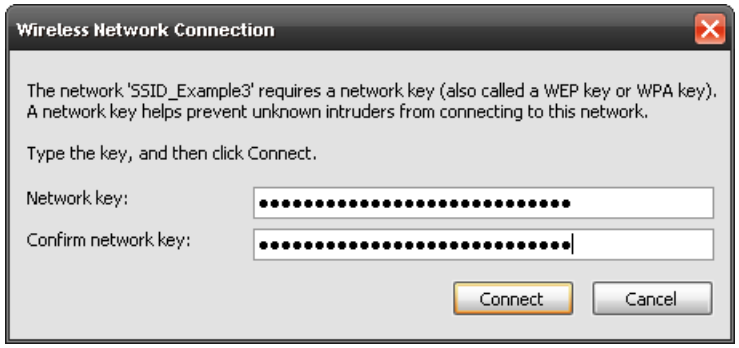
3 After you've installed the driver and attached the NWD6505 to your computer's USB port, right-click the **Wireless Network Connection** icon in your computer's system tray, select and click **View Available Wireless Networks**.


4 The **Wireless Network Connection** screen displays. Click **Refresh network list** to view the available wireless APs within range.

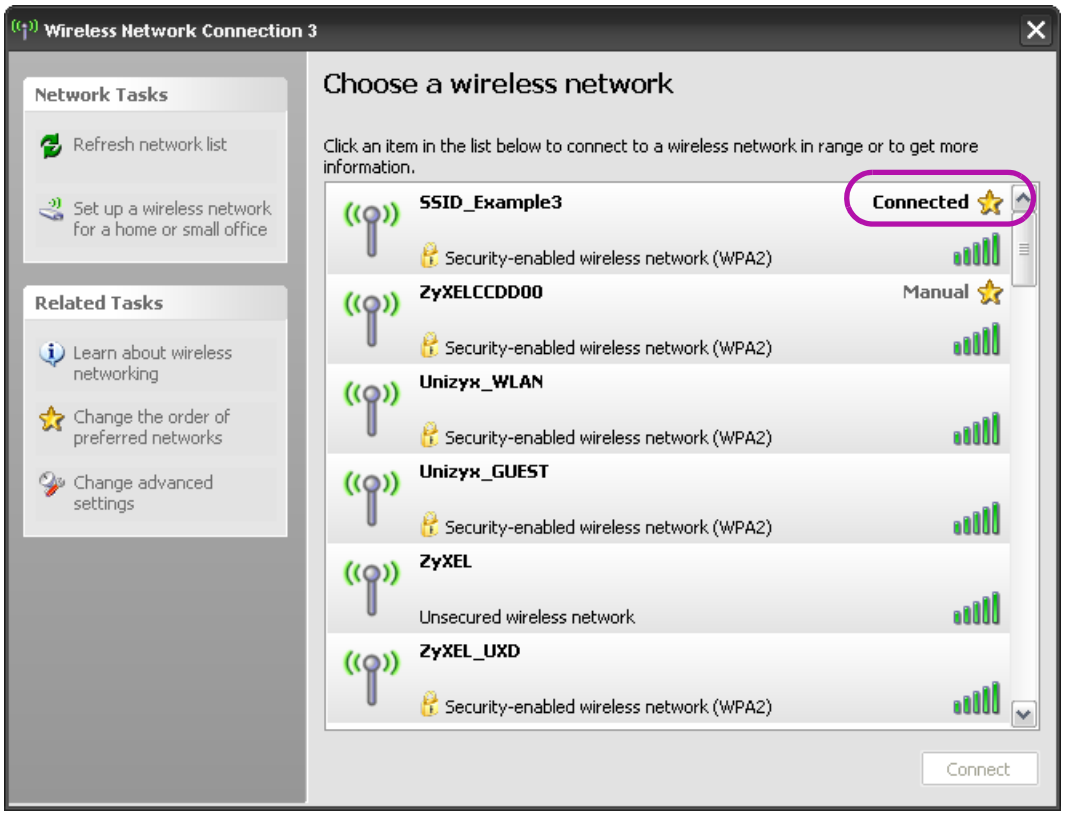
5 Select **SSID_Example3** and click **Connect**.




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



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




8 If the wireless client keeps trying to connect to or acquiring an IP address from the LTE3311, 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 LTE3311.

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.

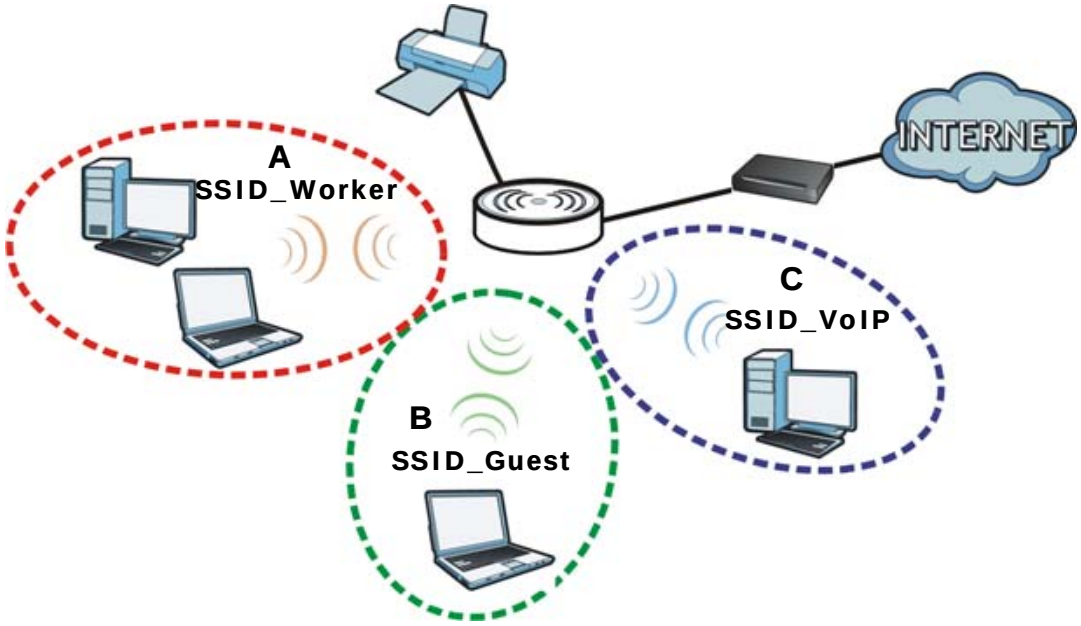
# 4.4 Using Multiple SSIDs on the LTE3311

You can configure more than one SSID on a LTE3311. See Section 7.4 on page 74.

This allows you to configure multiple independent wireless networks on the LTE3311 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 LTE3311 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 LTE3311 (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 LTE3311 is in router mode by default.

This example shows you how to configure the SSIDs with the following parameters on your LTE3311 .

| SSID | SECURITY TYPE | KEY |
|---|---|---|
| SSID_Worker | WPA2-PSK<br>WPA Compatible | DoNotStealMyWirelessNetwork |
| SSID_VoIP | WPA-PSK | VoIPOnly12345678 |
| SSID_Guest | WPA-PSK | keyexample123 |

1 Connect your computer to the LAN port of the LTE3311 using an Ethernet cable.

2 The default IP address of the LTE3311is "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".

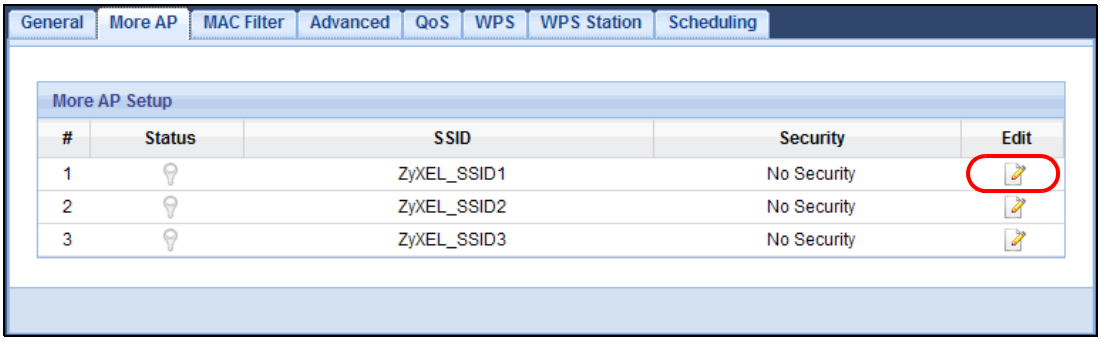
3 Click **Start > Run** on your computer in Windows. Type "cmd" in the dialog box. Enter "ipconfig" to show your computer's IP address. If your computer's IP address is not in the correct range then see Appendix C on page 190 for information on changing your computer's IP address.

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.

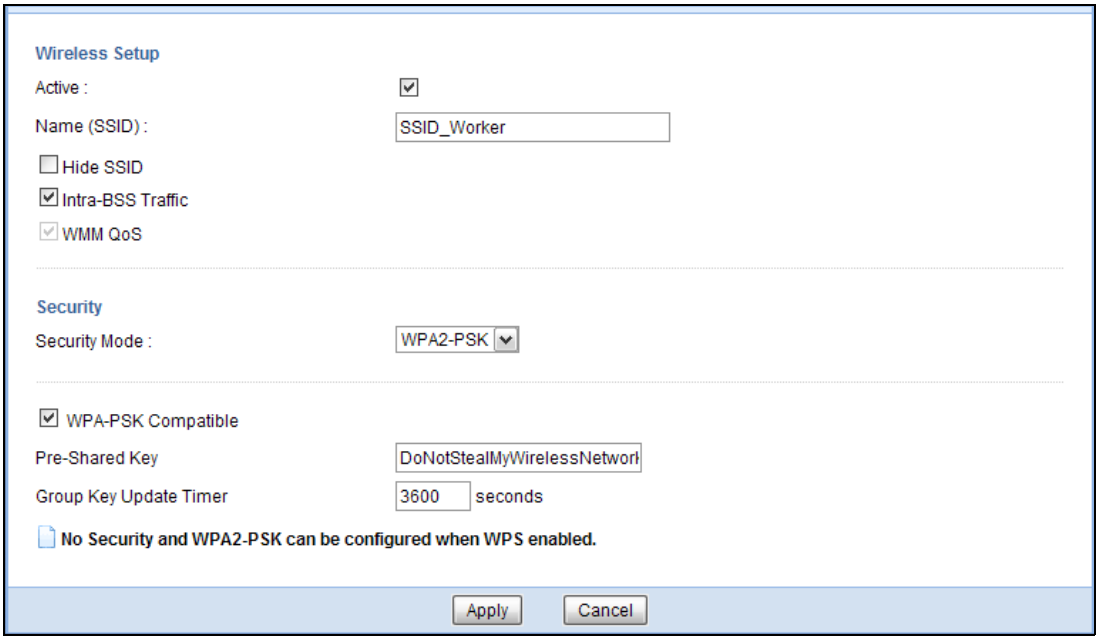
5 Enter "admin" as the user name and "1234" (default) as the password and click **Login**.

6 Type a new password and retype it to confirm, then click **Apply**. Otherwise, click **Ignore**.

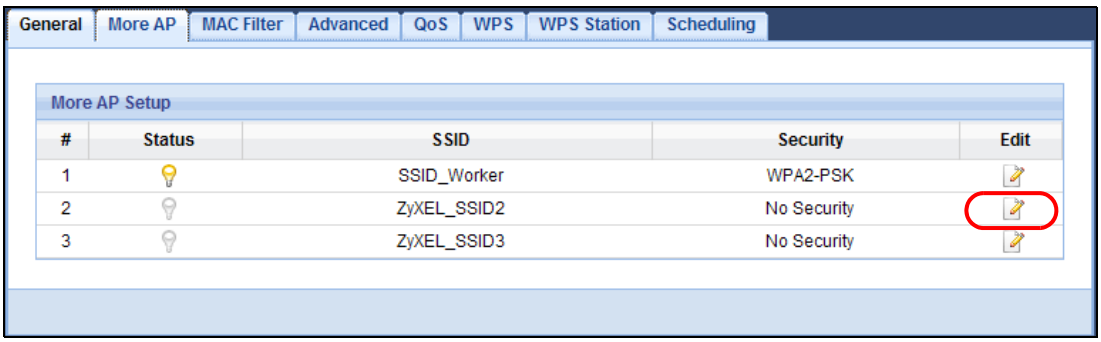
7 Go to **Configuration > Network > Wireless LAN > More AP**. Click the **Edit** icon of the first entry to configure wireless and security settings for **SSID_Worker**.



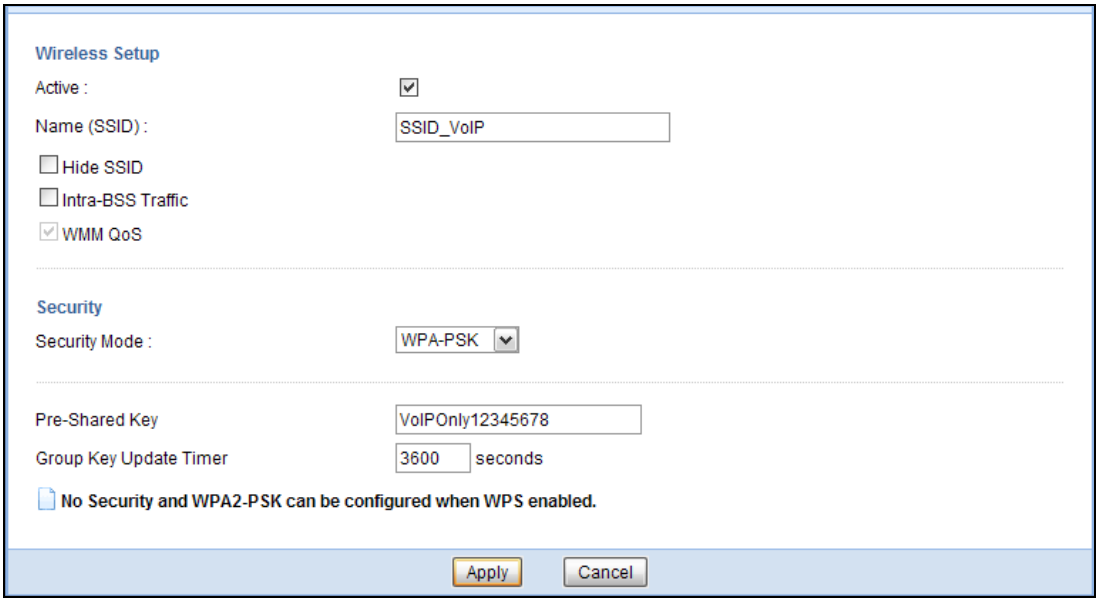

8 Configure the screen as follows. In this example, you enable **Intra-BSS Traffic** for **SSID_Worker** to allow wireless clients in the same wireless network to communicate with each other. Click **Apply**.



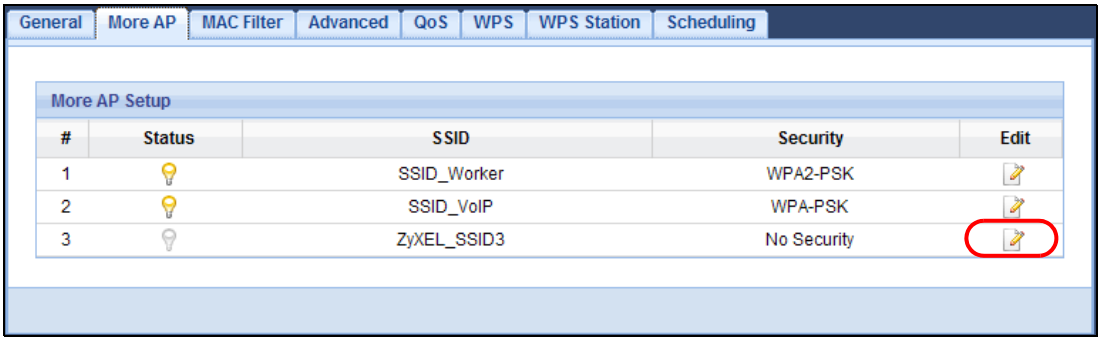

9 Click the **Edit** icon of the second entry to configure wireless and security settings for **SSID_VoIP**.



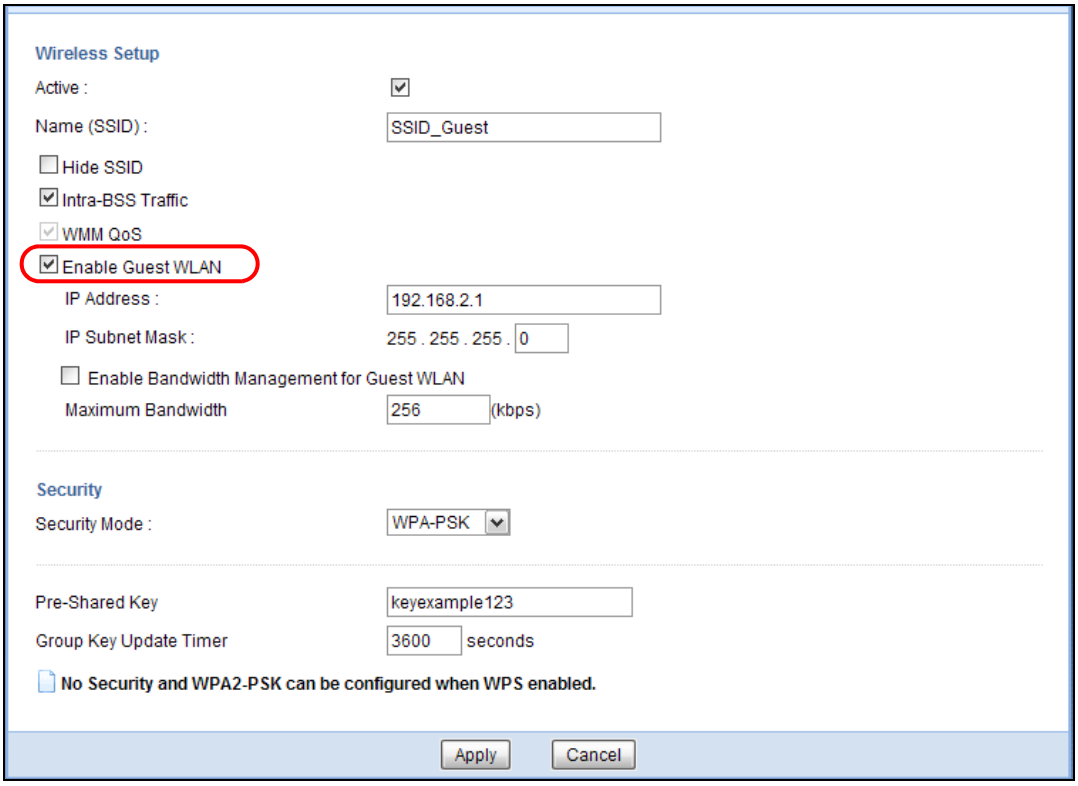

10 Configure the screen as follows. You do not enable **Intra-BSS Traffic** for **SSID_VoIP**. Click **Apply**.




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




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


Wireless Setup
Active :
Name (SSID) :
SSID_Guest
Hide SSID
Intra-BSS Traffic
WMM QoS
Enable Guest WLAN
IP Address :
192.168.2.1
IP Subnet Mask :
255 . 255 . 255 .
0
Enable Bandwidth Management for Guest WLAN
Maximum Bandwidth
256
(kbps)
Security
Security Mode :
WPA-PSK
Pre-Shared Key
keyexample123
Group Key Update Timer
3600
seconds
No Security and WPA2-PSK can be configured when WPS enabled.
Apply
Cancel

# PART II
# Technical Reference

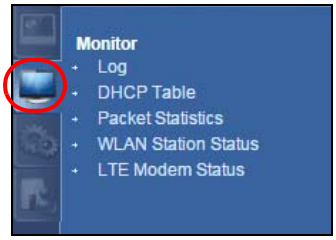
# 5

# Monitor

## 5.1 Overview

This chapter discusses read-only information related to the device state of the LTE3311.

To access the Monitor screens, click  after login.




You can also click the links in the **Summary** table of the **Status** screen to view the packets sent/ received as well as the status of wireless clients connected to the LTE3311.

## 5.2 What You Can Do

- Use the **Log** screen to see the logs for the activity on the LTE3311 (Section 5.3 on page 46).
- Use the **DHCP Table** screen to view information related to your DHCP status (Section 5.4 on page 48).
- use the **Packet Statistics** screen to view port status, packet specific statistics, the "system up time" and so on (Section 5.5 on page 48).
- Use the **WLAN Station Status** screen to view the wireless stations that are currently associated to the LTE3311 (Section 5.6 on page 49).
- 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 5.7 on page 50).

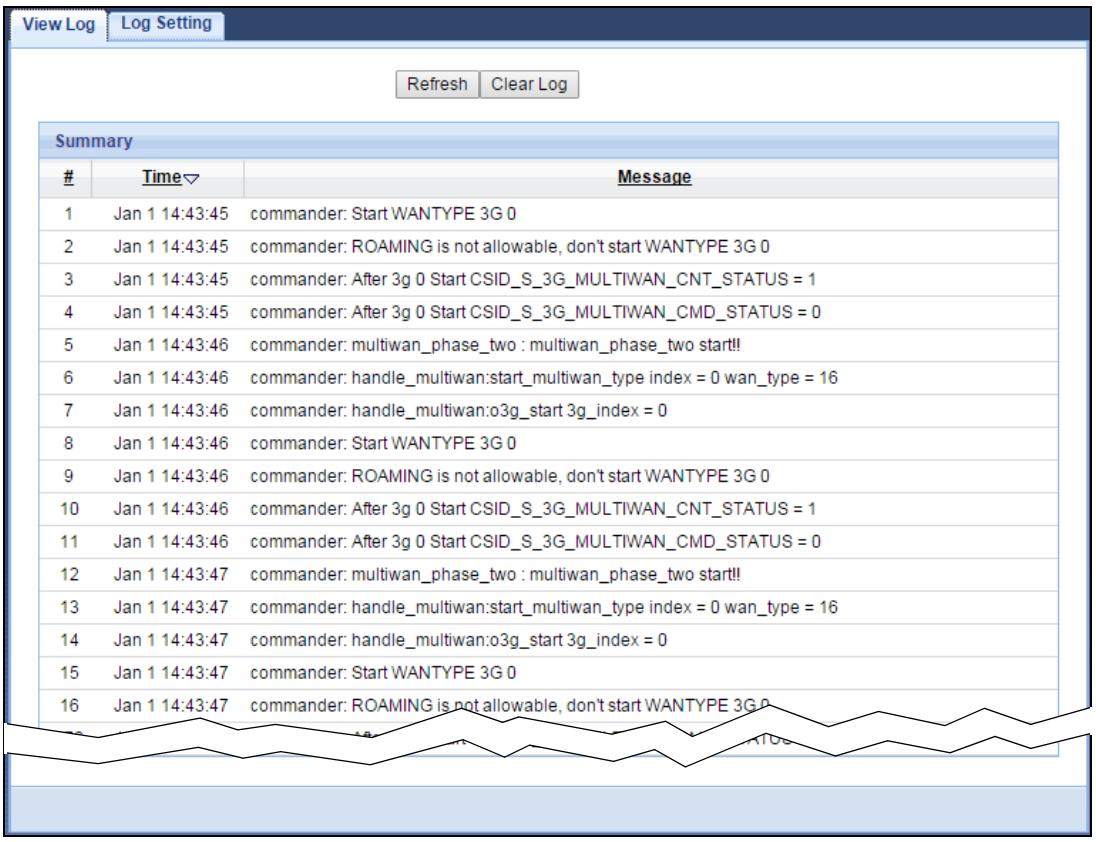
## 5.3 The Log Screens

The Web Configurator allows you to look at all of the LTE3311's logs in one location.

## 5.3.1 View Log

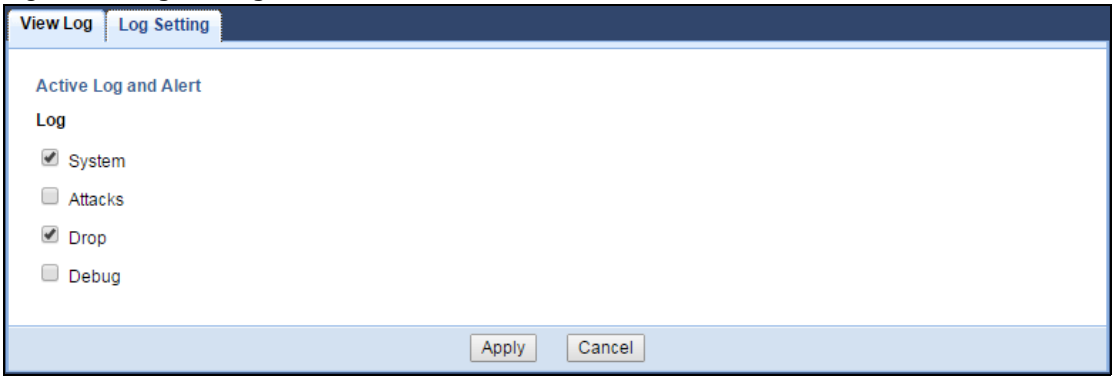
Use the **View Log** screen to see the logged messages for the LTE3311. The log wraps around and deletes the old entries after it fills. Select what logs you want to see in the **Log Setting** screen. Click **Refresh** to renew the log screen. Click **Clear Log** to delete all the logs.

**Figure 20** View Log




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 21** Log Settings

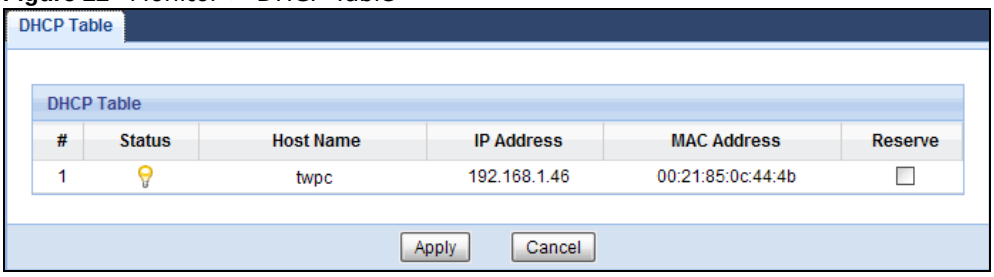


# 5.4 DHCP Table

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 LTE3311's LAN as a DHCP server or disable it. When configured as a server, the LTE3311 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 LTE3311's DHCP server.

**Figure 22** Monitor > DHCP Table




The following table describes the labels in this screen.

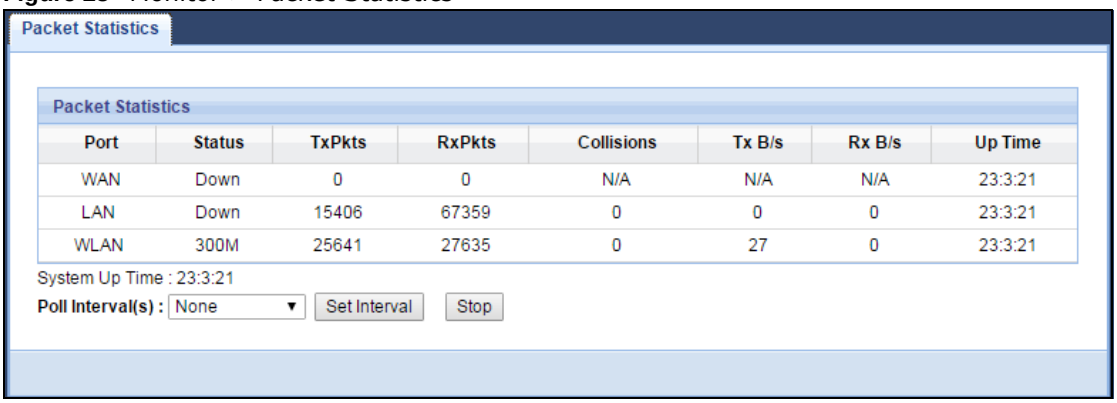
**Table 9** Monitor > DHCP Table

| 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.<br>Every Ethernet device has a unique MAC (Media Access Control) address which uniquely identifies a device. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. |
| Reserve | Select this if you want to reserve the IP address for this specific MAC address. |
| Apply | Click **Apply** to save your changes back to the LTE3311. |
| Cancel | Click **Cancel** to reload the previous configuration for this screen. |

# 5.5 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 23** Monitor > Packet Statistics




The following table describes the labels in this screen.

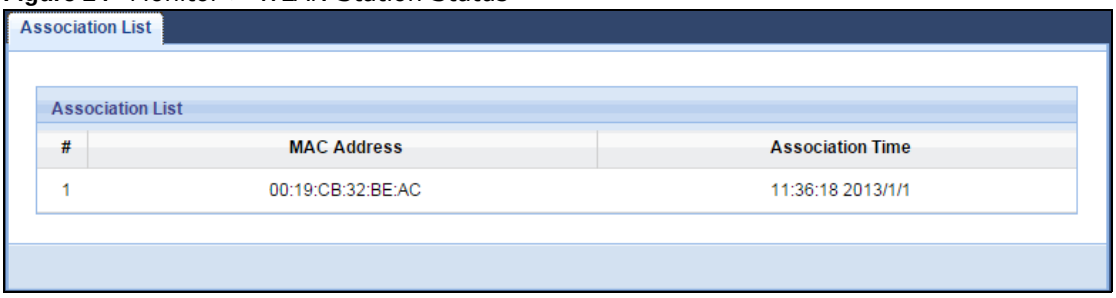
**Table 10** Monitor > Packet Statistics

| LABEL | DESCRIPTION |
|---|---|
| Port | This is the LTE3311's interface type. |
| Status | For the LAN ports, this displays the port speed and duplex setting or **Down** when the line is disconnected.<br>For the WAN port, it displays **Up** when the mobile data connection is up, **Connecting** when the LTE3311 is trying to bring the mobile data connection up, and displays **Down** when the 3G/4G connection is down or not activated.<br>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 LTE3311 has been for each session. |
| System Up Time | This is the total time the LTE3311 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. |

# 5.6 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 LTE3311'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 24** Monitor > WLAN Station Status




The following table describes the labels in this screen.

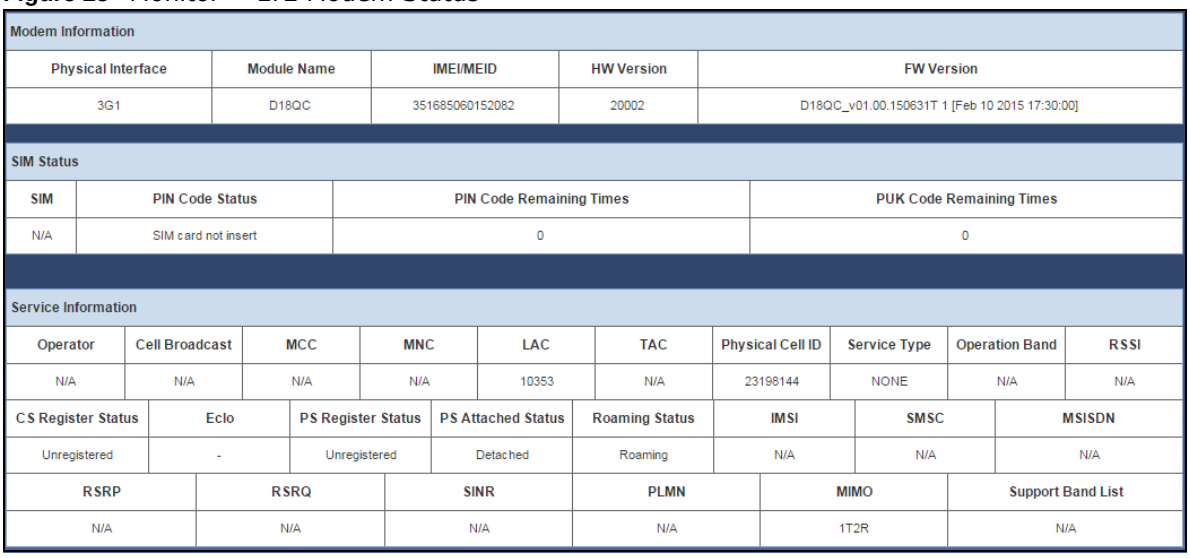
**Table 11** Monitor > WLAN Station Status

| 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 LTE3311's WLAN. |

# 5.7 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 LTE module, cellular interface, and SIM card. You can also check the LTE connection status.

**Figure 25** Monitor > LTE Modem Status




The following table describes the labels in this screen.

**Table 12** Monitor > LTE Modem Status

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

**Table 12** Monitor > LTE Modem Status (continued)

| LABEL | DESCRIPTION |
|---|---|
| Module Name | This displays the name of the built-in LTE module. |
| IMEI/MEID | This displays the International Mobile Equipment Number (IMEI) or Mobile Equipment Identifier (MEID), which is the serial number of the built-in LTE module. It is a unique 15-digit number used to identify a mobile device. |
| HW Version | This displays the hardware version of the built-in LTE module. |
| FW Version | This displays the firmware version of the built-in LTE module. |
| SIM Status | |
| SIM | This displays the status of the inserted SIM card. **N/A** displays if there is no SIM card inserted. |
| PIN Code Status | This displays the status of PIN code authentication. |
| PIN Code Remaining Times | This displays how many times you can enter the PIN code. |
| PUK Code Remaining Times | This displays how many times you can enter the PUK code. |
| Service Information | |
| Operator | This displays the name of the service provider. |
| 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 LTE3311 is connecting. |
| Operation Band | This displays the network type and the frequency band used by the mobile network to which the LTE3311 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 LTE3311 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. |

**Table 12** Monitor > LTE Modem Status (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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 LTE3311, 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 LTE3311. |

# 6

# WAN

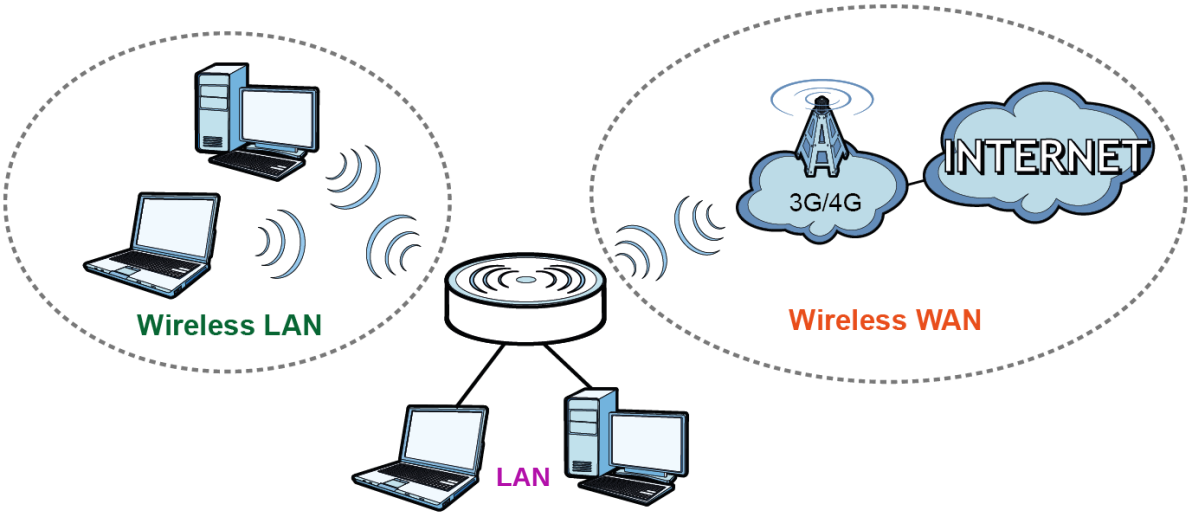
## 6.1 Overview

This chapter discusses the LTE3311's **WAN** screens. Use these screens to configure your LTE3311 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 3G/4G SIM card and set the LTE3311 to use this 3G/4G connection as your WAN.

**Figure 26** 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 56).
- Use the **Network Scan** screen to specify the type of the mobile network to which the LTE3311 is connected and how you want the LTE3311 to connect to an available mobile network (Section 6.5 on page 60).
- Use the **IPv6** screen to configure the LTE3311's IPv6 settings (Section 6.6 on page 62).
- Use the **PIN Management** screen to configure the LTE3311's PIN settings (Section 6.7 on page 63).

# 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 LTE3311.

### 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.

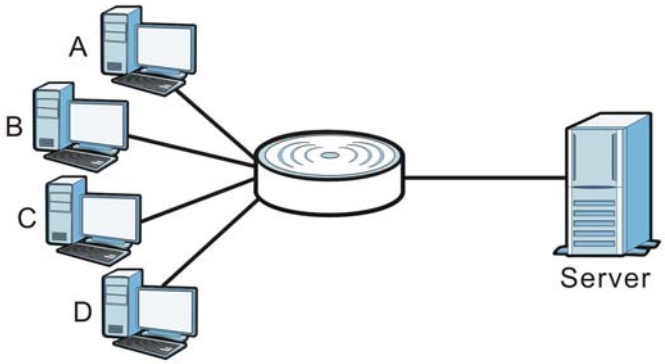
The LTE3311 can get the DNS server addresses in the following ways.

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 LTE3311'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 27** 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 LTE3311 supports both IGMP version 1 (**IGMP v1**), IGMP version 2 (**IGMP v2**) and IGMP version 3 (**IGMP v3**).

At start up, the LTE3311 queries all directly connected networks to gather group membership. After that, the LTE3311 periodically updates this information. IP multicasting can be enabled/disabled on the LTE3311 WAN interface in the Web Configurator.

## IPv6 Introduction

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to $3.4 \times 10^{38}$ IP addresses. The LTE3311 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

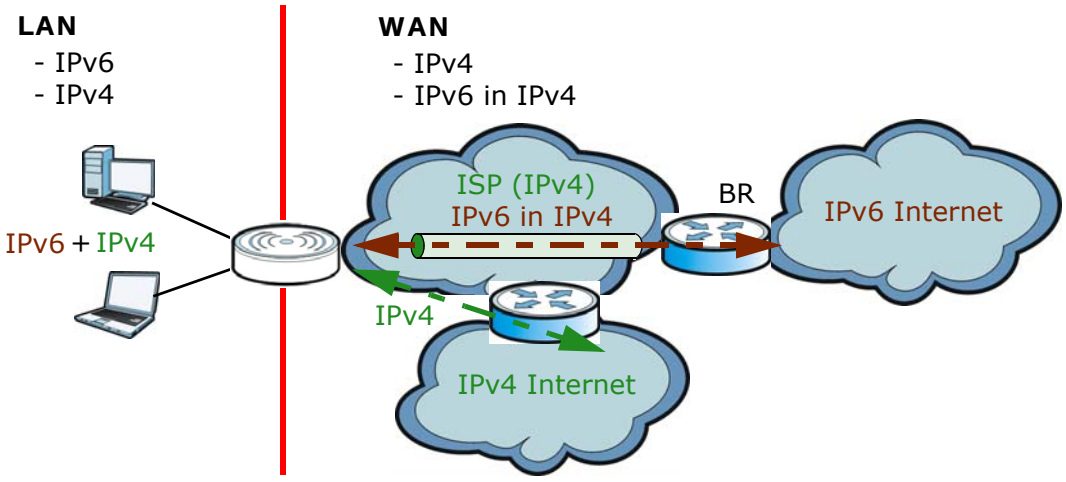
Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block's 16 bits are then represented by four hexadecimal characters. For example, 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 LTE3311 has an IPv4 WAN address, you can enable 6rd to encapsulate IPv6 packets in IPv4 packets to cross the ISP's IPv4 network.

The LTE3311 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 LTE3311 uses it's configured IPv4 WAN IP to route IPv4 traffic to the IPv4 Internet.

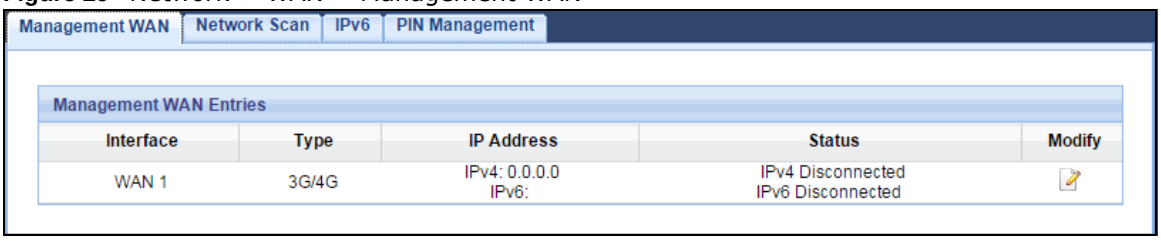
**Figure 28** IPv6 Rapid Deployment




# 6.4 Management WAN

The summary table shows you the WAN connection configured on the LTE3311. Click **Network** > **WAN** > **Management WAN** from the **Configuration** menu.

**Figure 29** Network > WAN > Management WAN




The following table describes the labels in this screen.

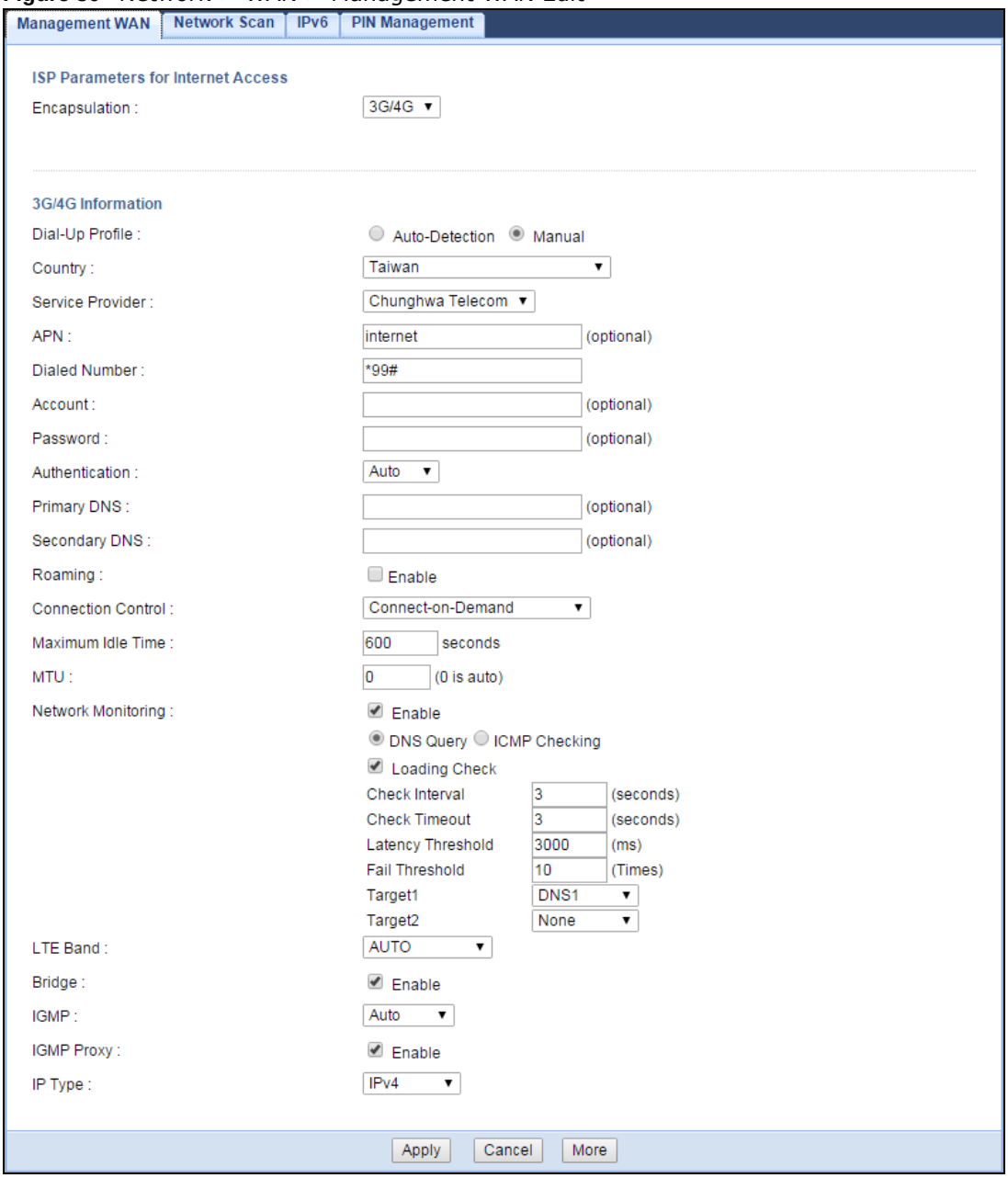
**Table 13** Network > WAN > Management WAN

| 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 LTE3311's 3G/4G WAN connection settings. Click the Edit icon in the **Network** > **WAN > Management WAN** screen.

**Figure 30** Network > WAN > Management WAN Edit




The following table describes the labels in this screen.

**Table 14** Network > WAN > Management WAN Edit

| LABEL | DESCRIPTION |
|---|---|
| ISP Parameters for Internet Access | |
| Encapsulation | This shows the WAN connection type. |
| 3G/4G Information | |
| Dial-Up Profile | Select **Auto-Detection** to have the LTE3311 use the inserted SIM card's default settings to connect to any available mobile network.<br><br>Select **Manual** and enter the information provided by your service provider to connect to the service provider's mobile network. |

**Table 14** Network > WAN > Management WAN Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Country | Select the country in which you use the LTE3311. |
| Service Provider | Select the name of your service provider. The options vary depending on the country you selected.<br><br>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.<br><br>The corresponding APN automatically displays when you select a pre-defined service provider.<br><br>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.<br><br>The corresponding phone number automatically displays when you select a pre-defined service provider.<br><br>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 LTE3311 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<br><br>Select an authentication protocol (**PAP**, or **CHAP**) used by the service provider. Otherwise, select **Auto** to have the LTE3311 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 LTE3311 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.<br><br>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 LTE3311 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 **Enable** to have the LTE3311 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. |
| 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. |

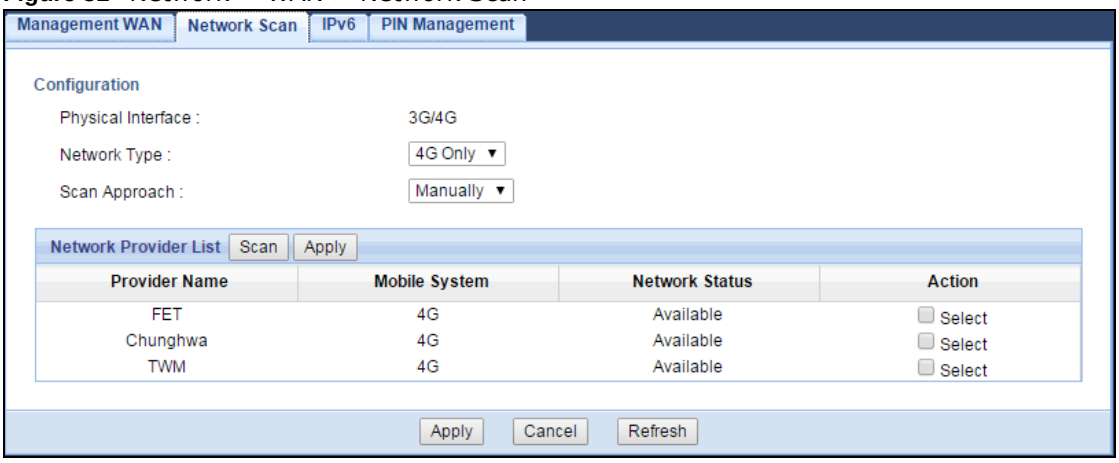
**Table 14** Network > WAN > Management WAN Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Check Timeout | Type the number of seconds (0 to 99999) for your LTE3311 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.<br>If the specified latency threshold is exceeded, the LTE3311 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 LTE3311 still checks a "down" connection to detect if it reconnects. |
| Target1/Target2 | Select **DNS1** to have the LTE3311 send a DNS query to the first DNS server address assigned by the service provider.<br>Select **DNS2** to have the LTE3311 send a DNS query to the second DNS server address assigned by the service provider.<br>Select **Other Host** and enter a domain name or IP address of a reliable nearby computer to have the LTE3311 ping that address. |
| LTE Band | Select the LTE band on which you want the LTE3311 to be. Select **Auto** if you want the LTE3311 to switch to a supported band automatically. |
| Bridge | Select this option to allow the computer connected to the first Ethernet LAN port to get an individual IP address from the ISP's DHCP server directly. |
| IGMP | Select **IGMP v1**, **IGMP v2**, **IGMP v3** or **Auto** to enable multicasting. This applies to traffic routed from the WAN to the LAN.<br>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.<br>Select this option to have the LTE3311 act as an IGMP proxy on this connection. This allows the LTE3311 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 LTE3311 to run IPv4 only.<br>Select **IPv4/IPv6** to allow the LTE3311 to run IPv4 and IPv6 at the same time.<br>Select **IPv6** if you want the LTE3311 to run IPv6 only. |
| Apply | Click **Apply** to save your changes back to the LTE3311. |
| Cancel | Click **Cancel** to reload the previous configuration for this screen. |
| More | Click **More** to display advanced fields. |

# 6.5 Network Scan

Use this screen to set how you want the LTE3311 to connect to an available mobile network. Click **Network** > **WAN > Network Scan** from the **Configuration** menu.

**Figure 31** Network > WAN > Network Scan




The following table describes the labels in this screen.

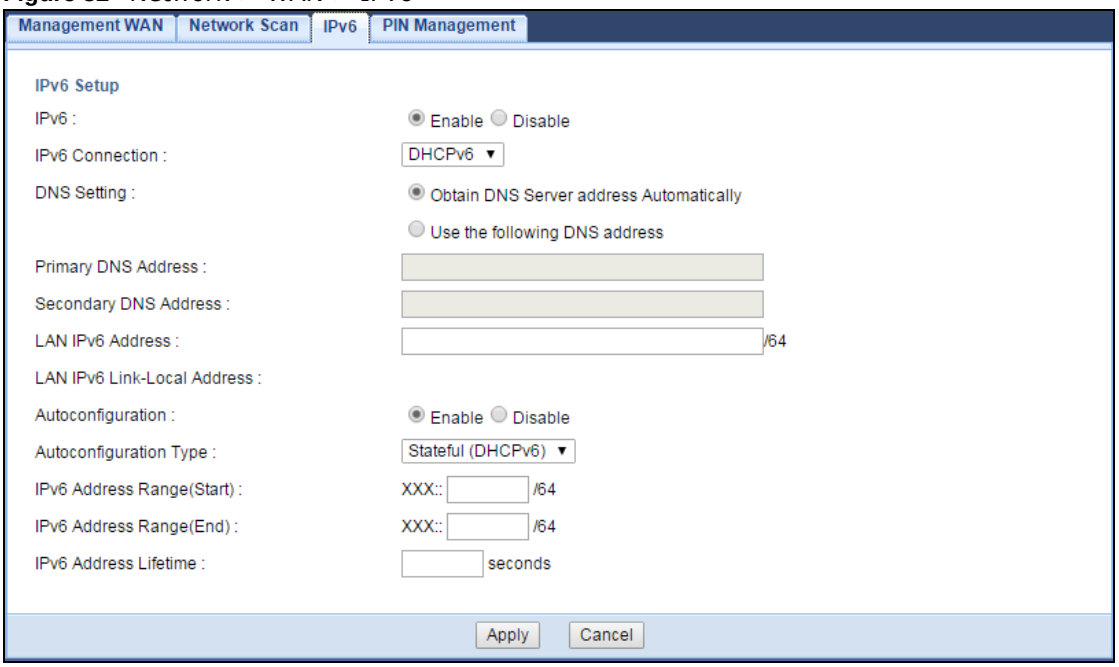
**Table 15** Network > WAN > Network Scan

| 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**) to which you want the LTE3311 to connect when there is a SIM card inserted. |
| Scan Approach | Select **Auto** to have the LTE3311 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 LTE3311 switches to another available mobile network.<br><br>Select **Manually** to search for and select the mobile network(s) to which you want the LTE3311 to connect. |
| Network Provider List | This table is available only when you set **Scan Approach** to **Manually**.<br><br>Click **Scan** to search for available mobile networks based on the network type you selected.<br><br>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 LTE3311 establish a connection to the selected mobile network. |
| Apply | Click **Apply** to save your changes back to the LTE3311. |
| Cancel | Click **Cancel** to reload the previous configuration for this screen. |
| Refresh | Click **Refresh** to update this screen. |

# 6.6 IPv6

Use this screen to configure the LTE3311's IPv6 settings. Click **Network** > **WAN > IPv6** from the **Configuration** menu.

**Figure 32** Network > WAN > IPv6




The following table describes the labels in this screen.

**Table 16** Network > WAN > IPv6

| LABEL | DESCRIPTION |
|---|---|
| IPv6 | Select **Enable** to allow the LTE3311 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 LTE3311 get the IPv6 DNS server addresses from the ISP automatically.<br><br>Select **Use the following DNS address** to have the LTE3311 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 LTE3311 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 LTE3311 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**. |
| Autoconfiguration Type | Select **Stateless** if you want the LTE3311 interface to automatically generate a link-local address via stateless autoconfiguration.<br><br>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. |

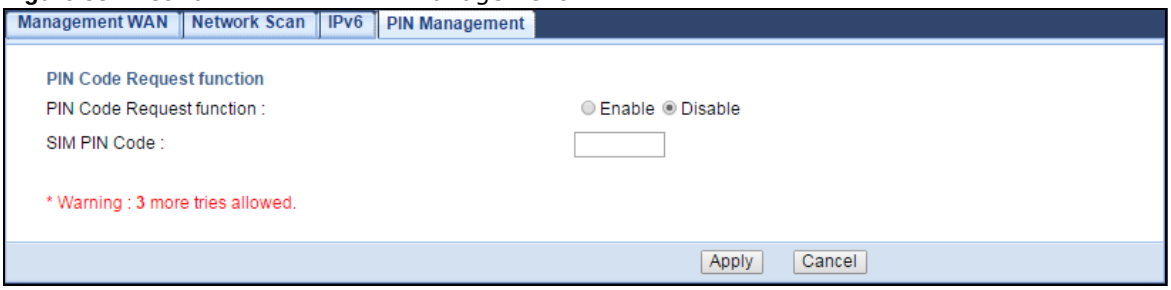
**Table 16** Network > WAN > IPv6 (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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. |
| Apply | Click **Apply** to save your changes back to the LTE3311. |
| Cancel | Click **Cancel** to reload the previous configuration for this screen. |

# 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 33** Network > WAN > PIN Management




The following table describes the labels in this screen.

**Table 17** 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.<br><br>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 LTE3311. |
| Cancel | Click **Cancel** to reload the previous configuration for this screen. |

# 7

# Wireless LAN

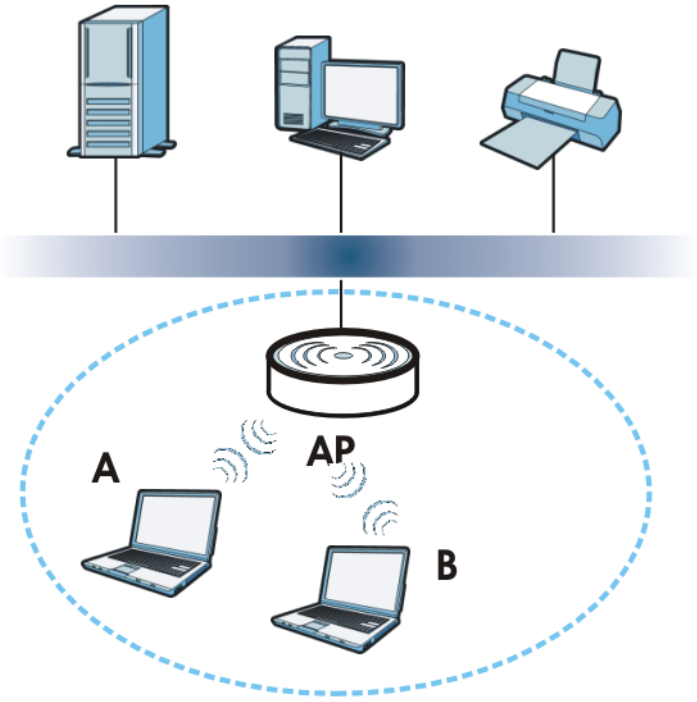
## 7.1 Overview

This chapter discusses how to configure the wireless network settings in your LTE3311.

See the appendices for more detailed information about wireless networks.

The following figure provides an example of a wireless network.

**Figure 34** 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 LTE3311 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 LTE3311 and the wireless clients, and make other basic configuration changes (Section 7.2 on page 67).
- Use the **More AP** screen to set up multiple wireless networks on your LTE3311 (Section 7.4 on page 74).
- Use the **MAC Filter** screen to allow or deny wireless stations based on their MAC addresses from connecting to the LTE3311 (Section 7.5 on page 76).
- Use the **Advanced** screen to allow intra-BSS networking and set the RTS/CTS Threshold (Section 7.6 on page 78).
- Use the **QoS** screen to ensure Quality of Service (QoS) in your wireless network (Section 7.7 on page 79).
- 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 79).
- Use the **WPS Station** screen to add a wireless station using WPS (Section 7.9 on page 81).
- Use the **Scheduling** screen to set the times your wireless LAN is turned on and off (Section 7.10 on page 81).
- Use the **WDS** screen to configure the LTE3311's WDS settings (Section 7.11 on page 82).

## 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.

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.

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.

The types of encryption you can choose depend on the type of user authentication. (See page 66 for information about this.)

**Table 18** 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 LTE3311, 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 LTE3311.

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 34.

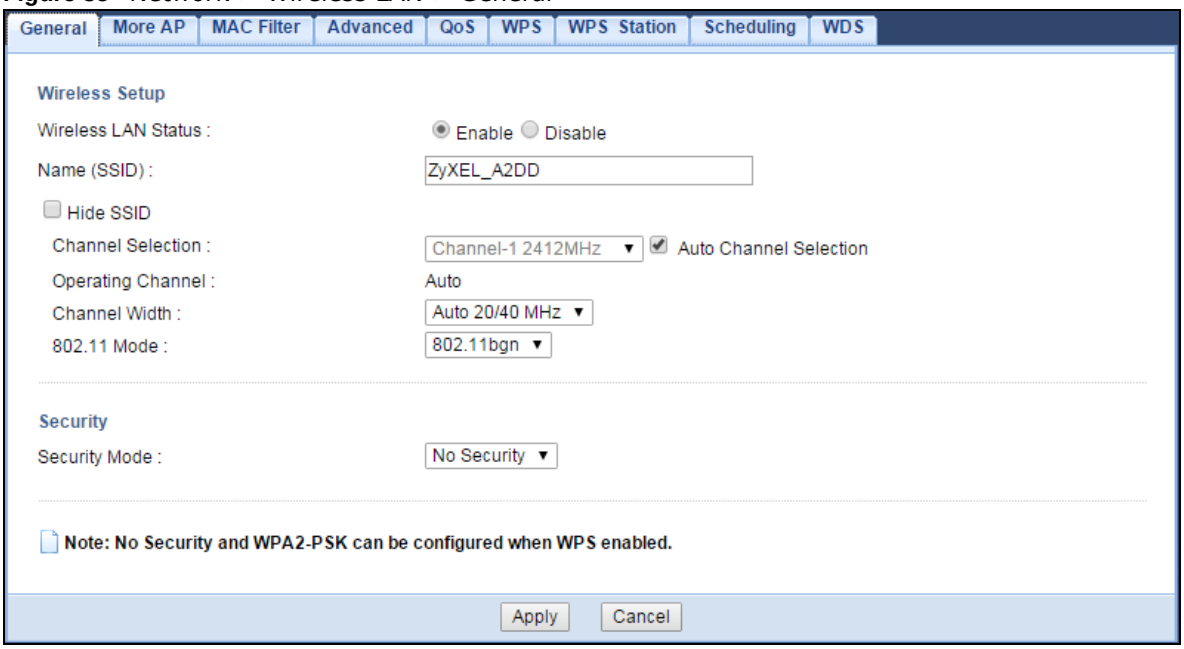
## 7.2 General Wireless LAN Screen

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

Note: If you are configuring the LTE3311 from a computer connected to the wireless LAN and you change the LTE3311'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 LTE3311's new settings.

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

**Figure 35** Network > Wireless LAN > General




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

**Table 19** Network > Wireless LAN > General

| LABEL | DESCRIPTION |
|---|---|
| Wireless LAN Status | Select **Enable** to activate the 2.4GHz wireless LAN. Select **Disable** to turn it off.<br>You can also enable or disablethe 2.4GHz wireless LANs by using the **WIFI** button located on the back panel of the LTE3311. |
| 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.<br>Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in.<br>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 LTE3311 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 LTE3311 is currently using. |

**Table 19** Network > Wireless LAN > General (continued)

| LABEL | DESCRIPTION |
|---|---|
| Channel Width | Select the wireless channel width used by LTE3311.<br><br>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).<br><br>Because not all devices support 40 MHz channels, select **Auto 20/40MHz** to allow the LTE3311 to adjust the channel bandwidth automatically.<br><br>**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.<br><br>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:<br><br>• **802.11b**: allows either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the LTE3311. In this mode, all wireless devices can only transmit at the data rates supported by IEEE 802.11b.<br>• **802.11g**: allows IEEE 802.11g compliant WLAN devices to associate with the Device. IEEE 802.11b compliant WLAN devices can associate with the LTE3311 only when they use the short preamble type.<br>• **802.11bg**: allows either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the LTE3311. The LTE3311 adjusts the transmission rate automatically according to the wireless standard supported by the wireless devices.<br>• **802.11n**: allows IEEE 802.11n compliant WLAN devices to associate with the LTE3311. This can increase transmission rates, although IEEE 802.11b or IEEE 802.11g clients will not be able to connect to the LTE3311.<br>• **802.11gn**: allows either IEEE 802.11g or IEEE 802.11n compliant WLAN devices to associate with the LTE3311. The transmission rate of your LTE3311 might be reduced.<br>• **802.11bgn**: allows IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the LTE3311. The transmission rate of your LTE3311 might be reduced. |
| 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 69 for detailed information on different security modes. Or you can select **No Security** to allow any client to associate this network without authentication.<br><br>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 LTE3311. |
| 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

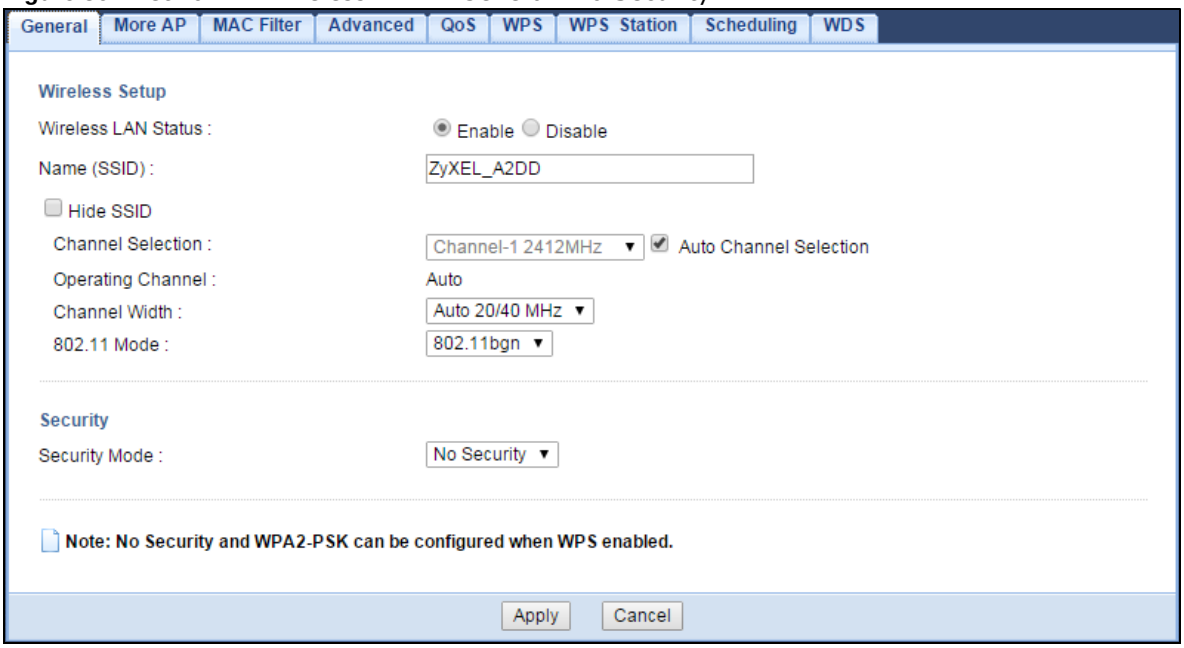
The screen varies depending on what you select in the **Security Mode** field.

## 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 LTE3311, your network is accessible to any wireless networking device that is within range.

**Figure 36** Network > Wireless LAN > General: No Security




The following table describes the labels in this screen.

**Table 20** Network > Wireless LAN > General: No Security

| LABEL | DESCRIPTION |
|---|---|
| Security Mode | Choose **No Security** from the drop-down list box. |
| Apply | Click **Apply** to save your changes back to the LTE3311. |
| Cancel | Click **Cancel** to reload the previous configuration for this screen. |

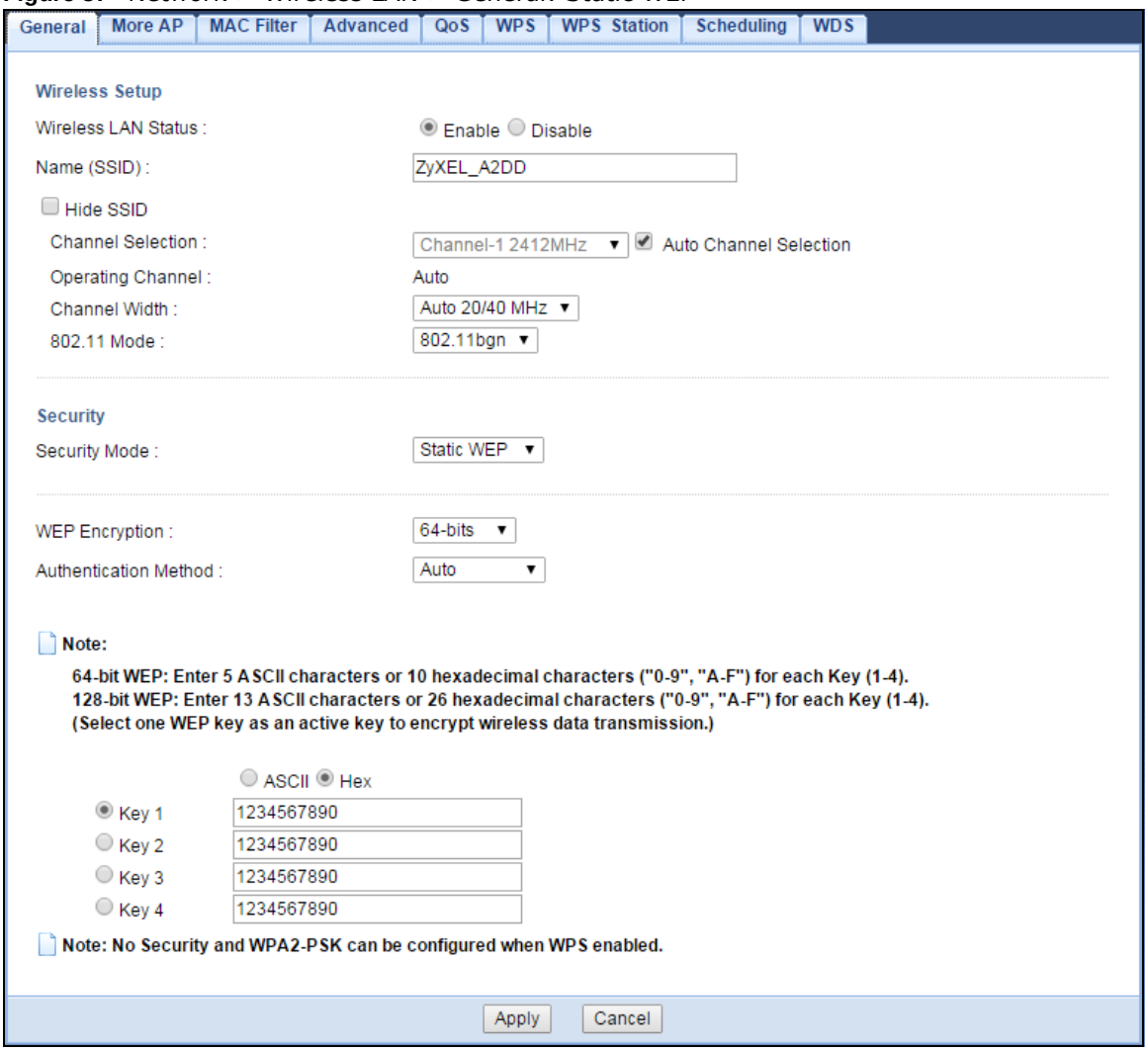
## 7.3.2 WEP Encryption

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 LTE3311 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 37** Network > Wireless LAN > General: Static WEP




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

**Table 21** 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**.<br>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.<br>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 LTE3311 occurs.<br>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.<br>The preceding "0x", that identifies a hexadecimal key, is entered automatically. |

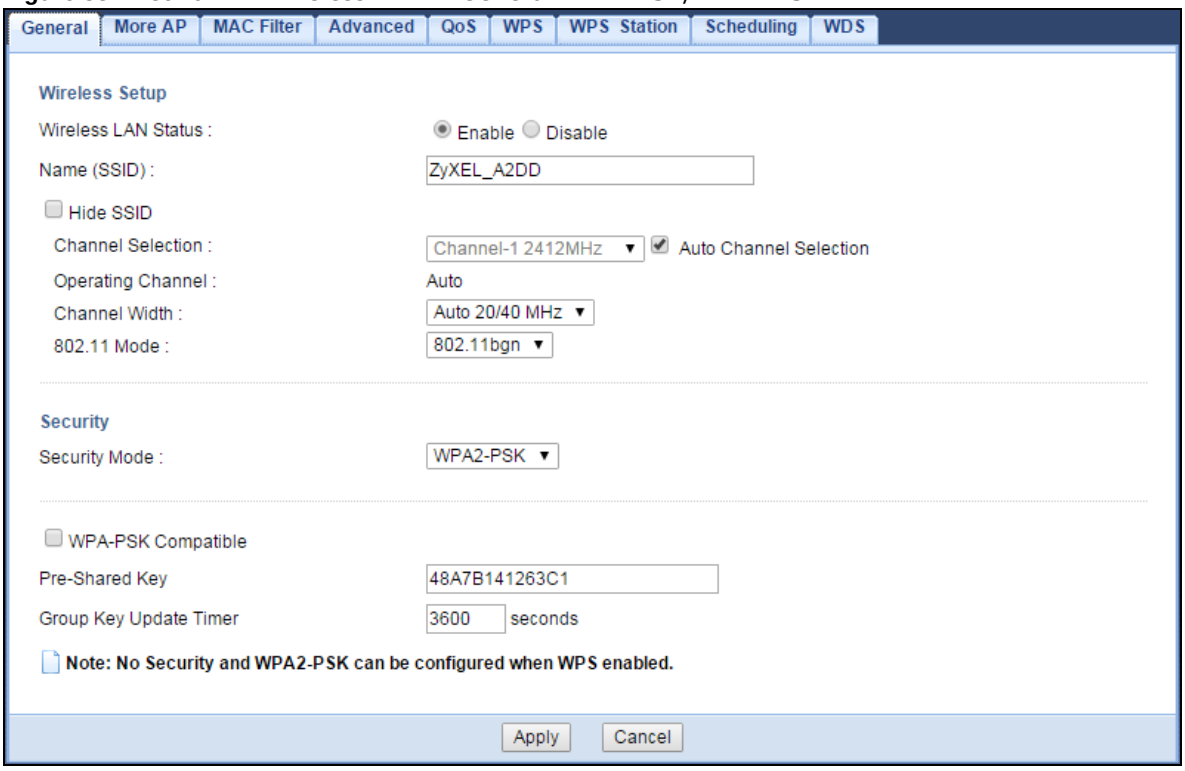
**Table 21** Network > Wireless LAN > General: Static WEP (continued)

| LABEL | DESCRIPTION |
|---|---|
| Key 1 to Key 4 | The WEP keys are used to encrypt data. Both the LTE3311 and the wireless stations must use the same WEP key for data transmission.<br>If you chose **64-bits**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").<br>If you chose **128-bits**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").<br>You must configure at least one key, only one key can be activated at any one time. The default key is key 1. |
| Apply | Click **Apply** to save your changes back to the LTE3311. |
| Cancel | Click **Cancel** to reload the previous configuration for this screen. |

## 7.3.3 WPA-PSK/WPA2-PSK

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

**Figure 38** Network > Wireless LAN > General: WPA-PSK/WPA2-PSK




The following table describes the labels in this screen.

**Table 22** 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**.<br>Check this field to allow wireless devices using **WPA-PSK** security mode to connect to your LTE3311. |

**Table 22** Network > Wireless LAN > General: WPA-PSK/WPA2-PSK (continued)

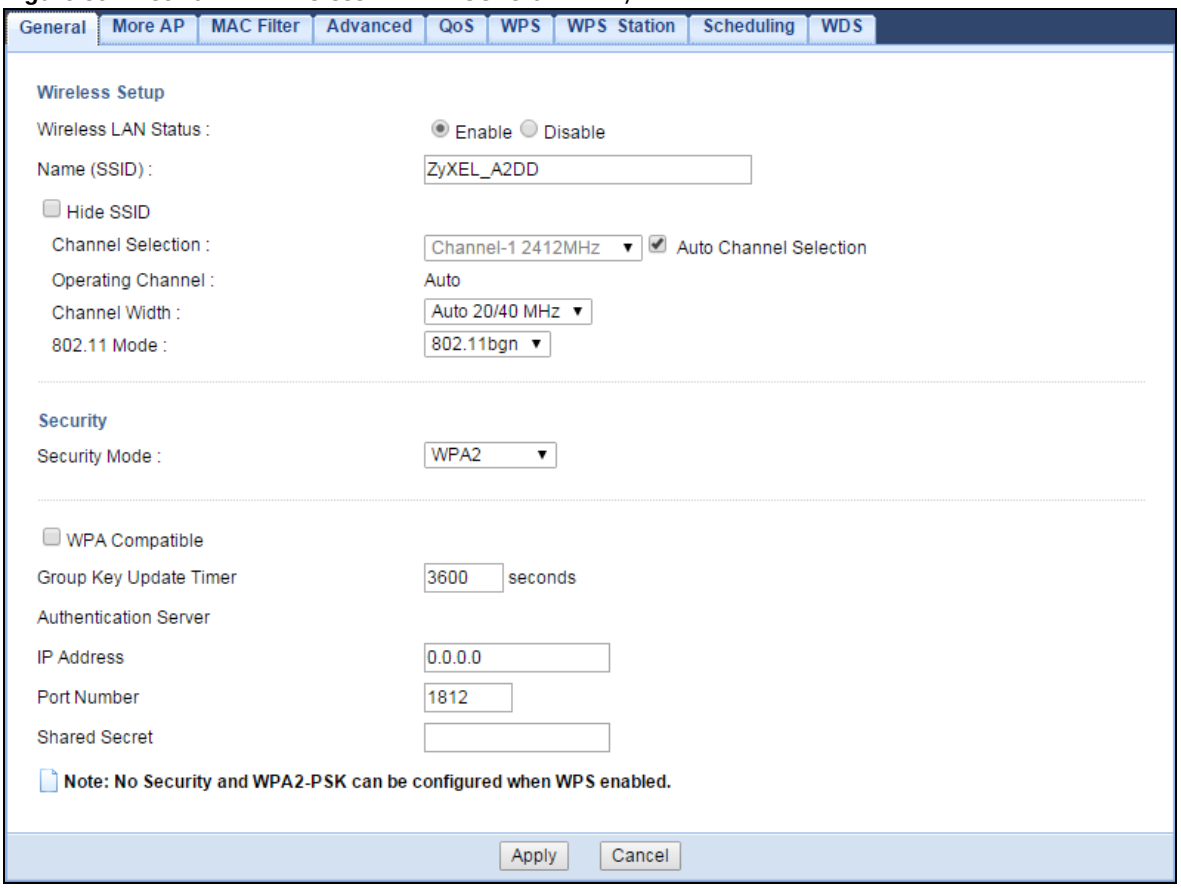
| LABEL | DESCRIPTION |
|---|---|
| Pre-Shared Key | **WPA-PSK / WPA2-PSK** uses a simple common password for authentication.<br>Type a pre-shared key from 8 to 63 case-sensitive keyboard characters. |
| Group Key Update Timer | The **Group Key Update Timer** is the rate at which the AP sends a new group key out to all clients.<br>The default is **3600** seconds (60 minutes). |
| Apply | Click **Apply** to save your changes back to the LTE3311. |
| Cancel | Click **Cancel** to reload the previous configuration for this screen. |

## 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 39** Network > Wireless LAN > General: WPA/WPA2



The following table describes the labels in this screen.

**Table 23** 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.<br>Select the check box to have both WPA2 and WPA wireless clients be able to communicate with the LTE3311 even when the LTE3311 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.<br>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 LTE3311.<br>The key must be the same on the external authentication server and your LTE3311. The key is not sent over the network. |
| Apply | Click **Apply** to save your changes back to the LTE3311. |
| Cancel | Click **Cancel** to reload the previous configuration for this screen. |

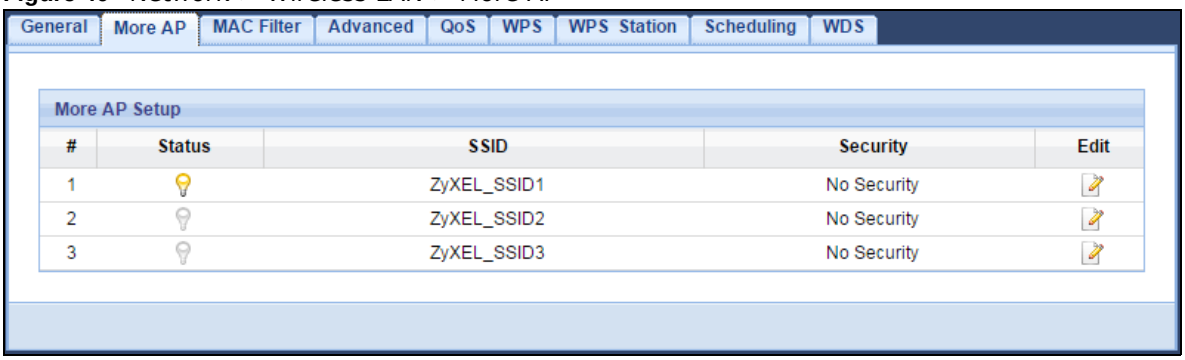
# 7.4 More AP Screen

This screen allows you to enable and configure multiple wireless networks and guest wireless network settings on the LTE3311.

You can configure up to four SSIDs to enable multiple BSSs (Basic Service Sets) on the LTE3311. 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 **Network > Wireless LAN > More AP**. The following screen displays.

**Figure 40** Network > Wireless LAN > More AP




The following table describes the labels in this screen.

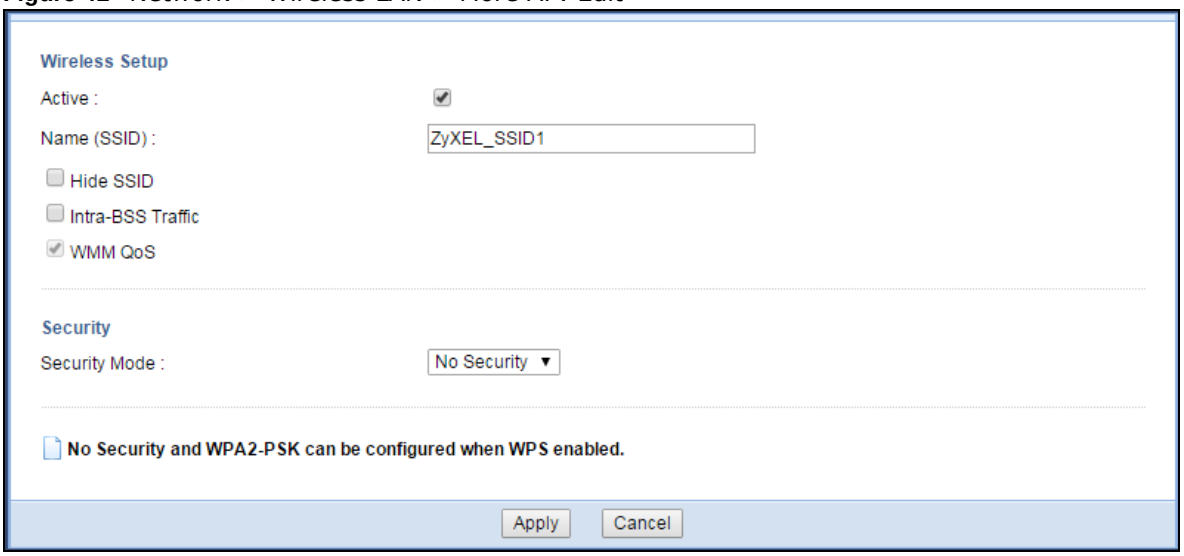
**Table 24** Network > Wireless LAN > More AP

| 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 LTE3311's BSSs. The SSID (Service Set IDentifier) identifies the Service Set with which a wireless device is associated.<br>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 41** Network > Wireless LAN > More AP: Edit



The following table describes the labels in this screen.

**Table 25** Network > Wireless LAN > More AP: Edit

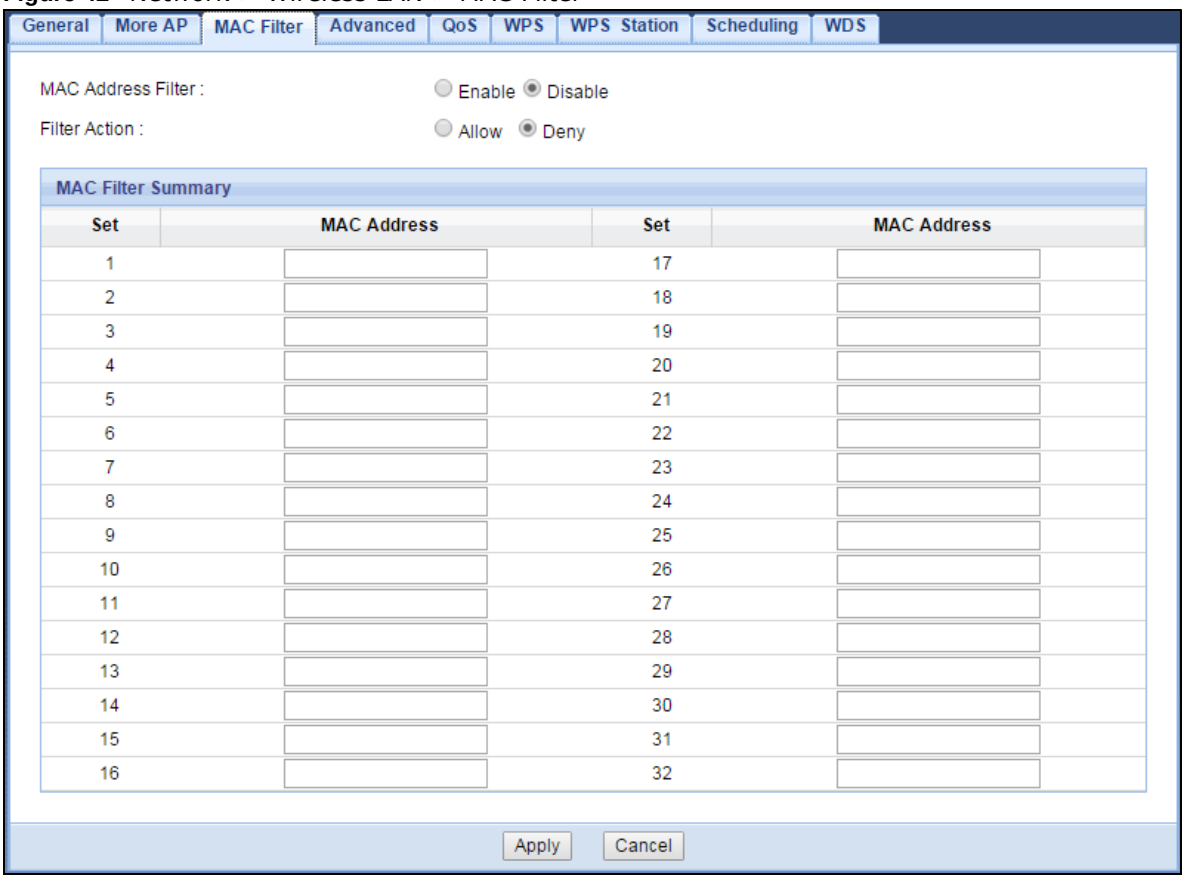
| LABEL | DESCRIPTION |
|---|---|
| Active | Select this to activate the SSID profile. |
| Name (SSID) | The SSID (Service Set IDentity) identifies the Service Set with which a wireless client is associated. Enter a descriptive name (up to 32 printable characters found on a typical English language keyboard) for the wireless LAN. |
| Hide SSID | Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. |
| 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).<br>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 LTE3311 automatically give a service a priority level according to the ToS value in the IP header of packets it sends.<br>WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly. |
| 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 69 for detailed information on different security modes. Or you can select **No Security** to allow any client to associate this network without authentication.<br>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 LTE3311. |
| Cancel | Click **Cancel** to reload the previous configuration for this screen. |

# 7.5 MAC Filter Screen

The MAC filter screen allows you to configure the LTE3311 to give exclusive access to devices (**Allow**) or exclude devices from accessing the LTE3311 (**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 LTE3311's MAC filter settings, click **Network** > **Wireless LAN** > **MAC Filter**. The screen appears as shown.

**Figure 42** Network > Wireless LAN > MAC Filter




The following table describes the labels in this menu.

**Table 26** Network > Wireless LAN > MAC Filter

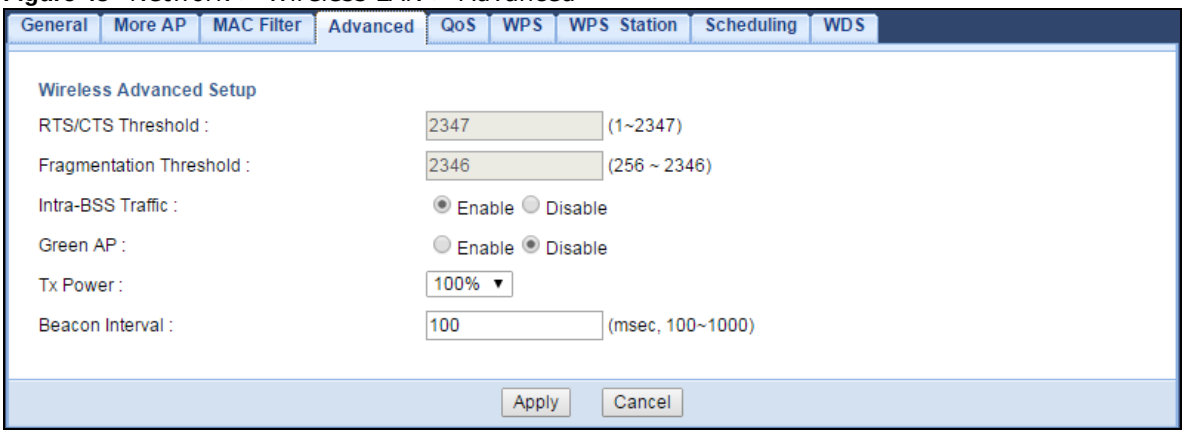
| LABEL | DESCRIPTION |
|---|---|
| MAC Address Filter | Select to turn on (**Enable**) or off (**Disable**) MAC address filtering. |
| Filter Action | Define the filter action for the list of MAC addresses in the **MAC Filter Summary** table.<br>Select **Allow** to permit access to the LTE3311, MAC addresses not listed will be denied access to the LTE3311.<br>Select **Deny** to block access to the LTE3311, MAC addresses not listed will be allowed to access the LTE3311. |
| 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 LTE3311. |
| Apply | Click **Apply** to save your changes back to the LTE3311. |
| Cancel | Click **Cancel** to reload the previous configuration for this screen. |

# 7.6 Wireless LAN Advanced Screen

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

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

**Figure 43** Network > Wireless LAN > Advanced




The following table describes the labels in this screen.

**Table 27** Network > Wireless LAN > Advanced

| LABEL | DESCRIPTION |
|---|---|
| RTS/CTS Threshold | Data with its frame size larger than this value will perform the RTS (Request To Send)/ CTS (Clear To Send) handshake.<br><br>This field is not configurable and the LTE3311 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.<br><br>This field is not configurable and the LTE3311 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).<br><br>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 LTE3311 reduces the output power of the transmitter from about 260mA to 188mA when there is no IEEE 802.11 wireless clients associated with the LTE3311 wireless network. |
| Tx Power | Set the output power of the LTE3311 in this field. If there is a high density of APs in an area, decrease the output power of the LTE3311 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 27** Network > Wireless LAN > Advanced (continued)

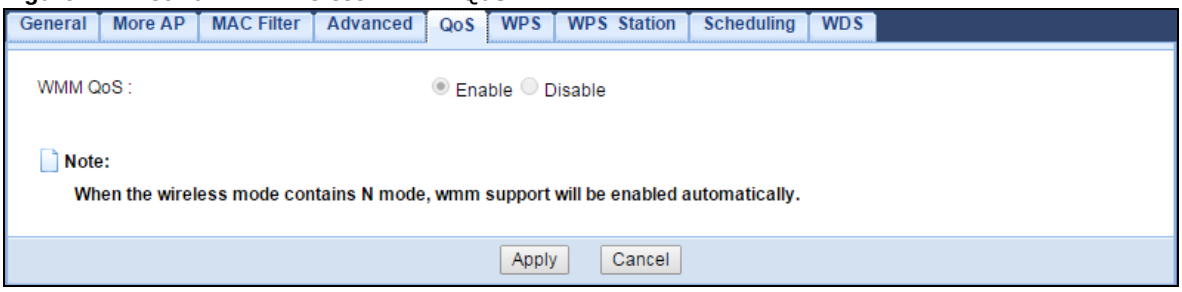
| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save your changes back to the LTE3311. |
| Cancel | Click **Cancel** to reload the previous configuration for this screen. |

# 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 **Network** > **Wireless LAN** > **QoS**. The following screen appears.

**Figure 44** Network > Wireless LAN > QoS




The following table describes the labels in this screen.

**Table 28** Network > Wireless LAN > QoS

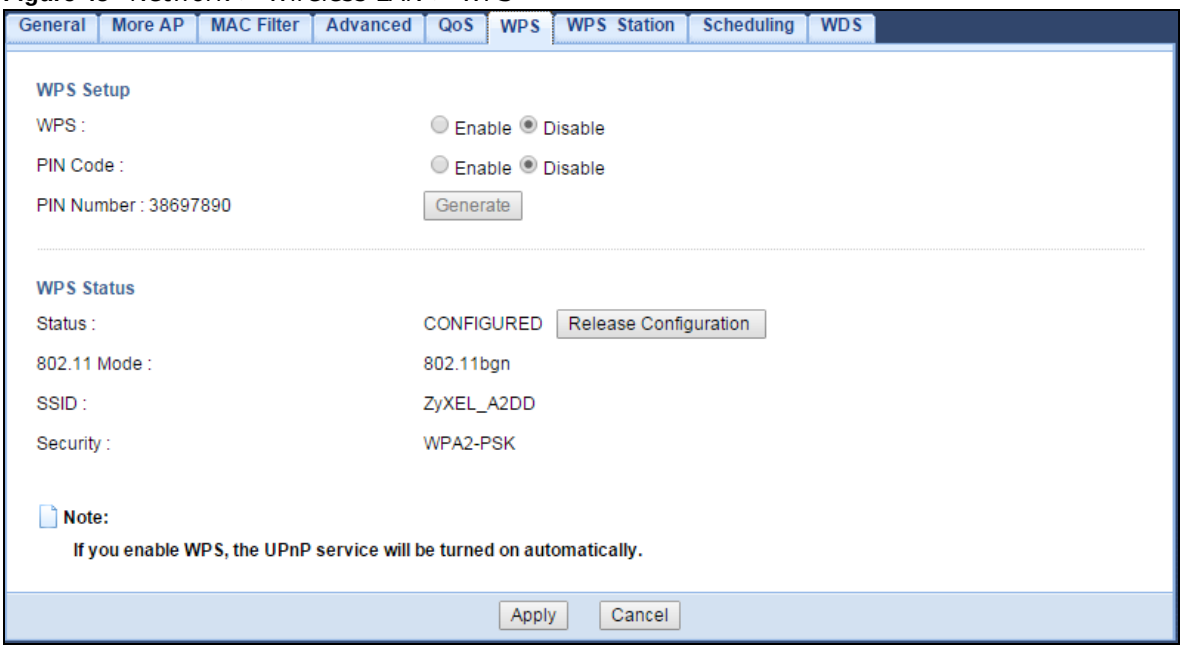
| LABEL | DESCRIPTION |
|---|---|
| WMM QoS | Select **Enable** to have the LTE3311 automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly.<br>This field is not configurable and the LTE3311 automatically enables WMM QoS if you select **802.11n**, **802.11gn** or **802.11bgn** in the **Wireless LAN > General** screen. |
| Apply | Click **Apply** to save your changes to the LTE3311. |
| Cancel | Click **Cancel** to reload the previous configuration for this screen. |

# 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 **Network** > **Wireless LAN** > **WPS**.

Note: With WPS, wireless clients can only connect to the wireless network using the first SSID on the LTE3311.

**Figure 45** Network > Wireless LAN > WPS




The following table describes the labels in this screen.

**Table 29** Network > Wireless LAN > WPS

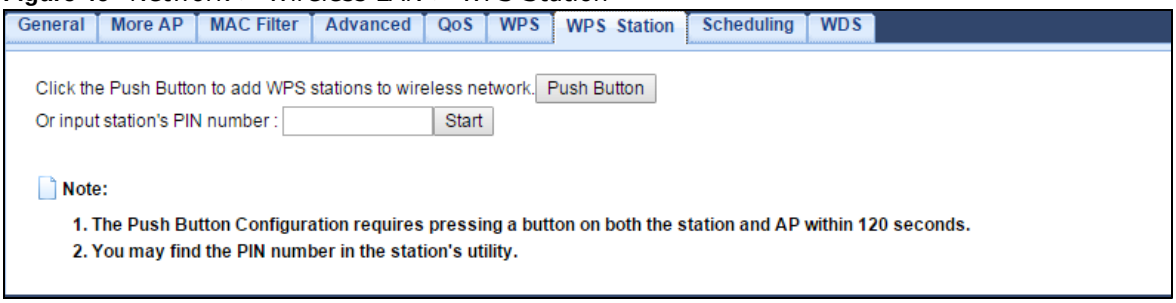
| LABEL | DESCRIPTION |
|---|---|
| WPS Setup | |
| WPS | Select **Enable** to turn on the WPS feature. Otherwise, select **Disable**. |
| PIN Code | Select **Enable** and click **Apply** to allow the PIN Configuration method. If you select **Disable**, you cannot create a new PIN number. |
| PIN Number | This is the WPS PIN (Personal Identification Number) of the LTE3311. Enter this PIN in the configuration utility of the device you want to connect to the LTE3311 using WPS.<br>The PIN is not necessary when you use WPS push-button method.<br>Click **Generate** to generate a new PIN number. |
| WPS Status | |
| Status | This displays **Configured** when the LTE3311 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.<br>This displays **Unconfigured** if WPS is disabled and there are no wireless or wireless security changes on the LTE3311 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**.<br>Click this button to remove all configured wireless and wireless security settings for WPS connections on the LTE3311. |
| 802.11 Mode | This is the 802.11 mode used. Only compliant WLAN devices can associate with the LTE3311. |
| SSID | This is the name of the wireless network (the LTE3311's first SSID). |
| Security | This is the type of wireless security employed by the network. |
| Apply | Click **Apply** to save your changes back to the LTE3311. |
| Cancel | Click **Cancel** to reload the previous configuration for this screen. |

# 7.9 WPS Station Screen

Use this screen when you want to add a wireless station using WPS. To open this screen, click **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 46** Network > Wireless LAN > WPS Station




The following table describes the labels in this screen.

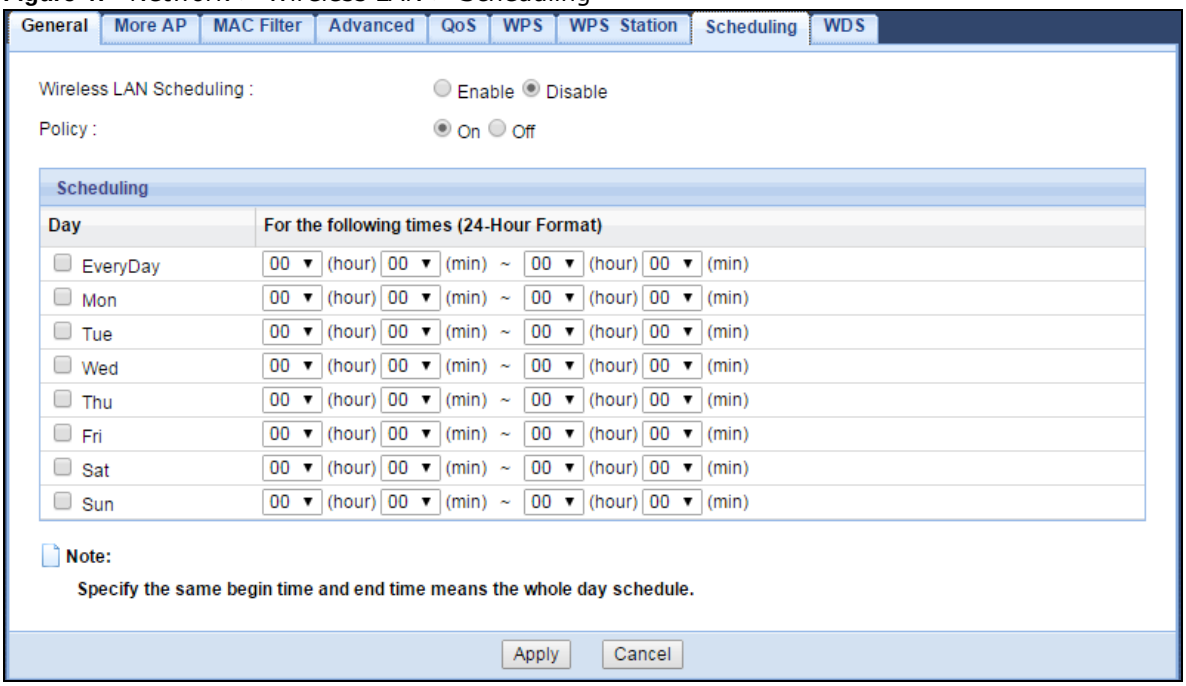
**Table 30** Network > Wireless LAN > WPS Station

| LABEL | DESCRIPTION |
|---|---|
| Push Button | Use this button when you use the PBC (Push Button Configuration) method to configure wireless station's wireless settings.<br><br>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.<br><br>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 **Network** > **Wireless LAN** > **Scheduling** tab.

**Figure 47** Network > Wireless LAN > Scheduling




The following table describes the labels in this screen.

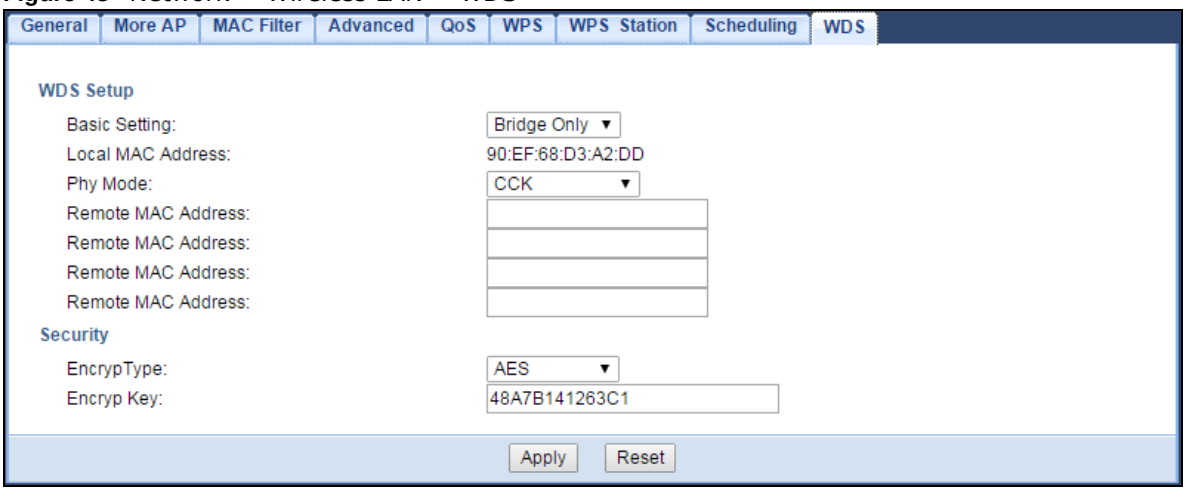
**Table 31** Network > Wireless LAN > Scheduling

| 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. |
| Apply | Click **Apply** to save your changes back to the LTE3311. |
| Cancel | Click **Cancel** to reload the previous configuration for this screen. |

# 7.11 WDS Screen

A Wireless Distribution System (WDS) is a wireless connection between two or more APs. Use this screen to configure the LTE3311's WDS settings. To open this screen, click **Network** > **Wireless LAN** > **WDS** tab.

**Figure 48** Network > Wireless LAN > WDS




The following table describes the labels in this screen.

**Table 32** Network > Wireless LAN > WDS

| LABEL | DESCRIPTION |
|---|---|
| WDS Setup | |
| Basic Setting | Select **Disable** to turn off the WDS function on the LTE3311.<br>Select **AP+Bridge** to have the LTE3311 function as a bridge and access point simultaneously.<br>Select **Bridge Only** to have the LTE3311 act as a wireless bridge only. |
| Local MAC Address | This shows the MAC address of the LTE3311. |
| Phy Mode | Select the physical mode supported by the LTE3311.<br>You must also set the peer device to use the same physical mode. |
| 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. |
| Security | |
| Encryp Type | Select the type of security you want to use (**TKIP** or **AES**) to secure traffic on your WDS. Otherwise, select **No Security**.<br>Select **TKIP** to enable Temporal Key Integrity Protocol (TKIP) security on your WDS. This option is compatible with other ZyXEL access points that support WDS security. Use this if the other access points on your network support WDS security but do not have an AES option.<br>AES provides superior security to TKIP. Use **AES** if the other access points on your network support it for the WDS. |
| Encryp Key | Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).<br>You must also set the peer device to use the same pre-shared key. |
| Apply | Click **Apply** to save your changes back to the LTE3311. |
| Reset | Click **Reset** to reload the previous configuration for this screen. |

# 8

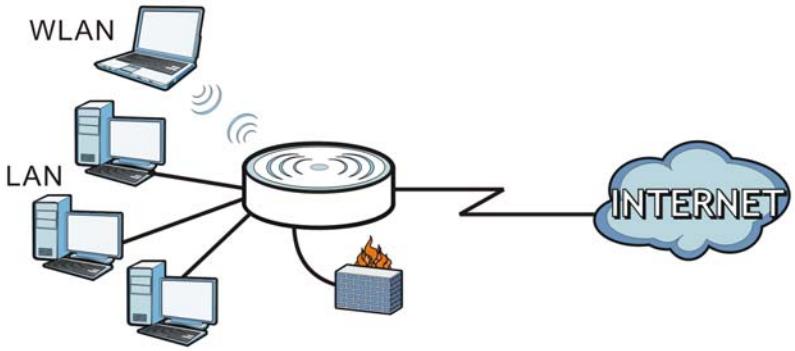
# LAN

## 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 49** LAN Example




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

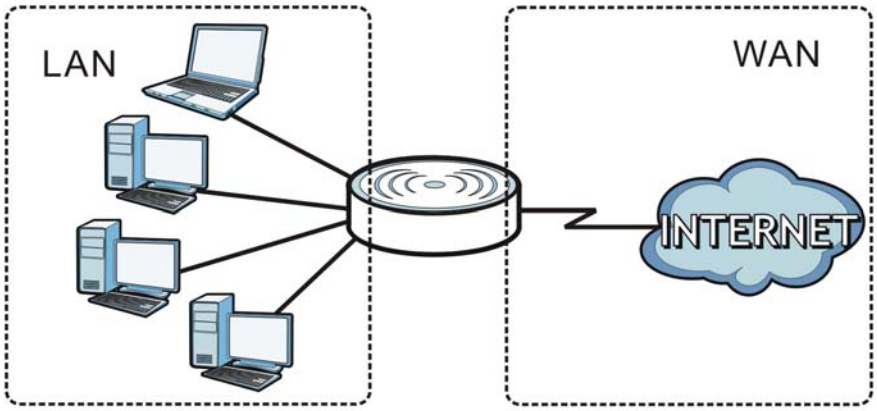
## 8.2 What You Can Do

- Use the **IP** screen to change the IP address for your LTE3311 (Section 8.4 on page 85).

## 8.3 What You Need To Know

The actual physical connection determines whether the LTE3311 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 50** LAN and WAN IP Addresses




The LAN parameters of the LTE3311 are preset in the factory with the following values:

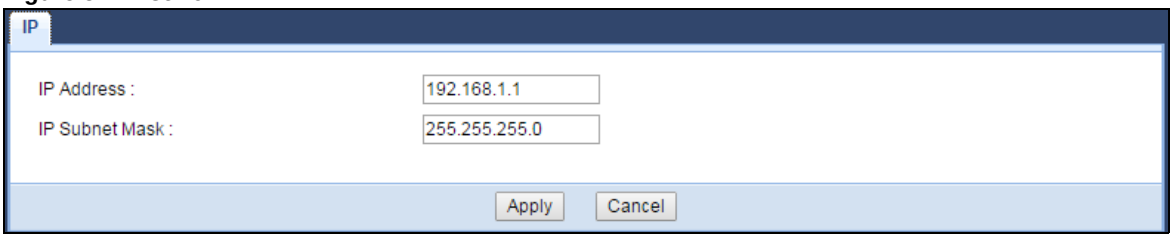
- IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

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 LTE3311. Click **Network > LAN > IP**.

**Figure 51** Network > LAN > IP




The following table describes the labels in this screen.

**Table 33** Network > LAN > IP

| LABEL | DESCRIPTION |
|---|---|
| IP Address | Type the IP address of your LTE3311 in dotted decimal notation. |
| IP Subnet Mask | The subnet mask specifies the network number portion of an IP address. Your LTE3311 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 LTE3311. |
| Apply | Click **Apply** to save your changes back to the LTE3311. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

# 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 LTE3311's LAN as a DHCP server or disable it. When configured as a server, the LTE3311 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 86).
- 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 88).
- Use the **Client List** screen to view the current DHCP client information (Section 9.4 on page 90).

### 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.

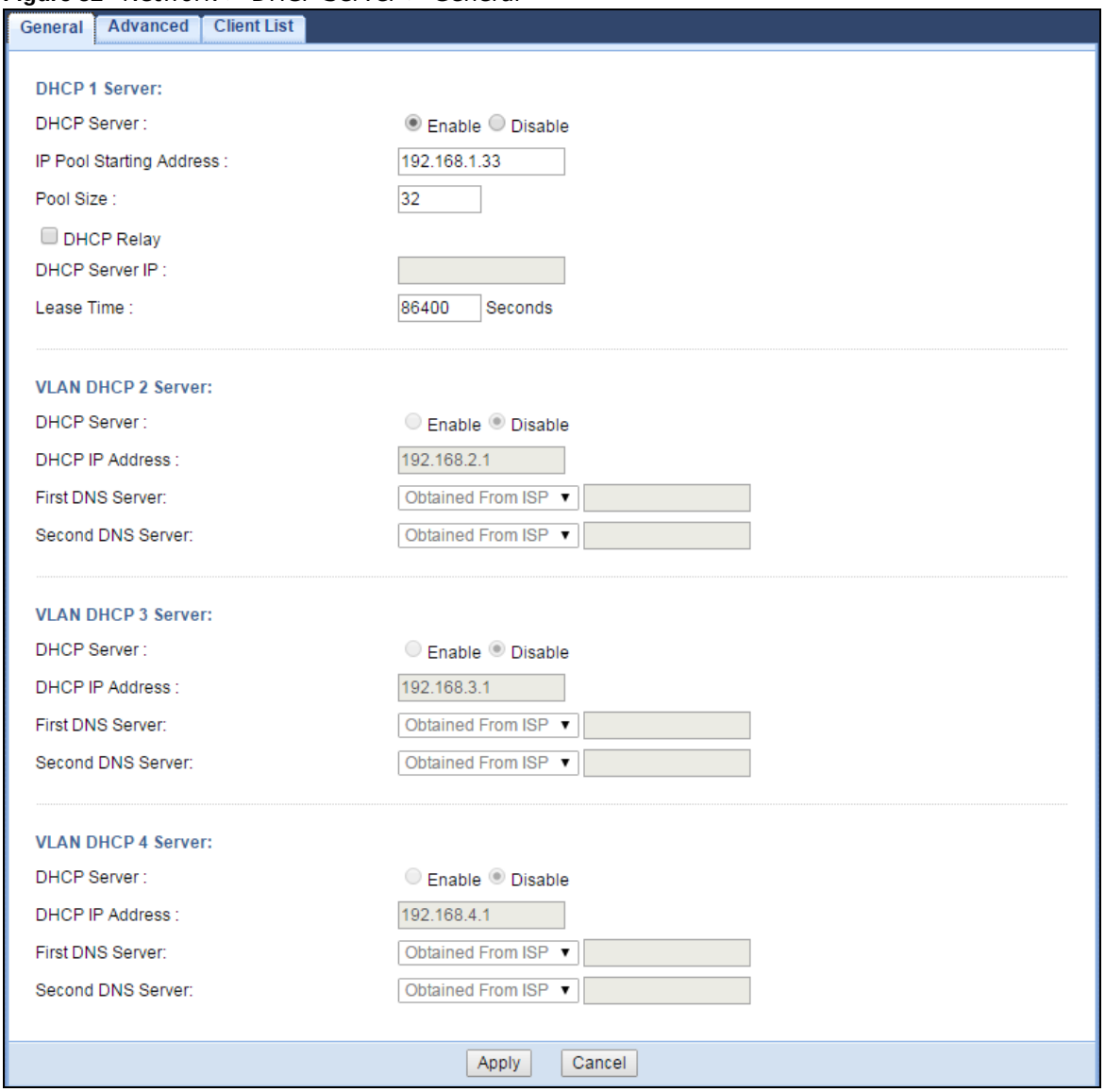
#### IP Pool Setup

The LTE3311 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 LTE3311 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 LTE3311 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 **Network** > **DHCP Server**. The following screen displays.

**Figure 52** Network > DHCP Server > General




The following table describes the labels in this screen.

**Table 34** Network > DHCP Server > General

| LABEL | DESCRIPTION |
|---|---|
| DHCP Server | Select **Enable** to activate DHCP for LAN.<br><br>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 LTE3311 acting as a DHCP server. When configured as a server, the LTE3311 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. |
| DHCP Relay | Select this option to have the LTE3311 forward DHCP requests to the DHCP server. |

**Table 34** Network > DHCP Server > General (continued)

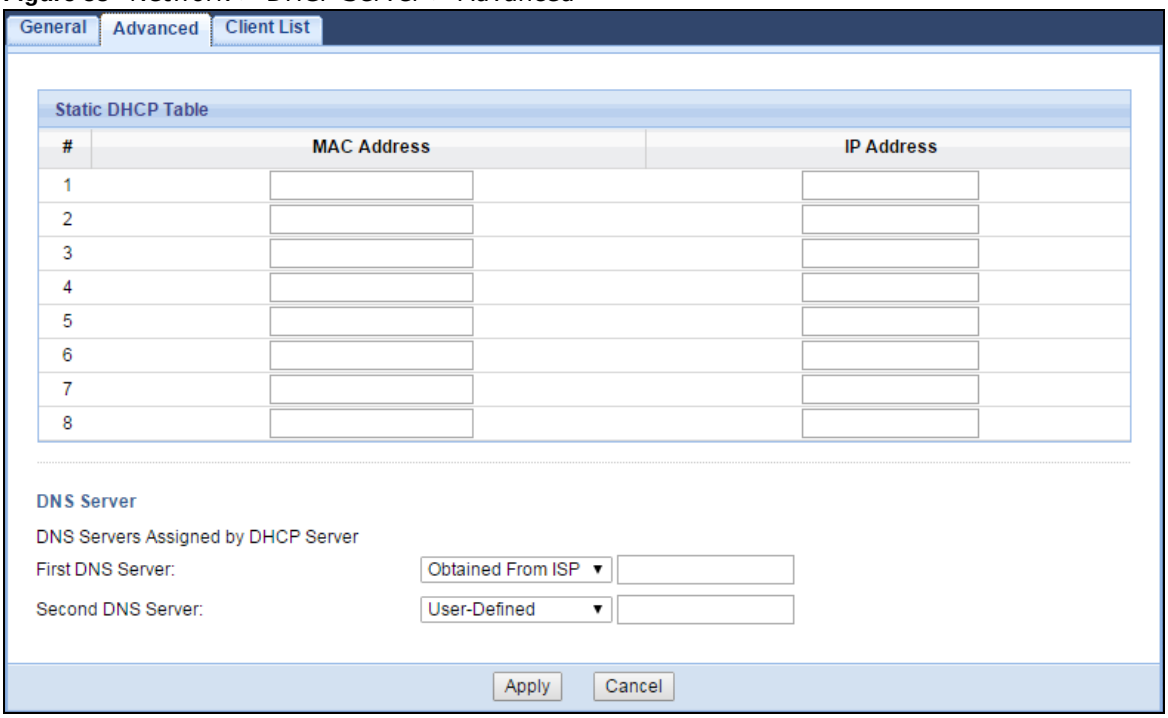
| LABEL | DESCRIPTION |
|---|---|
| DHCP Server IP | This field is configurable only when you select **DHCP Relay**.<br><br>Enter the IP address of the actual remote DHCP server in this field. |
| Lease Time | This is the period of time DHCP-assigned addresses is used. DHCP automatically assigns IP addresses 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<br><br>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. |
| DHCP IP Address | Enter the LAN IP address you want to assign to your LTE3311 in this VLAN group. |
| First DNS Server<br><br>Second DNS Server | Specify the IP addresses up to two DNS servers for the DHCP clients to use.<br><br>Select **Obtained From ISP** if your ISP dynamically assigns DNS server information (and the LTE3311's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.<br><br>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.<br><br>Select **DNS Relay** to have the LTE3311 act as a DNS proxy. The LTE3311's LAN IP address displays in the field to the right (read-only). The LTE3311 tells the DHCP clients on the LAN that the LTE3311 itself is the DNS server. When a computer on the LAN sends a DNS query to the LTE3311, the LTE3311 forwards the query to the LTE3311's system DNS server (configured in the **WAN** screen) and relays the response back to the computer. |
| Apply | Click **Apply** to save your changes back to the LTE3311. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

# 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 LTE3311 sends to the DHCP clients.

To change your LTE3311's static DHCP settings, click **Network** > **DHCP Server** > **Advanced**. The following screen displays.

**Figure 53** Network > DHCP Server > Advanced




The following table describes the labels in this screen.

**Table 35** 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 LTE3311 passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. The LTE3311 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<br><br>Second DNS Server | Select **Obtained From ISP** if your ISP dynamically assigns DNS server information (and the LTE3311's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.<br><br>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.<br><br>Select **DNS Relay** to have the LTE3311 act as a DNS proxy. The LTE3311's LAN IP address displays in the field to the right (read-only). The LTE3311 tells the DHCP clients on the LAN that the LTE3311 itself is the DNS server. When a computer on the LAN sends a DNS query to the LTE3311, the LTE3311 forwards the query to the LTE3311's system DNS server (configured in the **WAN** screen) and relays the response back to the computer. |
| Apply | Click **Apply** to save your changes back to the LTE3311. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

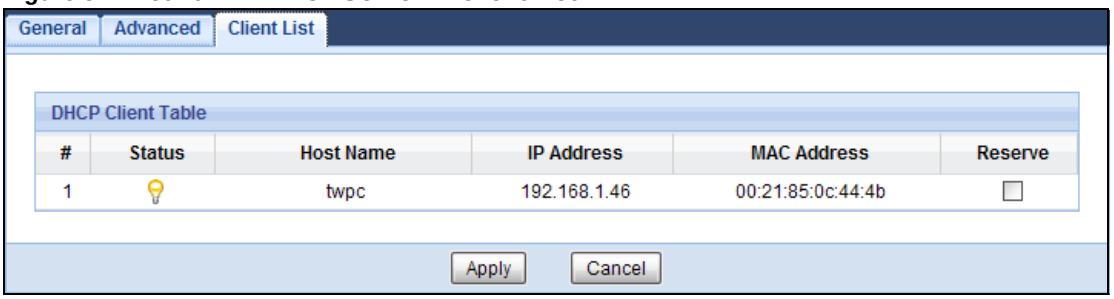
# 9.4 DHCP Client List Screen

The DHCP table shows current DHCP client information (including IP Address, Host Name and MAC Address) of network clients using the LTE3311's DHCP servers.

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

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

**Figure 54** Network > DHCP Server > Client List




The following table describes the labels in this screen.

**Table 36** Network > DHCP Server > Client List

| LABEL | DESCRIPTION |
|---|---|
| # | This is the index number of the host computer. |
| Status | This field displays whether the connection to the host computer is up (a yellow bulb) or down (a gray bulb). |
| Host Name | This field displays the computer host name. |
| IP Address | This field displays the IP address relative to the # field listed above. |
| MAC Address | This field shows the MAC address of the computer with the name in the **Host Name** field.<br>Every Ethernet device has a unique MAC (Media Access Control) address which uniquely identifies a device. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. |
| Reserve | Select this if you want to reserve the IP address for this specific MAC address. |
| Apply | Click **Apply** to save your changes back to the LTE3311. |
| Cancel | Click **Cancel** to reload the previous configuration for this screen. |

# 10 NAT

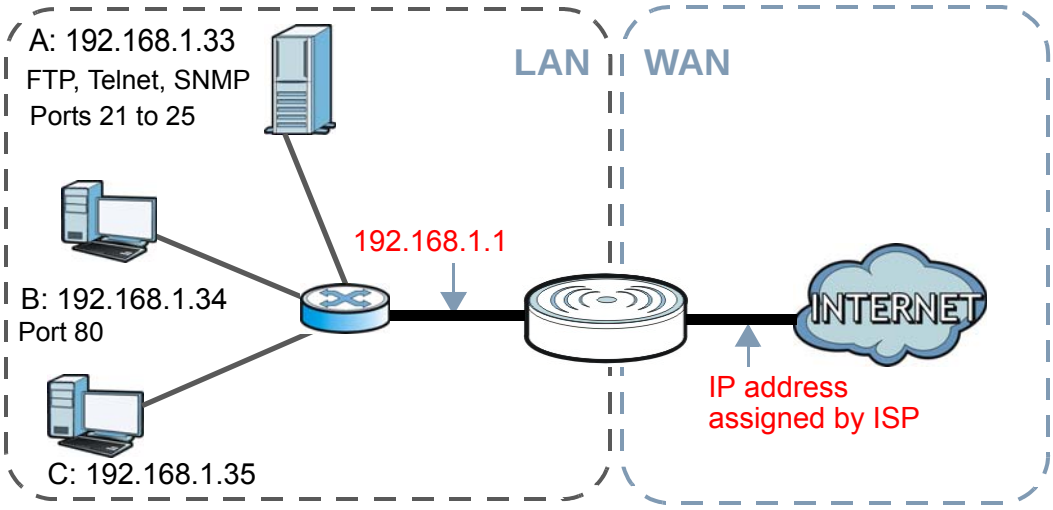
## 10.1 Overview

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 LTE3311. 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 LTE3311, which is 192.168.1.1.

**Figure 55** 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 LTE3311.

### 10.1.1 What You Can Do

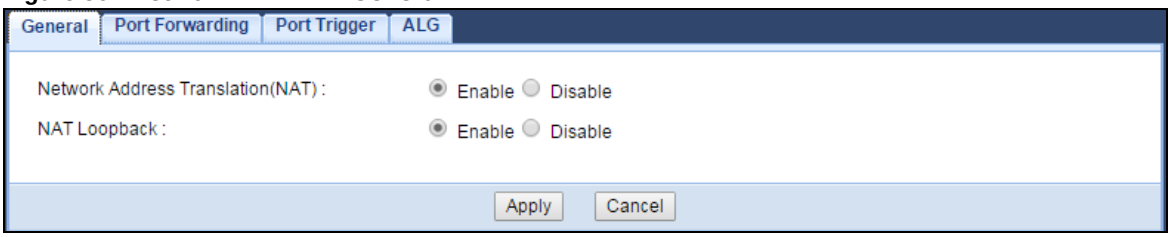
- Use the **General** screen to enable NAT (Section 10.2 on page 92).
- Use the **Port Forwarding** screen to set a default server and change your LTE3311's port forwarding settings to forward incoming service requests to the server(s) on your local network (Section 10.3 on page 92).

- Use the **Port Trigger** screen to change your LTE3311's trigger port settings (Section 10.4 on page 95).
- Use the **ALG** screen to enable or disable SIP (VoIP) ALG (Application Layer Gateway) in the LTE3311 (Section 10.5 on page 96).

# 10.2 General Screen

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

**Figure 56** Network > NAT > General




The following table describes the labels in this screen.

**Table 37** 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).<br><br>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 LTE3311). With NAT loopback enabled, the LTE3311 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.<br><br>Select **Enable** to activate NAT loopback. Select **Disable** to turn it off. |
| Apply | Click **Apply** to save your changes back to the LTE3311. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

# 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.

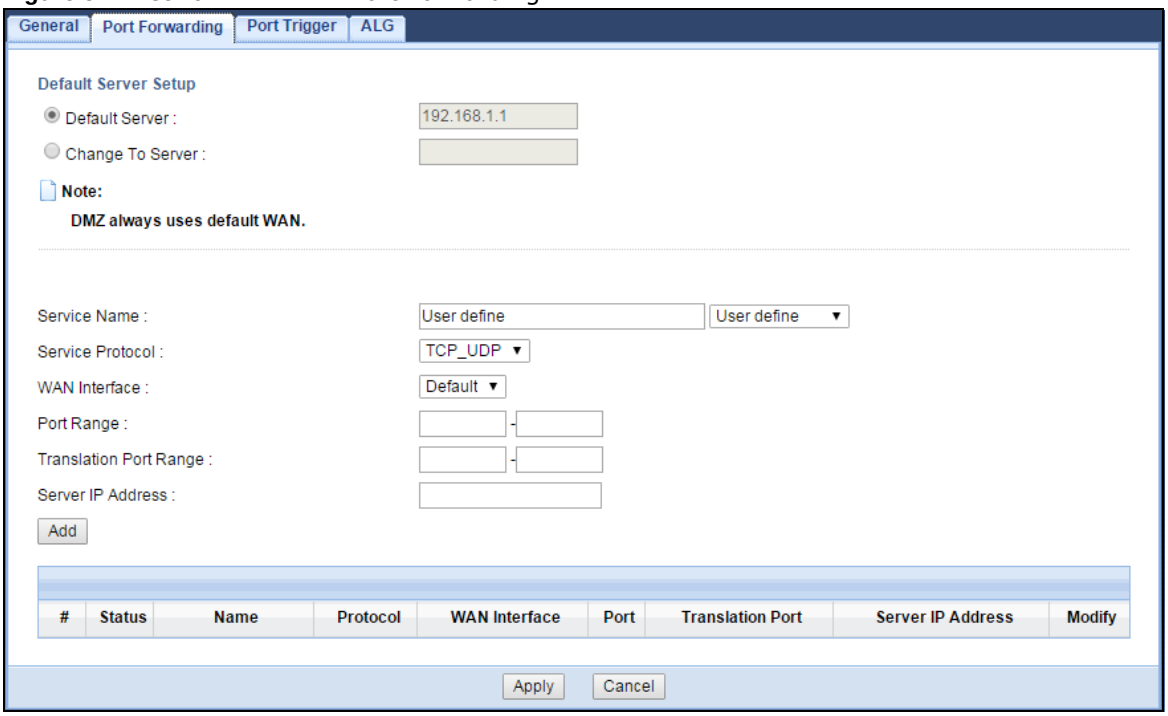
Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your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

Port forwarding allows you to define the local servers to which the incoming services will be forwarded. To change your LTE3311's port forwarding settings, click **Network > NAT** > **Port Forwarding**. The screen appears as shown.

Note: If you do not assign a **Default Server**, the LTE3311 discards all packets received for ports that are not specified in this screen or remote management.

Refer to Appendix D on page 216 for port numbers commonly used for particular services.

**Figure 57** Network > NAT > Port Forwarding




The following table describes the labels in this screen.

**Table 38** 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.<br><br>Select this to use the default server. |
| Change to Server | Select this and manually enter the server's IP address. |

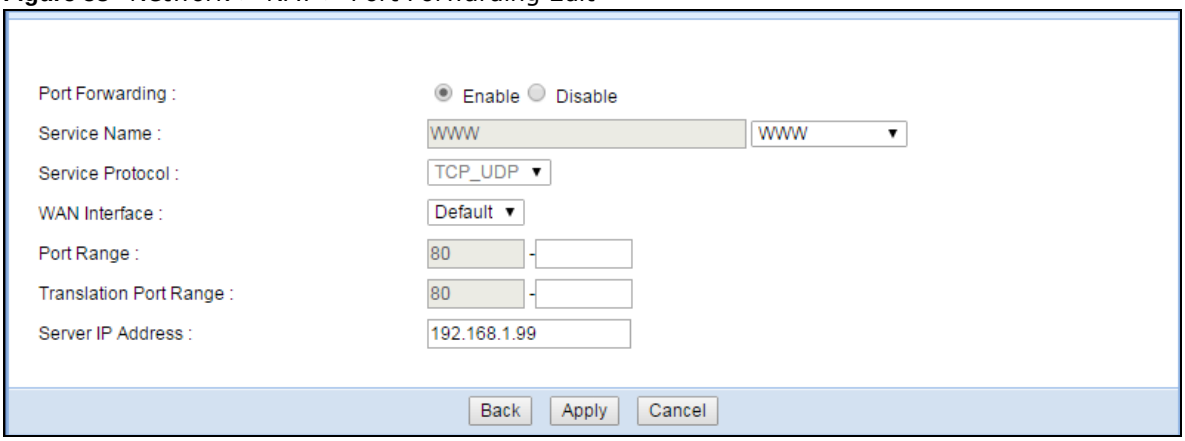
**Table 38** Network > NAT > Port Forwarding (continued)

| 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.<br>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**.<br>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.<br>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.<br>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.<br>Click the **Delete** icon to remove a rule. |
| Apply | Click **Apply** to save your changes back to the LTE3311. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

## 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 58** Network > NAT > Port Forwarding Edit




The following table describes the labels in this screen.

**Table 39** Network > NAT > Port Forwarding Edit

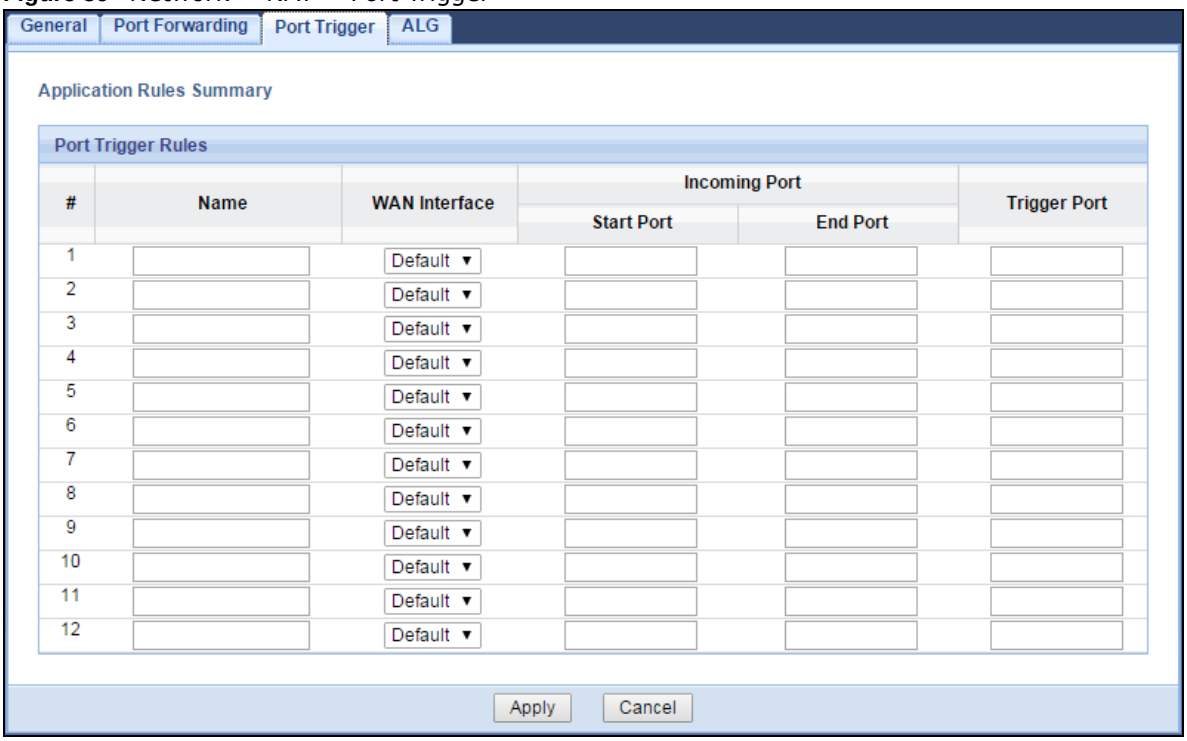
| LABEL | DESCRIPTION |
|---|---|
| Port Forwarding | Select **Enable** to turn on this rule and the requested service can be forwarded to the host with a specified internal IP address.<br>Select **Disable** to disallow forwarding of these ports to an inside server without having to delete the entry. |
| 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**.<br>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.<br>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.<br>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. |
| Apply | Click **Apply** to save your changes back to the LTE3311. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

# 10.4 Port Trigger Screen

To change your LTE3311's trigger port settings, click **Network > NAT > Port Trigger**. The screen appears as shown.

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

**Figure 59** Network > NAT > Port Trigger




The following table describes the labels in this screen.

**Table 40** Network > NAT > Port Trigger

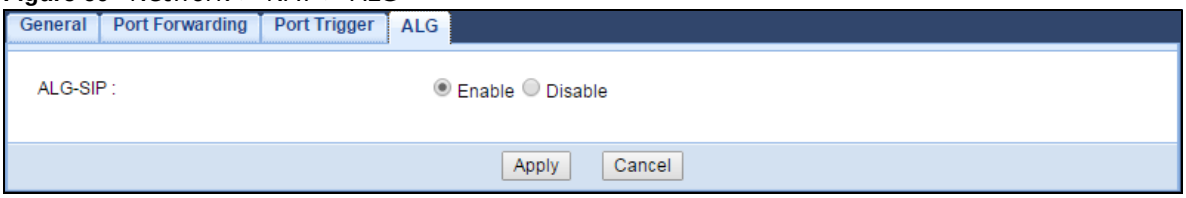
| LABEL | DESCRIPTION |
|---|---|
| # | This is the rule index number (read-only). |
| Name | Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces. |
| WAN Interface | Select the WAN interface through which the matched packets are transmitted. |
| Incoming Port | Incoming Port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The LTE3311 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 LTE3311 to record the IP address of the LAN computer that sent the traffic to a server on the WAN. |
| Apply | Click **Apply** to save your changes back to the LTE3311. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

# 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 LTE3311 registers with the SIP register server, the SIP ALG translates the LTE3311'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 LTE3311 is behind a SIP ALG

To enable and disable the SIP ALG in the LTE3311, click **Network > NAT > ALG**. The screen appears as shown.

**Figure 60** Network > NAT > ALG




The following table describes the labels in this screen.

**Table 41** 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. |
| Apply | Click **Apply** to save your changes back to the LTE3311. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

# 10.6 Technical Reference

The following section contains additional technical information about the LTE3311 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.

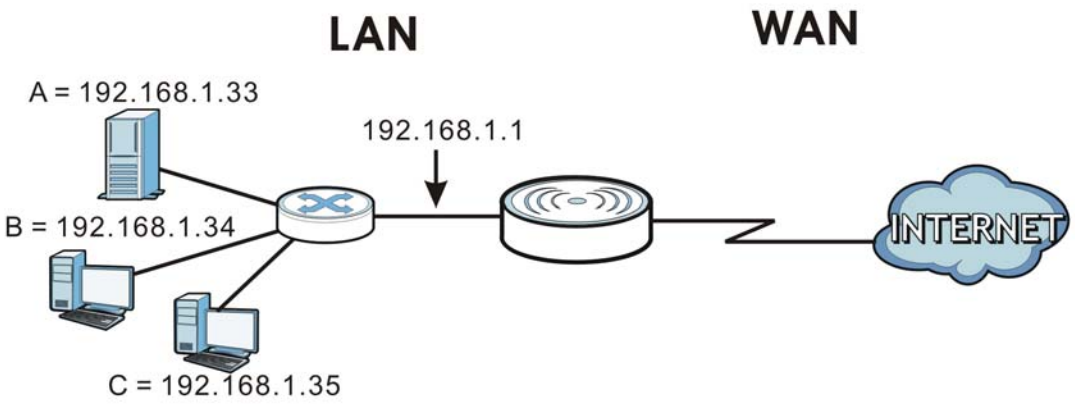
In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

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 61** Multiple Servers Behind NAT Example




## 10.6.3 Trigger Port Forwarding

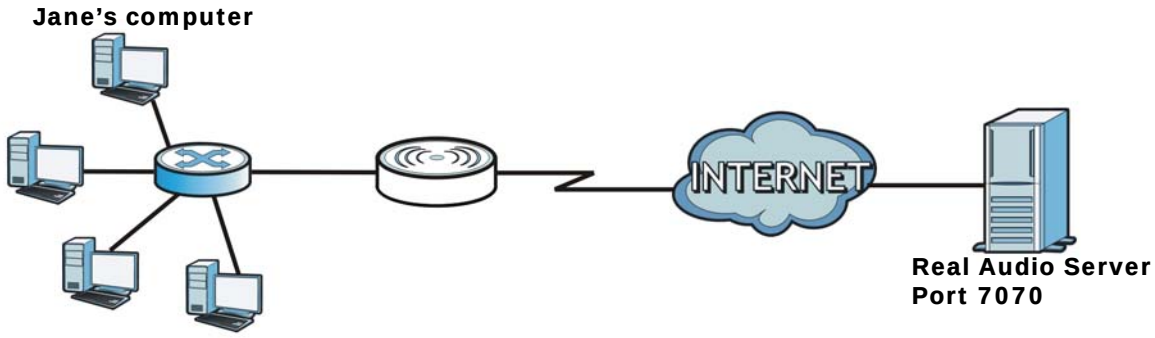
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem 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 LTE3311 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 LTE3311's WAN port receives a response with a specific port number and protocol ("incoming" port), the LTE3311 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 62** 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 LTE3311 to record Jane's computer IP address. The LTE3311 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 LTE3311 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 LTE3311 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 LTE3311 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.

# 11

# DDNS

## 11.1 Overview

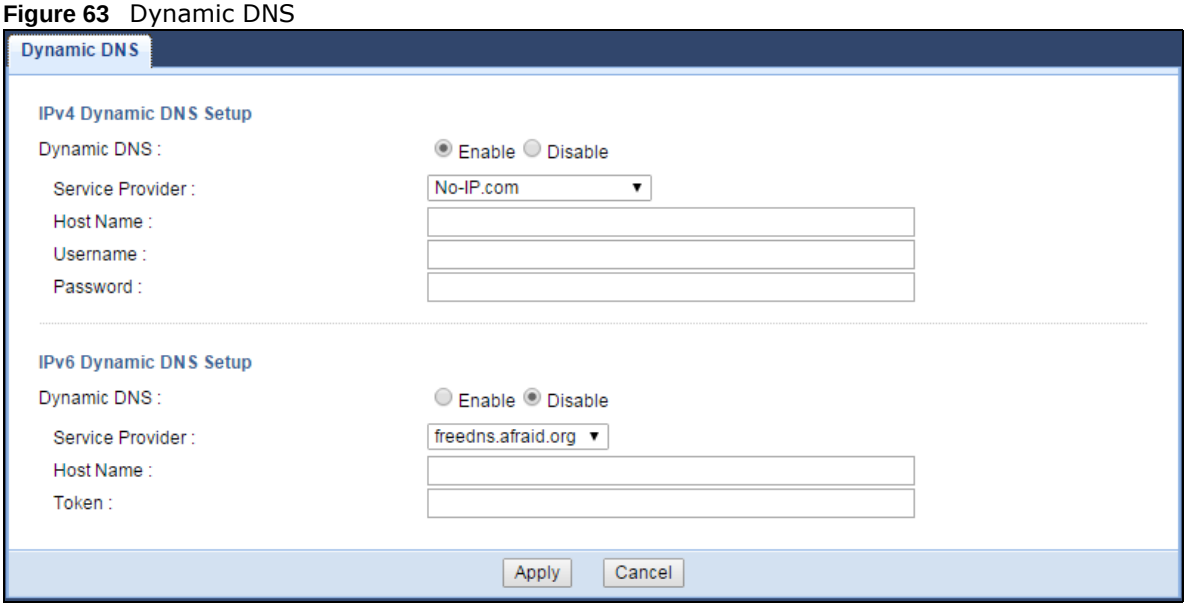
Dynamic Domain Name Service (DDNS) services let you use a fixed domain name with a dynamic IP address. Users can always use the same domain name instead of a different dynamic IP address that changes each time to connect to the LTE3311 or a server in your network.

Note: The LTE3311 must have a public global IP address and you should have your registered DDNS account information on hand.

## 11.2 General

To change your LTE3311's DDNS, click **Network > DDNS**. The screen appears as shown.

**Figure 63** Dynamic DNS




The following table describes the labels in this screen.

**Table 42** 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 42** 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. |
| Apply | Click **Apply** to save your changes back to the LTE3311. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

# 12 Routing

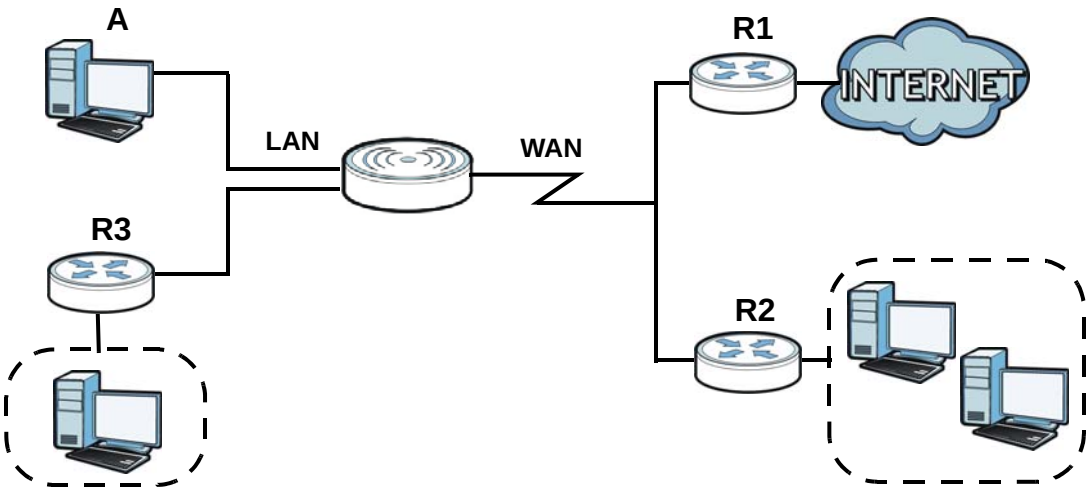
## 12.1 Overview

This chapter shows you how to configure static routes for your LTE3311.

The LTE3311 usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the LTE3311 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 LTE3311's LAN interface. The LTE3311 routes most traffic from **A** to the Internet through the LTE3311'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.

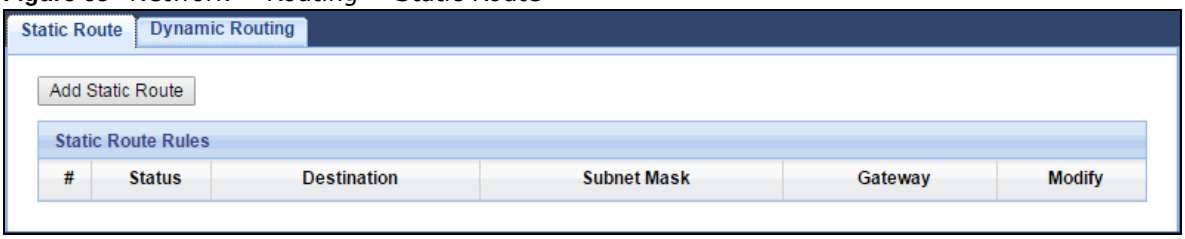
**Figure 64** Example of Static Routing Topology




## 12.2 Static Route Screen

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

**Figure 65** Network > Routing > Static Route




The following table describes the labels in this screen.

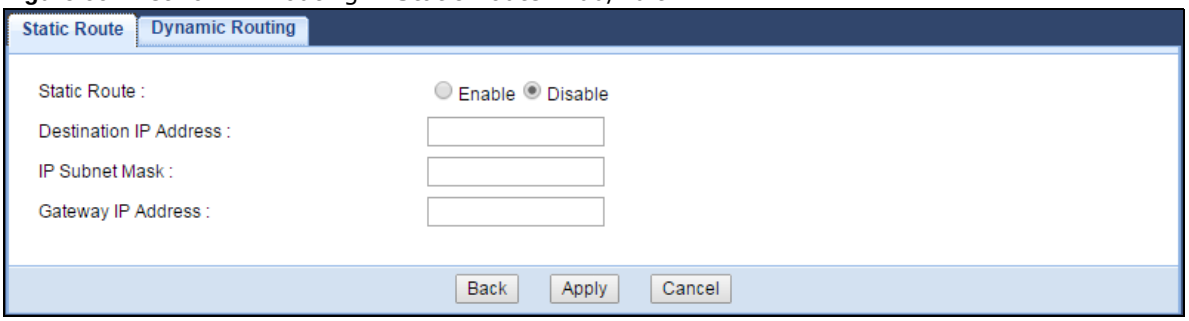
**Table 43** Network > Routing > Static Route

| 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.<br>Click the **Delete** icon to remove a rule from the LTE3311. |

## 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 66** Network > Routing > Static Route: Add/Edit




The following table describes the labels in this screen.

**Table 44** 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. |

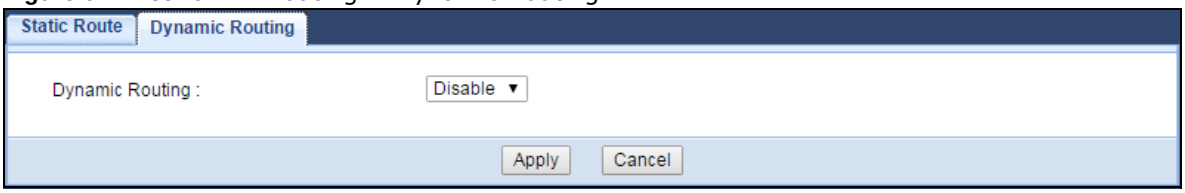
**Table 44** Network > Routing > Static Route: Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| 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 LTE3311's interface(s). The gateway helps forward packets to their destinations. |
| Back | Click **Back** to return to the previous screen without saving. |
| Apply | Click **Apply** to save your changes back to the LTE3311. |
| Cancel | Click **Cancel** to set every field in this screen to its last-saved value. |

# 12.3 Dynamic Routing Screen

Use this screen to enable and configure RIP on the LTE3311. Click **Network > Routing > Dynamic Routing** to open the **Dynamic Routing** screen.

**Figure 67** Network > Routing > Dynamic Routing




The following table describes the labels in this screen.

**Table 45** 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 LTE3311 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.<br>Select the RIP version from **RIPv1** and **RIPv2**. Otherwise, select **Disable** to turn if off. |
| Apply | Click **Apply** to save your changes back to the LTE3311. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

# 13

# Interface Group

## 13.1 Overview

By default, the four LAN interfaces on the LTE3311 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).

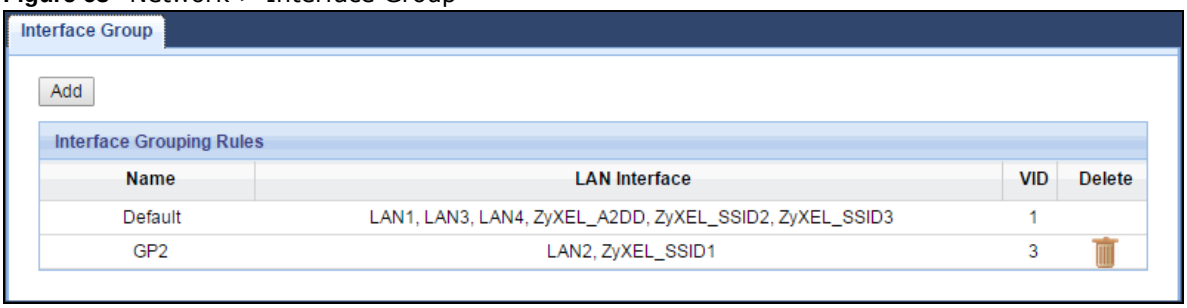
## 13.2 Interface Group Screen

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 LTE3311 assigns to the clients in the default and/or user-defined groups. See Chapter 9 on page 86 for more information.

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

**Figure 68** Network > Interface Group




The following table describes the fields in this screen.

**Table 46** Network > Interface Group

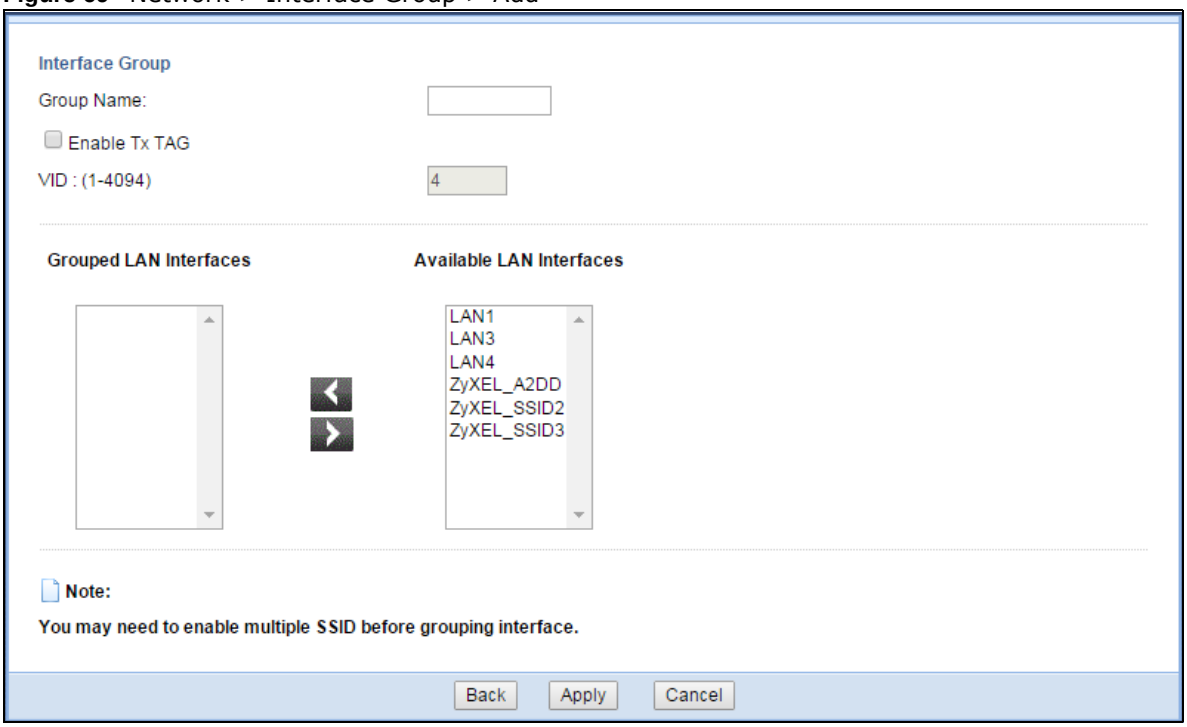
| LABEL | DESCRIPTION |
|---|---|
| Add | Click this button to create a new interface group. |
| Name | This shows the descriptive name of the group. |
| LAN Interface | This shows the interface group. |
| VID | This shows the VLAN ID number (from 0 to 4094) of the interface group. |
| Modify | Click 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 69** Network > Interface Group > Add




The following table describes the fields in this screen.

**Table 47** 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.<br><br>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.<br><br>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.<br><br>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. |
| Apply | Click **Apply** to save your changes back to the LTE3311. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 14 Firewall

## 14.1 Overview

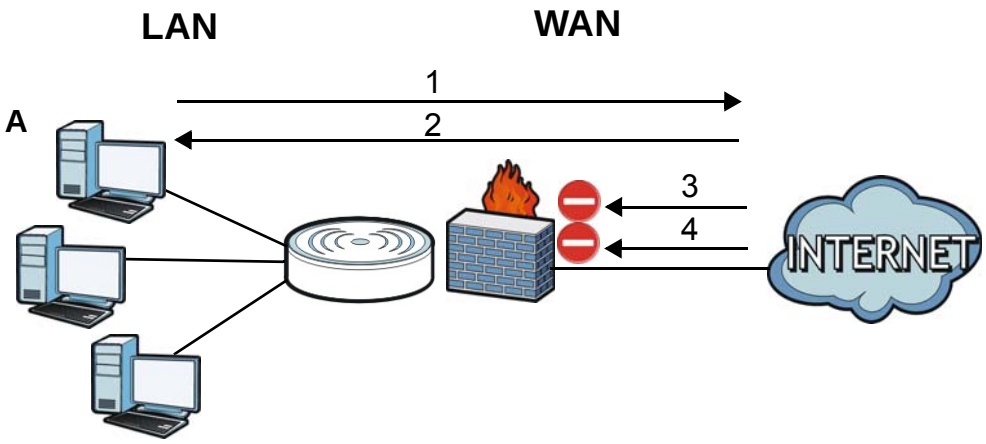
Use these screens to enable and configure the firewall that protects your LTE3311 and your LAN from unwanted or malicious traffic.

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 70** Default Firewall Action




### 14.1.1 What You Can Do

- Use the **General** screen to enable or disable the LTE3311's firewall (Section 14.2 on page 108).
- 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 109).

### 14.1.2 What You Need To Know

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

### About the LTE3311 Firewall

The LTE3311’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 LTE3311's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The LTE3311 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 LTE3311 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 LTE3311 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.

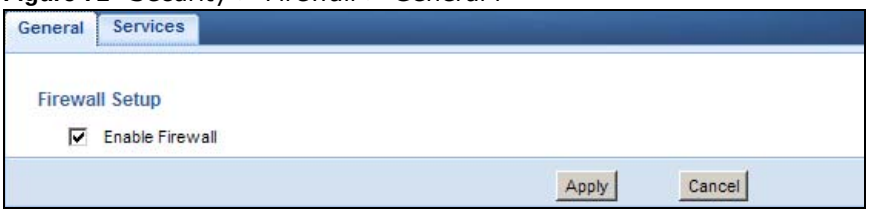
### Guidelines For Enhancing Security With Your Firewall

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 LTE3311’s firewall, and set up firewall logs. Click **Security** > **Firewall** to open the **General** screen.

**Figure 71** Security > Firewall > General l




The following table describes the labels in this screen.

**Table 48** Security > Firewall > General

| LABEL | DESCRIPTION |
|---|---|
| Enable Firewall | Select this check box to activate the firewall. The LTE3311 performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated. |
| Apply | Click **Apply** to save the settings. |
| Cancel | Click **Cancel** to start configuring this screen again. |

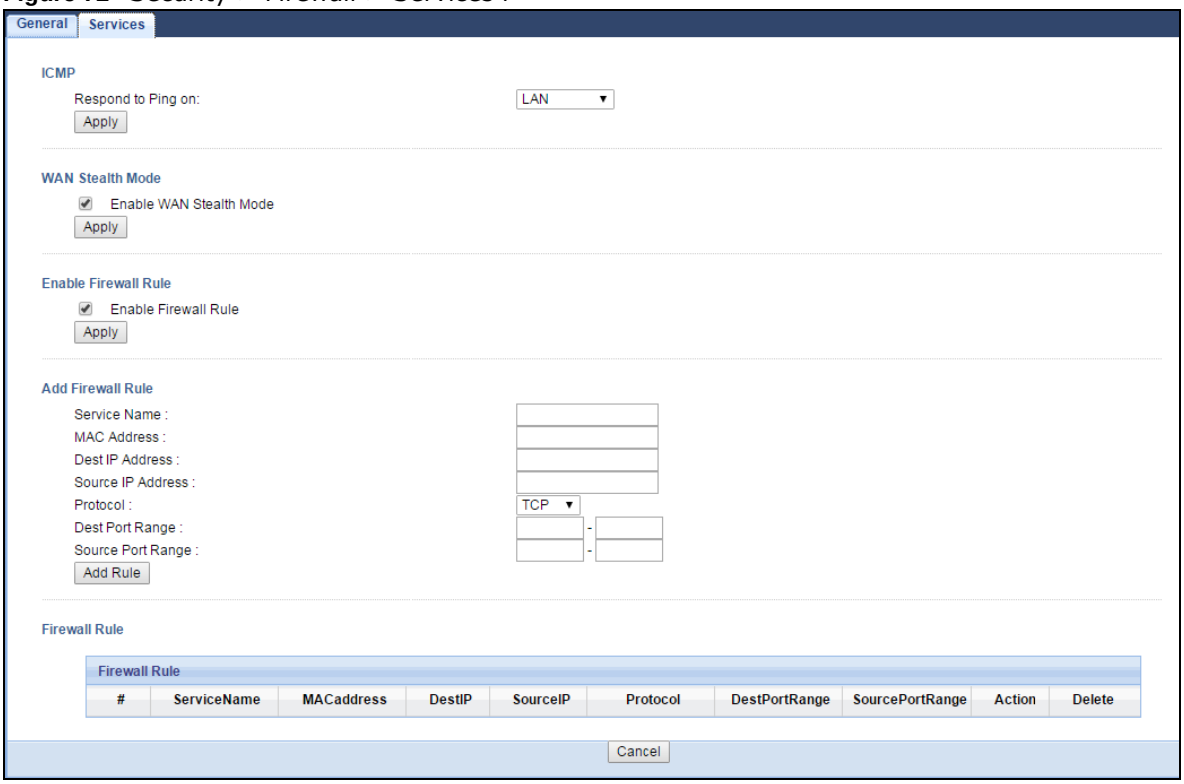
# 14.3 Services Screen

If an outside user attempts to probe an unsupported port on your LTE3311, an ICMP response packet is automatically returned. This allows the outside user to know the LTE3311 exists. Use this screen to prevent the ICMP response packet from being sent. This keeps outsiders from discovering your LTE3311 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 **Security** > **Firewall** > **Services**. The screen appears as shown next.

**Figure 72** Security > Firewall > Services l




The following table describes the labels in this screen.

**Table 49** 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 LTE3311 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. |
| Add Firewall Rule | |
| Service Name | Enter a name that identifies or describes the firewall rule. |
| MAC Address | Enter the MAC address of the computer for which the firewall rule applies. |

**Table 49** Security > Firewall > Services (continued)

| LABEL | DESCRIPTION |
|---|---|
| Dest IP Address | Enter the IP address of the computer to which traffic for the application or service is entering.<br>The LTE3311 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.<br>The LTE3311 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. |
| Cancel | Click **Cancel** to start configuring this screen again. |

See Appendix D on page 216 for commonly used services and port numbers.

# 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 LTE3311 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.

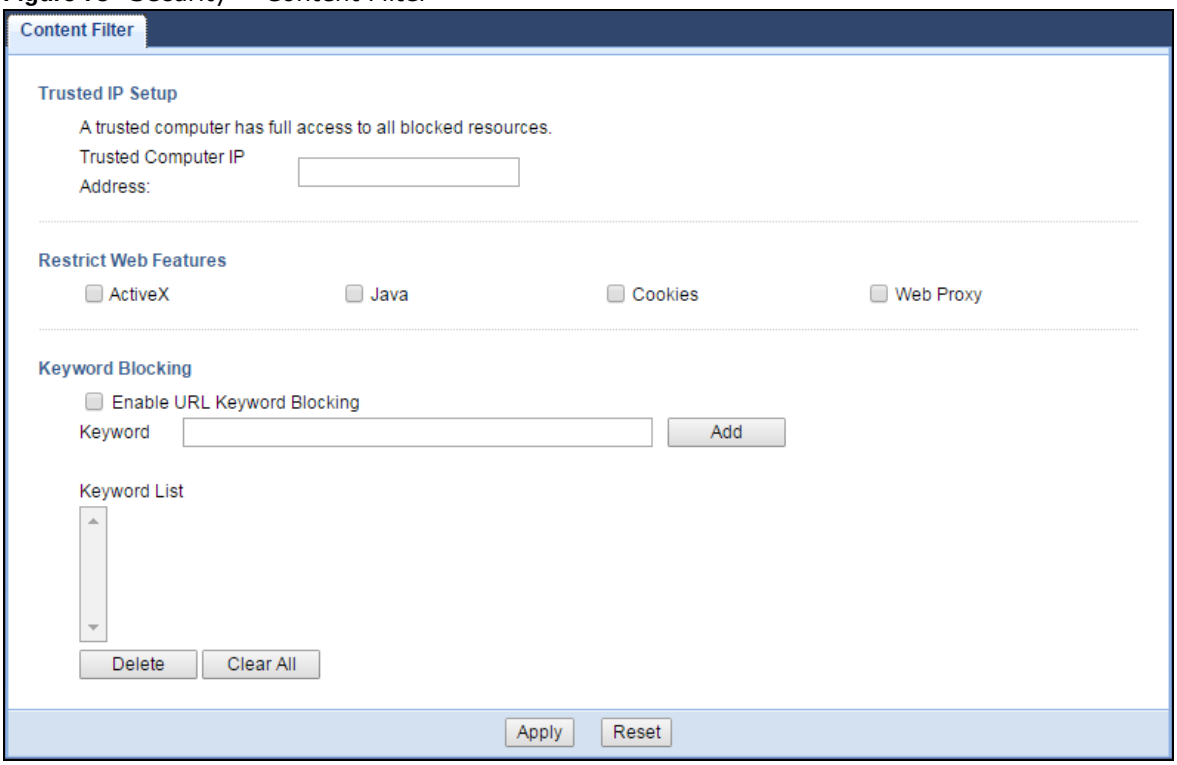
The file path is the characters that come after the first slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the file path is news/pressroom.php.

Since the LTE3311 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 LTE3311 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 **Security** > **Content Filter** to open the **Content Filter** screen.

**Figure 73** Security > Content Filter




The following table describes the labels in this screen.

**Table 50** 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.<br><br>Leave this field blank to have no trusted computers. |
| Restrict Web Features | Select the box(es) to restrict a feature. When you download a page containing a restricted feature, that part of the web page will appear blank or grayed out. |
| ActiveX | A tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again. |
| Java | A programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds. |
| Cookies | Used by Web servers to track usage and provide service based on ID. |
| Web Proxy | A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server. |
| Enable URL Keyword Blocking | The LTE3311 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. |
| Keyword List | This list displays the keywords already added. |

**Table 50** Security > Content Filter (continued)

| LABEL | DESCRIPTION |
|---|---|
| Add | Click **Add** after you have typed a keyword.<br>Repeat this procedure to add other keywords. Up to 64 keywords are allowed.<br>When you try to access a web page containing a keyword, you will get a message telling you that the content filter is blocking this request. |
| Delete | Highlight a keyword in the lower box and click **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. |
| Apply | Click **Apply** to save your changes. |
| Reset | Click **Reset** to begin configuring this screen afresh |

# 16

# IPv6 Firewall

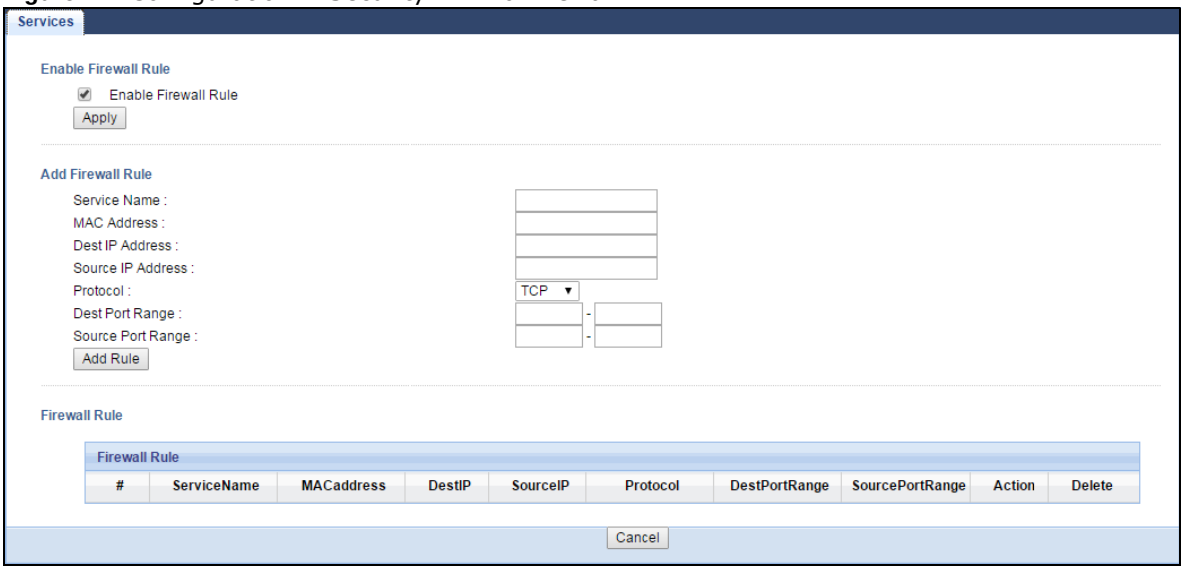
## 16.1 Overview

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 74** Configuration > Security > IPv6 Firewall




The following table describes the labels in this screen.

**Table 51** 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). |
| 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. |

**Table 51** Configuration > Security > IPv6 Firewall (continued)

| LABEL | DESCRIPTION |
|---|---|
| Dest IP Address | Enter the IPv6 address of the computer to which traffic for the application or service is entering.<br>The LTE3311 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.<br>The LTE3311 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. |

# 17

# Voice over IP

## 17.1 Overview

Use this chapter to:

- Connect an analog phone to the LTE3311.
- Make phone calls over the Internet, as well as the regular phone network.
- Configure settings such as speed dial.
- Configure network settings to optimize the voice quality of your phone calls.

### 17.1.1 What You Can Do in this Chapter

These screens allow you to configure your LTE3311 to make phone calls over the Internet and your regular phone line, and to set up the phone you connect to the LTE3311.

- Use the **General** screen to enable VoIP, NAT traversal and dialing plan on the LTE3311 (Section 17.3 on page 118).
- Use the **Phone Book** screen to manage your contact names and phone numbers (Section 17.4 on page 119).
- Use the **Speed Dial** screen to set up shortcuts for dialing frequently-used (VoIP) phone numbers (Section 17.5 on page 120).
- Use the **Phone Conf.** screen to configure call features (Section 17.6 on page 121).
- Use the **SIP Conf.** screen to set up information about your SIP account, and configure the SIP server information (Section 17.7 on page 123).

### 17.1.2 What You Need to Know About VoIP

#### VoIP

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

#### SIP

SIP stands for Session Initiation Protocol. SIP is a signalling standard that lets one network device (like a computer or the LTE3311) send messages to another. In VoIP, these messages are about phone calls over the network. For example, when you dial a number on your LTE3311, it sends a SIP message over the network asking the other device (the number you dialed) to take part in the call.

### SIP Accounts

A SIP account is a type of VoIP account. It is an arrangement with a service provider that lets you make phone calls over the Internet. When you set the LTE3311 to use your SIP account to make calls, the LTE3311 is able to send all the information about the phone call to your service provider on the Internet.

Strictly speaking, you don't need a SIP account. It is possible for one SIP device (like the LTE3311) to call another without involving a SIP service provider. However, the networking difficulties involved in doing this make it tremendously impractical under normal circumstances. Your SIP account provider removes these difficulties by taking care of the call routing and setup - figuring out how to get your call to the right place in a way that you and the other person can talk to one another.

### How to Find Out More

See Section 17.8 on page 127 for advanced technical information on SIP.

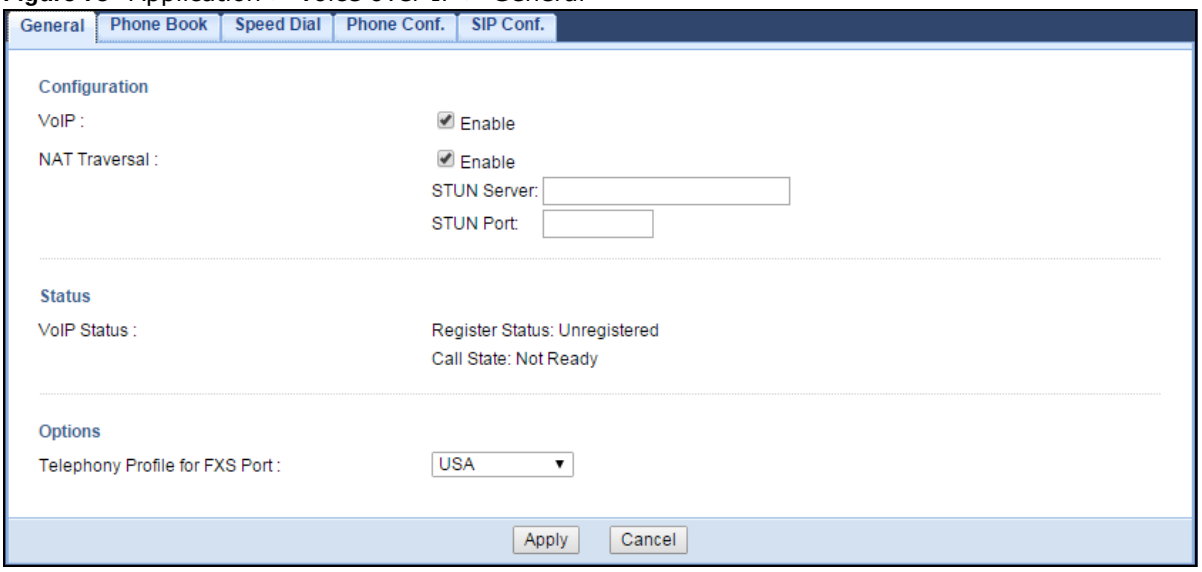
## 17.2 Before You Begin

- Before you can use these screens, you need to have a VoIP account already set up. If you don't have one yet, you can sign up with a VoIP service provider over the Internet.
- You should have the information your VoIP service provider gave you ready, before you start to configure the LTE3311.

## 17.3 VoIP General Screen

Use this screen to enable VoIP and configure general VoIP settings on the LTE3311. To access this screen, click **Application > Voice over IP > General**.

**Figure 75** Application > Voice over IP > General



The following table describes the labels in this screen.

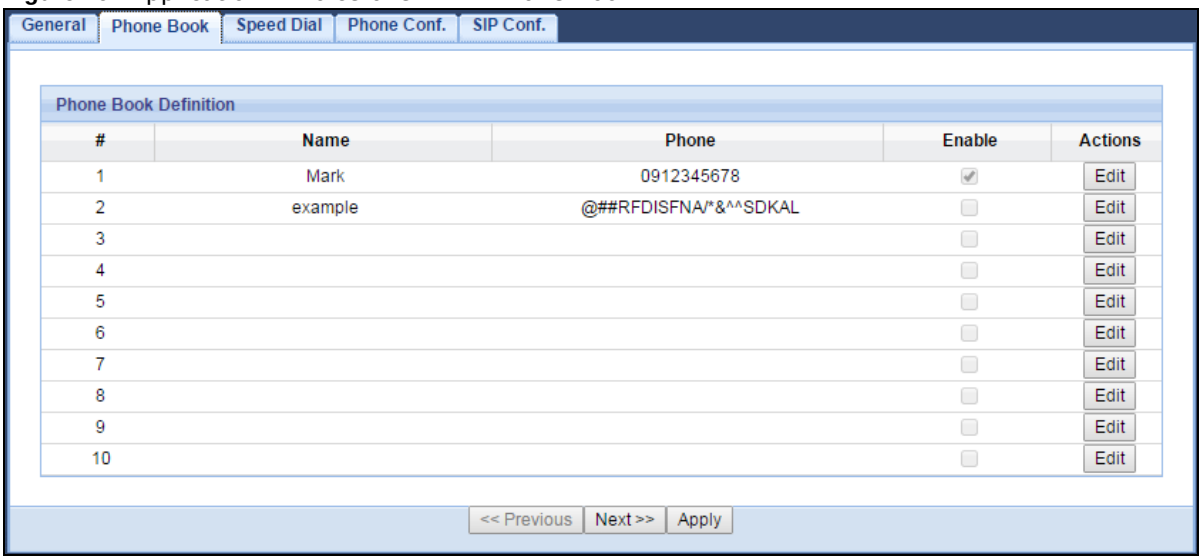
**Table 52** Application > Voice over IP > General

| LABEL | DESCRIPTION |
|---|---|
| VoIP | Select **Enable** to activate VoIP on the LTE3311. |
| NAT Traversal | Select **Enable** to use the STUN service.<br><br>STUN (Simple Traversal of UDP through NATs) allows the VoIP device to find the presence and types of NAT routers and/or firewalls between it and the public Internet. STUN also allows the VoIP device to find the public IP address that NAT assigned, so the VoIP device can embed it in the SIP data stream. |
| STUN Server | Enter the IP address of the STUN server. |
| STUN Port | Enter the port number used by the STUN server. |
| VoIP Status | This shows the current registration status of the SIP account. It also shows the current state of the phone call.<br><br>• **ready**: VoIP is enabled and a SIP account is registered for the phone port.<br>• **not ready**: VoIP is disabled or there is no SIP account registered for the phone port.<br>• **busy**: There is a VoIP call in progress or the callee's line is busy?<br>• **ringing**: The phone is ringing for an incoming VoIP call<br>• **dialing**: The callee's phone is ringing.<br>• **off hook**: The callee hung up or your phone was left off the hook? |
| Telephony Profile for FXS port | One FXS port is an RJ11 port that connects to an analog phone.<br><br>Select a country to specify the type of the dial tone for your VoIP phone. If your country is not in the list, it's recommended that you use the US dial tone. |
| Apply | Click **Apply** to save the settings. |
| Cancel | Click **Cancel** to start configuring this screen again. |

# 17.4 Phone Book Screen

Use this screen to manage your contact names and phone numbers. To access this screen, click **Application > Voice over IP > Phone Book**.

**Figure 76** Application > Voice over IP > Phone Book



The following table describes the labels in this screen.

**Table 53** Application > Voice over IP > Phone Book

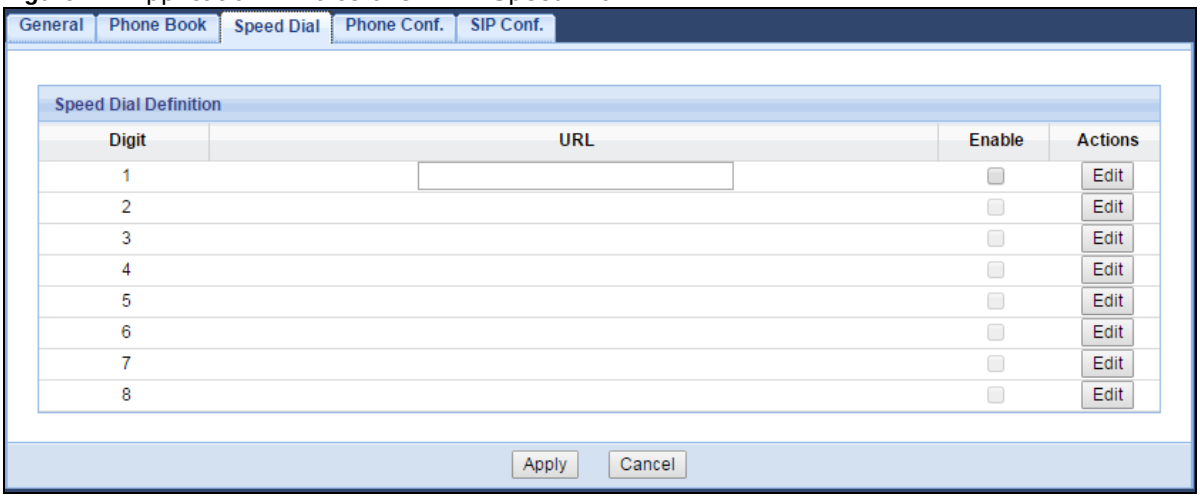
| LABEL | DESCRIPTION |
|---|---|
| # | This field displays the index number of the contact. |
| Name | This field displays the name of the contact.<br>Click **Edit** and enter the descriptive name of the contact. You can enter up to 40 characters for a contact. |
| Phone | This field displays the phone number of the contact.<br>Click **Edit** and enter the phone number or SIP number of the contact. |
| Enable | Select this option to activate this entry. |
| Actions | Click the **Edit** icon to create a new contact or change the contact name or phone number. |
| Previous | Click **Previous** to return to the previous page. |
| Next | Click **Next** to go to the next page. |
| Apply | Click this to save your changes and to apply them to the LTE3311. |

# 17.5 Speed Dial Screen

Use this screen to add, edit, or remove speed-dial numbers for outgoing calls. Speed dial provides shortcuts for dialing frequently-used (VoIP) phone numbers. You also have to create speed-dial entries if you want to call SIP numbers that contain letters. Once you have configured a speed dial rule, you can use a shortcut (the speed dial number and pound key, 1# for example) on your phone's keypad to call the phone number.

In peer-to-peer calls, you call another VoIP device directly without going through a VoIP service provider's SIP server. Enter the callee's IP address or domain name. The LTE3311 sends SIP INVITE requests to the peer VoIP device when you use the speed dial entry.

**Figure 77** Application > Voice over IP > Speed Dial



The following table describes the labels in this screen.

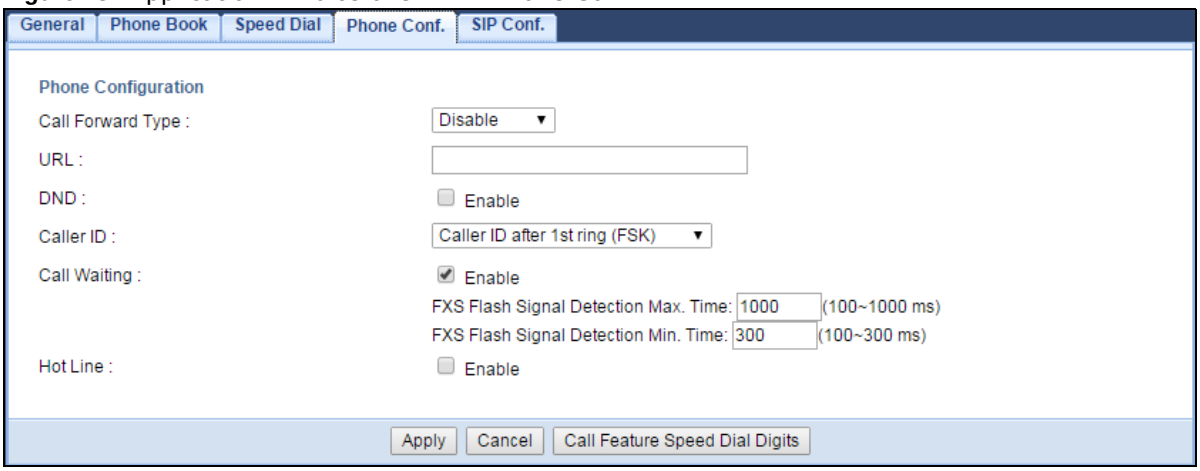
**Table 54** Application > Voice over IP > Speed Dial

| LABEL | DESCRIPTION |
|---|---|
| # | This field displays the speed-dial number you should dial to use this entry. |
| URL | This field displays the SIP number the LTE3311 calls when you dial the speed-dial number.<br>Click **Edit** and enter the SIP number you want the LTE3311 to call when you dial the speed-dial number. If you want to use a different SIP server or if you want to make a peer-to-peer call, enter the IP address or domain name of the SIP server or the other party. |
| Enable | Select this option to activate this entry. |
| Actions | Click the **Edit** icon to create a new entry or modify the existing entry. |
| Apply | Click this to save your changes and to apply them to the LTE3311. |
| Cancel | Click this to set every field in this screen to its last-saved value. |

# 17.6 Phone Conf. Screen

Use this screen to configure call features. To access this screen, click **Application > Voice over IP > Phone Conf.**.

**Figure 78** Application > Voice over IP > Phone Conf.



The following table describes the labels in this screen.

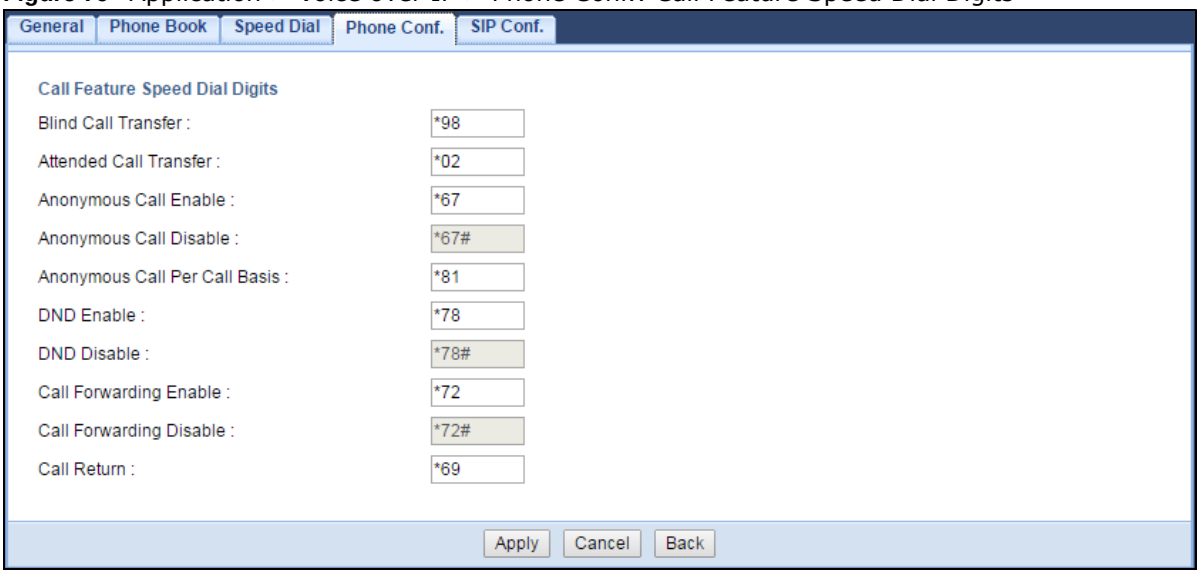
**Table 55** Application > Voice over IP > Phone Conf.

| LABEL | DESCRIPTION |
|---|---|
| Call Forward Type | Select **Disable** if you do not want the LTE3311 to forward any incoming calls.<br>Select **Always** if you want the LTE3311 to forward all incoming calls to the specified phone number.<br>Select **Busy** if you want the LTE3311 to forward incoming calls to the specified phone number if the phone port is busy.<br>Select **No Answer** if you want the LTE3311 to forward incoming calls to the specified phone number if the call is unanswered. |
| URL | Specify the phone number to which the LTE3311 forwards an incoming call. |
| DND | Select **Enable** to set your phone to not ring when someone calls you. |
| Caller ID | Select **Caller ID after 1st ring (FSK)** or **Caller ID after 1st ring (FSK-JP)** if you want to send identification when you make VoIP phone calls. Select **Don't show Caller ID** if you do not want to send identification. |
| Call Waiting | Select **Enable** to place a call on hold while you answer another incoming call on the same telephone number. |
| FXS Flash Signal Detection Max. Time | Enter the maximum time (in milliseconds) to detect a hook flash signal from the connected analog phone. This specifies the time that the LTE3311 waits before rejecting the second call if you do not answer it.<br>If the flash signal is longer than the maximum time, the LTE3311 rejects the second call. |
| FXS Flash Signal Detection Min. Time | Enter the minimum time (in milliseconds) to detect a hook flash signal from the connected analog phone.<br>This specifies the time that the LTE3311 waits before rejecting the second call if you do not answer it. If the flash signal is shorter than the minimum time, the LTE3311 rejects the second call. |
| Hot Line | Select **Enable** to have the LTE3311 dial the specified hot line number after you pick up the telephone and do not press any keys on the keypad for a period of time. |
| Hot Line Number | Enter the number of the hot line that you want the LTE3311 to dial. |
| Waiting Time before Starting Hot Line | Enter a number of seconds that the LTE3311 waits before dialing the hot line number if you pick up the telephone and do not press any keys on the keypad. |
| Apply | Click this to save your changes and to apply them to the LTE3311. |
| Cancel | Click this to set every field in this screen to its last-saved value. |
| Call Feature Speed Dial Digits | Click this to open a screen where you can show and configure shows the key combinations you can enter on your phone's keypad to use certain features. See Section 17.6.1 on page 122. |

## 17.6.1 Call Feature Speed Dial Digits

Use this screen to view and change the key combinations you can enter on your phone's keypad to use certain features. To access this screen, click **Application > Voice over IP > Phone Conf.** and then click the **Call Feature Speed Dial Digits** button.

**Figure 79** Application > Voice over IP > Phone Conf.: Call Feature Speed Dial Digits




The following table describes the labels in this screen.

**Table 56** Application > Voice over IP > Phone Conf.: Call Feature Speed Dial Digits

| LABEL | DESCRIPTION |
|---|---|
| Blind Call Transfer | Transfer an incoming call (that you have answered) to another phone, without talking to him/her. |
| Attended Call Transfer | Call the number to which you want to transfer a call, speak with him/her and then transfer the call. |
| Anonymous Call Enable | Hide your name and phone number for the call. |
| Anonymous Call Disable | Display your name and phone number for the call. |
| Anonymous Call Per Call Basis | Disable caller ID on a per call basis. |
| DND Enable | Set your phone to not ring when someone calls you. |
| DND Disable | Allow your phone to ring when someone calls you. |
| Call Forwarding Enable | Allow the LTE3311 to forward all incoming calls to the specified phone number. |
| Call Forwarding Disable | Set the LTE3311 to not forward any incoming calls. |
| Call Return | Place a call to the last person who called you. |
| Apply | Click this to save your changes and to apply them to the LTE3311. |
| Cancel | Click this to set every field in this screen to its last-saved value. |
| Back | Click this to return to the previous screen. |

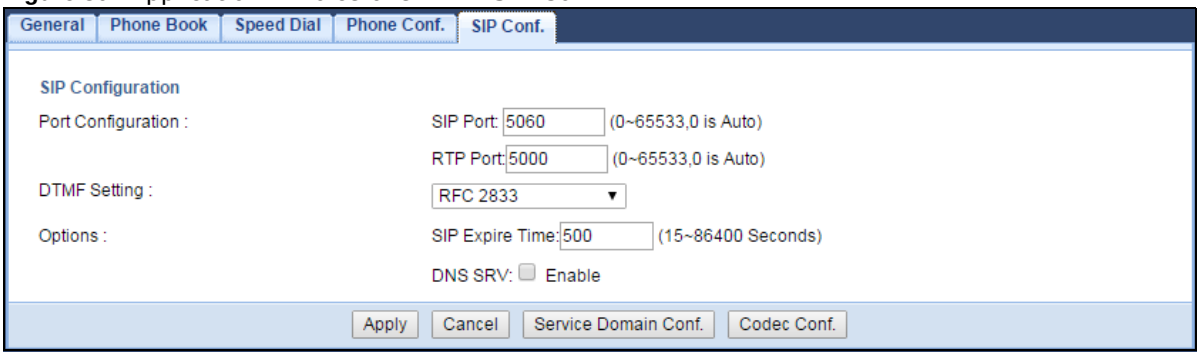
# 17.7 SIP Configuration Screen

The LTE3311 uses a SIP account to make outgoing VoIP calls and check if an incoming call's destination number matches your SIP account's SIP number. In order to make or receive a VoIP

call, you need to enable and configure a SIP account. The SIP account contains information that allows your LTE3311 to connect to your VoIP service provider.

Use this screen to maintain information about your SIP account, and configure the SIP server information. To access this screen, click **Application > Voice over IP > SIP Conf.**.

**Figure 80** Application > Voice over IP > SIP Conf.




The following table describes the labels in this screen.

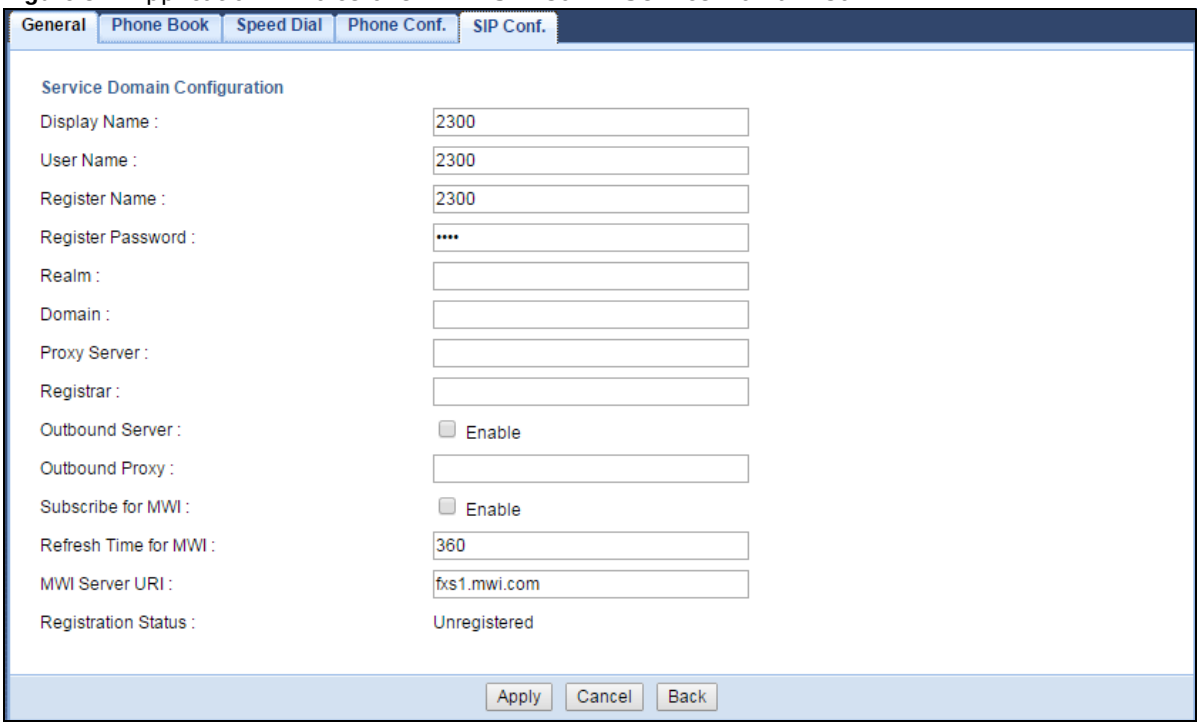
**Table 57** Application > Voice over IP > SIP Conf.

| LABEL | DESCRIPTION |
|---|---|
| Port Configuration | |
| SIP Port | Enter the SIP server's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value. |
| RTP Port | Enter the listening port number(s) for RTP traffic, if your VoIP service provider gave you this information. Otherwise, keep the default values. |
| DTMF Setting | Control how the LTE3311 handles the tones that your telephone makes when you push its buttons. You should use the same mode your VoIP service provider uses.<br>**RFC2833** - send the DTMF tones in RTP packets.<br>**Inband DTMF** - send the DTMF tones in the voice data stream. This method works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729 and G.726) can distort the tones.<br>**Send DTMF SIP Info** - send the DTMF tones in SIP messages. |
| Options | |
| SIP Expire Time | Enter the number of seconds the LTE3311 lets a SIP session remain idle (without traffic) before it automatically disconnects the session. |
| DNS SRV | Select **Enable** to have the LTE3311 use DNS procedures to resolve the SIP domain and find the SIP server's IP address, port number and supported transport protocol(s).<br>The LTE3311 first uses DNS Name Authority Pointer (NAPTR) records to determine the transport protocols supported by the SIP server. It then performs DNS Service (SRV) query to determine the port number for the protocol. The LTE3311 resolves the SIP server's IP address by a standard DNS address record lookup. |
| Apply | Click this to save your changes and to apply them to the LTE3311. |
| Cancel | Click this to set every field in this screen to its last-saved value. |
| Service Domain Conf. | Click this to open a screen where you can maintain information about the SIP service domain. See Section 17.7.1 on page 125. |
| Codec Conf. | Click this to open a screen where you can configure codec priority. See Section 17.7.2 on page 126. |

## 17.7.1 Service Domain Configuration

Use this screen to maintain information about the SIP service domain. To access this screen, click **Application > Voice over IP > SIP Conf.** and then click the **Service Domain Conf.** button.

**Figure 81** Application > Voice over IP > SIP Conf.: Service Domain Conf.




The following table describes the labels in this screen.

**Table 58** Application > Voice over IP > SIP Conf.: Service Domain Conf.

| LABEL | DESCRIPTION |
|---|---|
| Display Name | |
| User Name | Enter your SIP number. In the full SIP URI, this is the part before the @ symbol. You can use up to 127 printable ASCII characters. |
| Register Name | Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII characters. |
| Register Password | Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII Extended set characters. |
| Realm | Enter the SIP authentication realm. |
| Domain | Enter the SIP service domain name. In the full SIP URI, this is the part after the @ symbol. You can use up to 127 printable ASCII Extended set characters. |
| Proxy Server | Enter the IP address or domain name of the SIP server provided by your VoIP service provider. You can use up to 95 printable ASCII characters. It does not matter whether the SIP server is a proxy, redirect or register server. |
| Registrar | Enter the IP address or domain name of the SIP register server, if your VoIP service provider gave you one. Otherwise, enter the same address you entered in the **Proxy Server** field. You can use up to 95 printable ASCII characters. |

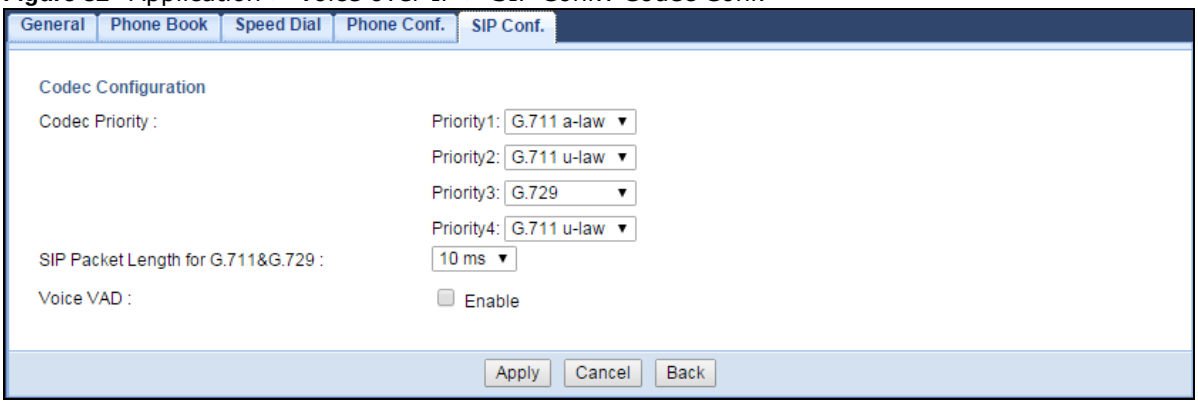
**Table 58** Application > Voice over IP > SIP Conf.: Service Domain Conf. (continued)

| LABEL | DESCRIPTION |
|---|---|
| Outbound Server | Select **Enable** if your VoIP service provider has a SIP outbound server to handle voice calls. This allows the LTE3311 to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off any SIP ALG on a NAT router in front of the LTE3311 to keep it from re-translating the IP address (since this is already handled by the outbound proxy server). |
| Outbound Proxy | Enter the IP address or domain name of the SIP outbound proxy server. |
| Subscribe for MWI | Select **Enable** if you want to hear a waiting (beeping) dial tone on your phone when you have at least one voice message. Your VoIP service provider must support the MWI (Message Waiting Indication) feature. |
| Refresh Time for MWI | Enter the number of seconds the SIP server should provide the message waiting service each time the LTE3311 subscribes to the service. Before this time passes, the LTE3311 automatically subscribes again. |
| MWI Server URI | Enter the domain name of the MWI server. |
| Registration Status | This shows the current registration status of the SIP account. |
| Apply | Click this to save your changes and to apply them to the LTE3311. |
| Cancel | Click this to set every field in this screen to its last-saved value. |
| Back | Click this to return to the previous screen. |

## 17.7.2 Codec Configuration

Use this screen to maintain information about your SIP account, and configure the SIP server information. To access this screen, click **Application > Voice over IP > SIP Conf.** and then click the **Codec Conf.** button.

**Figure 82** Application > Voice over IP > SIP Conf.: Codec Conf.



The following table describes the labels in this screen.

**Table 59** Application > Voice over IP > SIP Conf.: Codec Conf.

| LABEL | DESCRIPTION |
|---|---|
| Codec Priority | Select the type of voice coder/decoder (codec) that you want the LTE3311 to use.<br>G.711 provides high voice quality but requires more bandwidth (64 kbps). G.711 is the default codec used by phone companies and digital handsets.<br>• **G.711a-law** is typically used in Europe.<br>• **G.711u-law** is typically used in North America and Japan.<br>**G.726-32** operates at **32** kbps.<br>**G.729** provides good sound quality and reduces the required bandwidth to 8 kbps.<br>The LTE3311 must use the same codec as the peer. When two SIP devices start a SIP session, they must agree on a codec. |
| Priority1 | Select the LTE3311's first choice for voice coder/decoder. |
| Priority2 | Select the LTE3311's second choice for voice coder/decoder. |
| Priority3 | Select the LTE3311's third choice for voice coder/decoder. |
| Priority4 | Select the LTE3311's fourth choice for voice coder/decoder. |
| SIP Packet Length for G.711&G.729 | Select to change the voice payload size for VoIP packets. If you increase the voice payload size, the bandwidth will be reduced. |
| Voice VAD | Select **Enable** if the LTE3311 should stop transmitting when you are not speaking. This reduces the bandwidth the LTE3311 uses. |
| Apply | Click this to save your changes and to apply them to the LTE3311. |
| Cancel | Click this to set every field in this screen to its last-saved value. |
| Back | Click this to return to the previous screen. |

# 17.8 Technical Reference

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

## VoIP

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

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

## SIP

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

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

## SIP Identities

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

## SIP Number

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

## SIP Service Domain

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

## SIP Registration

Each LTE3311 is an individual SIP User Agent (UA). To provide voice service, it has a public IP address for SIP and RTP protocols to communicate with other servers.

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

Registration is initiated by the User Agent Client (UAC) running in the VoIP gateway (the LTE3311). The gateway must be configured with information letting it know where to send the REGISTER message, as well as the relevant user and authorization data.

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

The LTE3311 attempts to register all enabled subscriber ports when it is switched on. When you enable a subscriber port that was previously disabled, the LTE3311 attempts to register the port immediately.

## Authorization Requirements

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

## SIP Servers

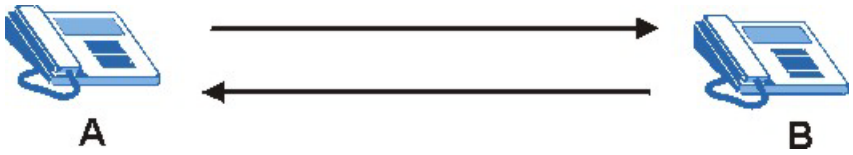
SIP is a client-server protocol. A SIP client is an application program or device that sends SIP requests. A SIP server responds to the SIP requests.

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

## SIP User Agent

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

**Figure 83** SIP User Agent




## SIP Proxy Server

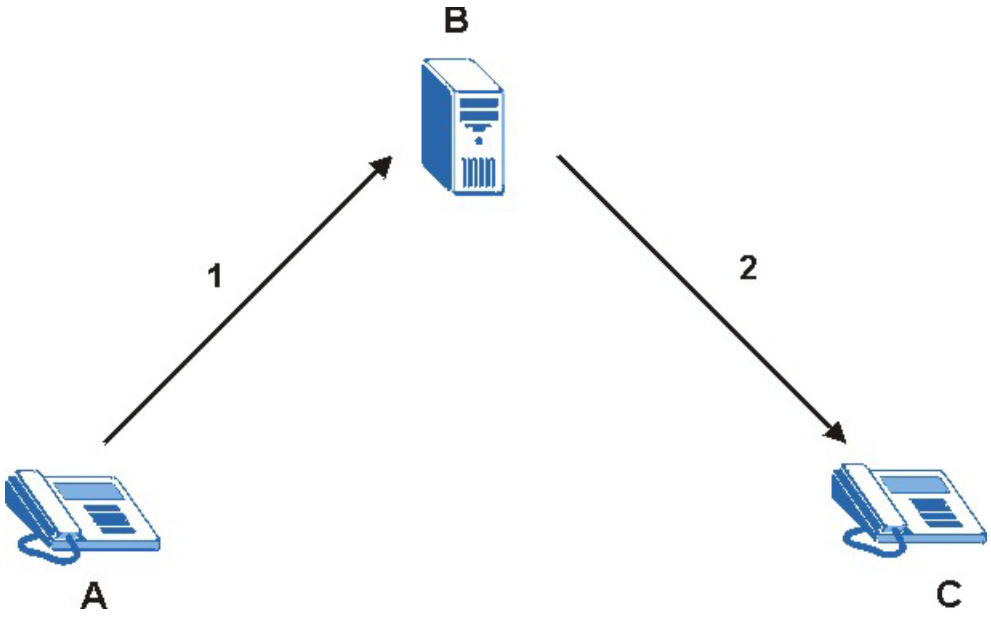
A SIP proxy server receives requests from clients and forwards them to another server.

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

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

2 The SIP proxy server forwards the call invitation to **C**.

**Figure 84** SIP Proxy Server



## SIP Redirect Server

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

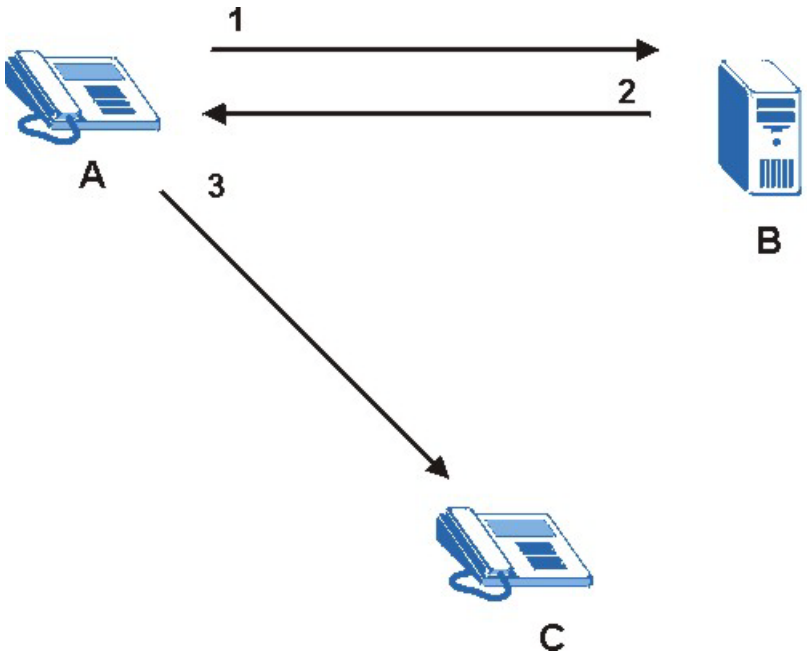
In the following example, you want to use client device **A** to call someone who is using client device **C**.

1 Client device **A** sends a call invitation for **C** to the SIP redirect server (**B**).

2 The SIP redirect server sends the invitation back to **A** with **C**'s IP address (or domain name).

3 Client device **A** then sends the call invitation to client device **C**.

**Figure 85** SIP Redirect Server




## SIP Register Server

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

## RTP

When you make a VoIP call using SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

## Pulse Code Modulation

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

## SIP Call Progression

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

**Table 60** SIP Call Progression

| A | | B |
|---|---|---|
| 1. INVITE | → | |
| | ← | 2. Ringing |
| | ← | 3. OK |
| 4. ACK | → | |
| | 5.Dialogue (voice traffic) | |
| 6. BYE | → | |
| | ← | 7. OK |

1 **A** sends a SIP INVITE request to **B**. This message is an invitation for **B** to participate in a SIP telephone call.

2 **B** sends a response indicating that the telephone is ringing.

3 **B** sends an OK response after the call is answered.

4 **A** then sends an ACK message to acknowledge that **B** has answered the call.

5 Now **A** and **B** exchange voice media (talk).

6 After talking, **A** hangs up and sends a BYE request.

7 **B** replies with an OK response confirming receipt of the BYE request and the call is terminated.

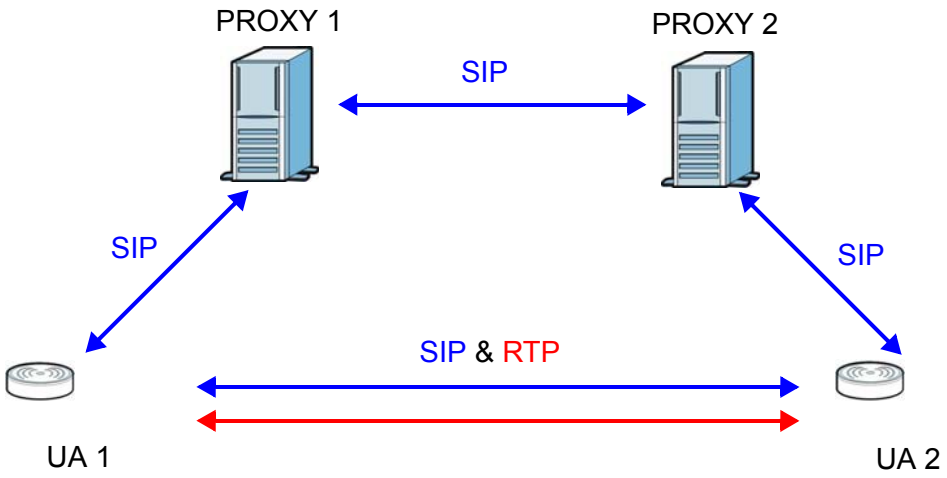
## SIP Call Progression Through Proxy Servers

Usually, the SIP UAC sets up a phone call by sending a request to the SIP proxy server. Then, the proxy server looks up the destination to which the call should be forwarded (according to the URI requested by the SIP UAC). The request may be forwarded to more than one proxy server before arriving at its destination.

The response to the request goes to all the proxy servers through which the request passed, in reverse sequence. Once the session is set up, session traffic is sent between the UAs directly, bypassing all the proxy servers in between.

The following figure shows the SIP and session traffic flow between the user agents (**UA 1** and **UA 2**) and the proxy servers (this example shows two proxy servers, **PROXY 1** and **PROXY 2**).

**Figure 86** SIP Call Through Proxy Servers




The following table shows the SIP call progression.

**Table 61** SIP Call Progression

| UA 1 | | PROXY 1 | | PROXY 2 | | UA 2 |
|---|---|---|---|---|---|---|
| Invite | → | | | | | |
| | | Invite | → | | | |
| | | 100 Trying | ← | | | |
| | | | | Invite | → | |
| | | | | 100 Trying | ← | |
| | | | | | | 180 Ringing ← |
| | | | | 180 Ringing | ← | |
| | | 180 Ringing | ← | | | |
| | | | | | | 200 OK ← |
| | | | | 200 OK | ← | |
| | | 200 OK | ← | | | |
| ACK | → | | | | | |
| RTP | ↔ | | | | | RTP |
| | | | | | | BYE ← |
| 200 OK | → | | | | | |

1 **User Agent 1** sends a SIP INVITE request to **Proxy 1**. This message is an invitation to **User Agent 2** to participate in a SIP telephone call. **Proxy 1** sends a response indicating that it is trying to complete the request.

2 **Proxy 1** sends a SIP INVITE request to **Proxy 2**. **Proxy 2** sends a response indicating that it is trying to complete the request.

3 **Proxy 2** sends a SIP INVITE request to **User Agent 2**.

4 **User Agent 2** sends a response back to **Proxy 2** indicating that the phone is ringing. The response is relayed back to **User Agent 1** via **Proxy 1**.

5 **User Agent 2** sends an OK response to **Proxy 2** after the call is answered. This is also relayed back to **User Agent 1** via **Proxy 1**.

6 **User Agent 1** and **User Agent 2** exchange RTP packets containing voice data directly, without involving the proxies.

7 When **User Agent 2** hangs up, he sends a BYE request.

8 **User Agent 1** replies with an OK response confirming receipt of the BYE request, and the call is terminated.

## Voice Coding

A codec (coder/decoder) codes analog voice signals into digital signals and decodes the digital signals back into analog voice signals. The LTE3311 supports the following codecs.

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

## Voice Activity Detection/Silence Suppression

Voice Activity Detection (VAD) detects whether or not speech is present. This lets the LTE3311 reduce the bandwidth that a call uses by not transmitting "silent packets" when you are not speaking.

## Comfort Noise Generation

When using VAD, the LTE3311 generates comfort noise when the other party is not speaking. The comfort noise lets you know that the line is still connected as total silence could easily be mistaken for a lost connection.

## Echo Cancellation

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

## MWI (Message Waiting Indication)

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

## Custom Tones (IVR)

IVR (Interactive Voice Response) is a feature that allows you to use your telephone to interact with the LTE3311. The LTE3311 allows you to record custom tones for the **Early Media** and **Music On Hold** functions. The same recordings apply to both the caller ringing and on hold tones.

**Table 62** Custom Tones Details

| LABEL | DESCRIPTION |
|---|---|
| Total Time for All Tones | 900 seconds for all custom tones combined |
| Maximum Time per Individual Tone | 180 seconds |
| Total Number of Tones Recordable | 5<br>You can record up to 5 different custom tones but the total time must be 900 seconds or less. |

## Recording Custom Tones

Use the following steps if you would like to create new tones or change your tones:

1. Pick up the phone and press "****" on your phone's keypad and wait for the message that says you are in the configuration menu.
2. Press a number from 1101~1105 on your phone followed by the "#" key.
3. Play your desired music or voice recording into the receiver's mouthpiece. Press the "#" key.
4. You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

## Listening to Custom Tones

Do the following to listen to a custom tone:

1. Pick up the phone and press "****" on your phone's keypad and wait for the message that says you are in the configuration menu.
2. Press a number from 1201~1208 followed by the "#" key to listen to the tone.
3. You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

## Deleting Custom Tones

Do the following to delete a custom tone:

1. Pick up the phone and press "****" on your phone's keypad and wait for the message that says you are in the configuration menu.
2. Press a number from 1301~1308 followed by the "#" key to delete the tone of your choice. Press 14 followed by the "#" key if you wish to clear all your custom tones.

You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

## 17.8.1 Quality of Service (QoS)

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

### Type of Service (ToS)

Network traffic can be classified by setting the ToS (Type of Service) values at the data source (for example, at the LTE3311) so a server can decide the best method of delivery, that is the least cost, fastest route and so on.

### DiffServ

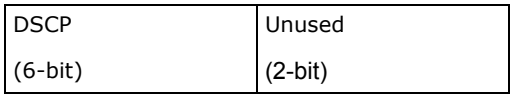
DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCP) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.[3]

### DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

**Figure 87** DiffServ: Differentiated Service Field




The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

3. The LTE3311 does not support DiffServ at the time of writing.

# 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 LTE3311 supports Circuit Switched FallBack (CSFB) to deliver/receive circuit-switched voice calls and 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 LTE3311, but not both at the same time.

### 18.1.1 What You Can Do in this Chapter

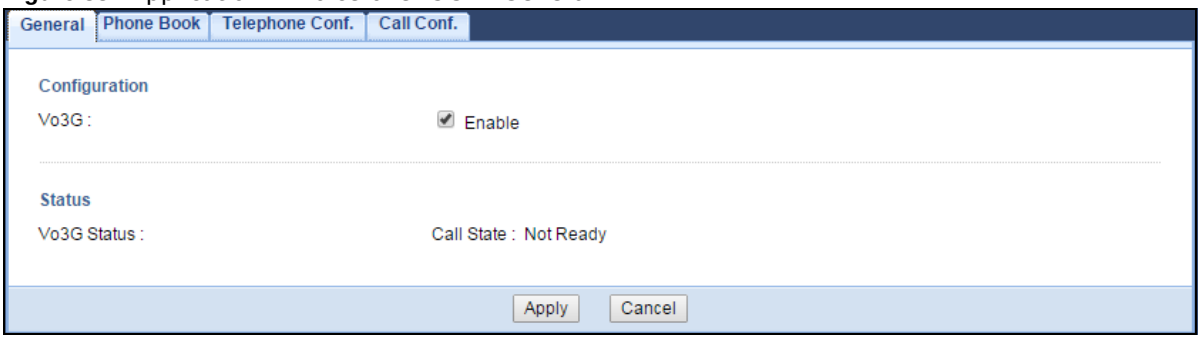
These screens allow you to configure your LTE3311 to make phone calls over the Internet and your regular phone line, and to set up the phone you connect to the LTE3311.

- Use the **General** screen to enable Vo3G on the LTE3311 (Section 18.2 on page 136).
- Use the **Phone Book** screen to manage your contact names and phone numbers (Section 18.3 on page 137).
- Use the **Telephone Conf.** screen to configure call features (Section 18.4 on page 138).
- Use the **Call Conf.** screen to maintain rules for handling incoming calls (Section 18.5 on page 139).

## 18.2 Vo3G General Screen

Use this screen to enable Vo3G on the LTE3311. To access this screen, click **Application > Voice over 3G > General**.

**Figure 88** Application > Voice over 3G > General



The following table describes the labels in this screen.

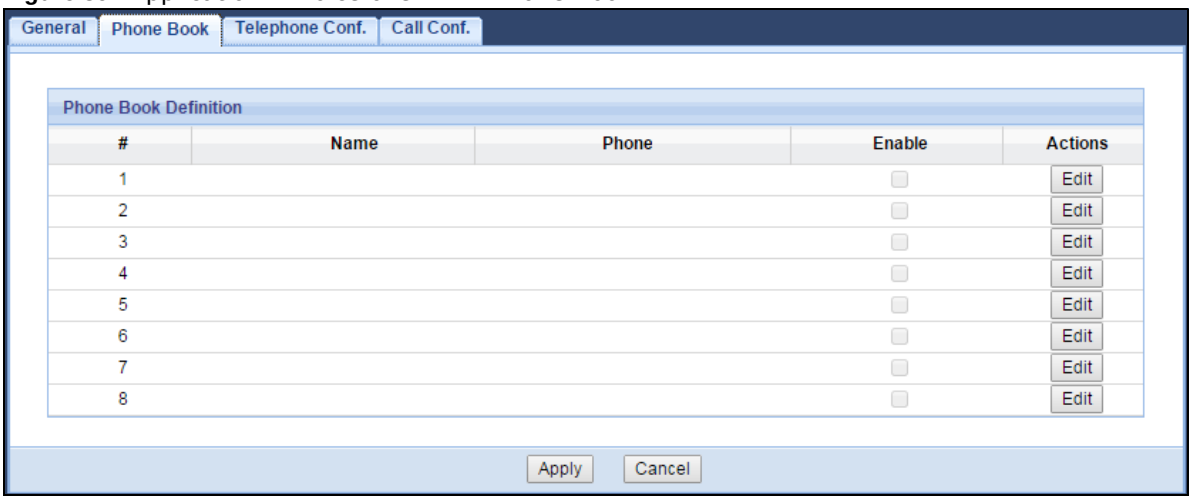
**Table 63** Application > Voice over 3G > General

| LABEL | DESCRIPTION |
|---|---|
| Vo3G | Select **Enable** to activate Vo3G on the LTE3311. |
| Vo3G Status | This shows the current state of the phone call.<br>• **ready**: Voice over 3G (Vo3G) is enabled and the 3G connection is up.<br>• **not ready**: Voice over 3G (Vo3G) is disabled and the 3G connection is down.<br>• **busy**: There is a Vo3G call in progress or the callee's line is busy.<br>• **ringing**: The phone is ringing for an incoming Vo3G call.<br>• **dialing**: The callee's phone is ringing.<br>• **off hook**: The callee hung up or your phone was left off the hook.<br>**N/A** means Voice over 3G (Vo3G) is disabled. |
| Apply | Click **Apply** to save the settings. |
| Cancel | Click **Cancel** to start configuring this screen again. |

# 18.3 Phone Book Screen

Use this screen to manage your contact names and phone numbers. To access this screen, click **Application > Voice over 3G > Phone Book**.

**Figure 89** Application > Voice over IP > Phone Book




The following table describes the labels in this screen.

**Table 64** Application > Voice over 3G > Phone Book

| LABEL | DESCRIPTION |
|---|---|
| # | This field displays the index number of the contact. |
| Name | This field displays the name of the contact.<br>Click **Edit** and enter the descriptive name of the contact. You can enter up to 40 characters for a contact. |

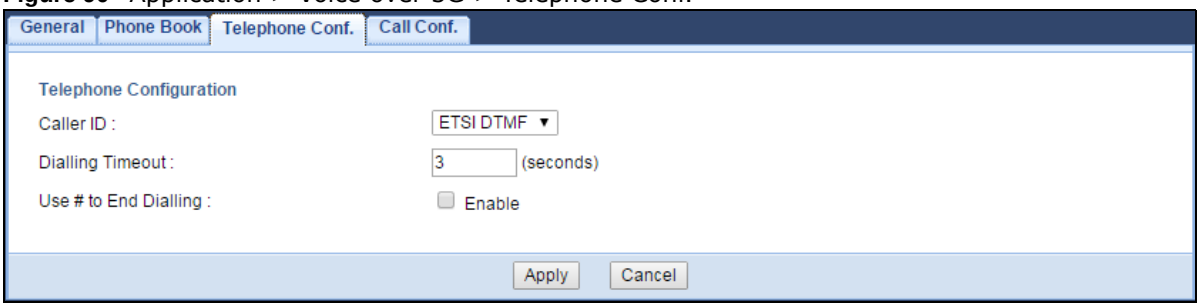
**Table 64** Application > Voice over 3G > Phone Book

| LABEL | DESCRIPTION |
|---|---|
| Phone | This field displays the mobile identification number of the contact.<br>Click **Edit** and enter the 10-digit mobile subscription identification number (MSIN) used to identify the contact. |
| Enable | Select this option to activate this entry. |
| Actions | Click the **Edit** icon to create a new contact or change the contact name or phone number. |
| Apply | Click this to save your changes and to apply them to the LTE3311. |
| Cancel | Click this to set every field in this screen to its last-saved value. |

# 18.4 Telephone Conf. Screen

Use this screen to configure call features. To access this screen, click **Application > Voice over 3G > Telephone Conf.**.

**Figure 90** Application > Voice over 3G > Telephone Conf.




The following table describes the labels in this screen.

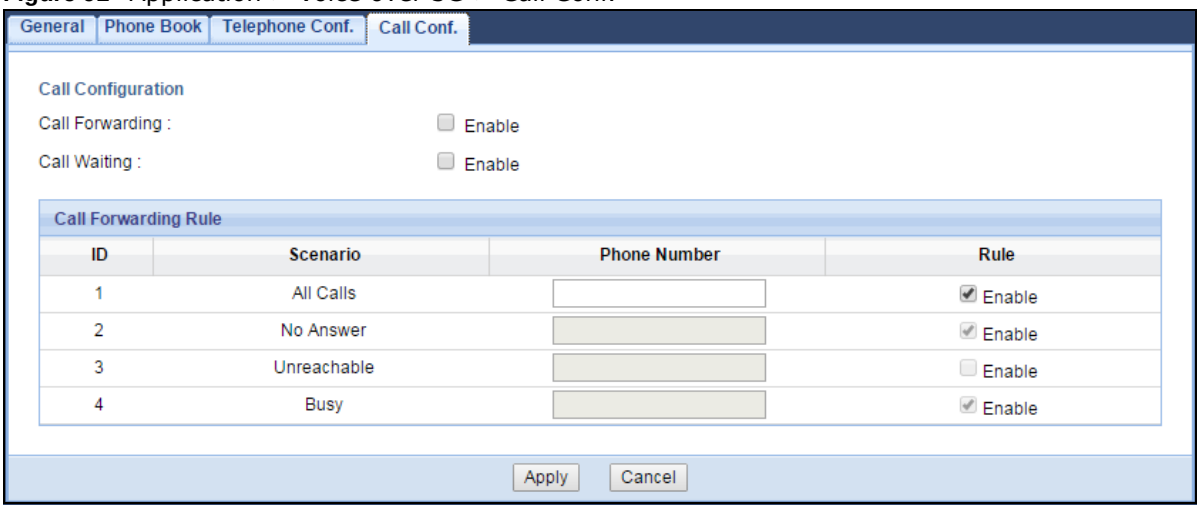
**Table 65** Application > Voice over 3G > Telephone Conf.

| LABEL | DESCRIPTION |
|---|---|
| Caller ID | This shows the caller ID standard (**ETSI DTMF**) used to send identification when you make Vo3G phone calls. |
| Dialling Timeout | Enter the number of seconds the LTE3311 should wait after you stop dialing numbers before it makes the phone call. The value depends on how quickly you dial phone numbers.<br>If you select **Enable** in the **Use # to End Dialling** field, you can press the pound key (#) to tell the LTE3311 to make the phone call immediately, regardless of this setting. |
| Use # to End Dialling | Select **Enable** if you want to use the pound key (#) to tell the LTE3311 to make the phone call immediately, instead of waiting the number of seconds you selected in the **Dialling Timeout** field.<br>If you select **Enable**, dial the phone number, and then press the pound key. The LTE3311 makes the call immediately, instead of waiting. You can still wait, if you want. |
| Apply | Click this to save your changes and to apply them to the LTE3311. |
| Cancel | Click this to set every field in this screen to its last-saved value. |

# 18.5 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 91** Application > Voice over 3G > Call Conf.




The following table describes the labels in this screen.

**Table 66** Application > Voice over 3G > Call Conf.

| LABEL | DESCRIPTION |
|---|---|
| Call Forwarding | Select **Enable** to forward incoming calls according to the call forwarding rules. Clear the check box if you do not want the LTE3311 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. |
| ID | This is the index number of the call forwarding rule. |
| Scenario | This shows the situations in which you want to forward incoming calls.<br>**All Calls**: the LTE3311 forwards all incoming calls to the specified phone number.<br>**No Answer**: the LTE3311 forwards incoming calls to the specified phone number if the call is unanswered.<br>**Unreachable**: the LTE3311 forwards incoming calls to the specified phone number if the phone is turned off or lost its signal.<br>**Busy**: the LTE3311 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.<br>Note: If you enable the **All Calls** rule, other rules are not configurable/applicable. |
| Apply | Click this to save your changes and to apply them to the LTE3311. |
| Cancel | Click this to set every field in this screen to its last-saved value. |

# 19

# SMS

## 19.1 Overview

SMS (Short Message Service) allows you to send and view the text messages that the LTE3311 received from mobile devices or the service provider.

When the SMS box is full the LTE3311 will begin to delete older entries as it adds new ones.

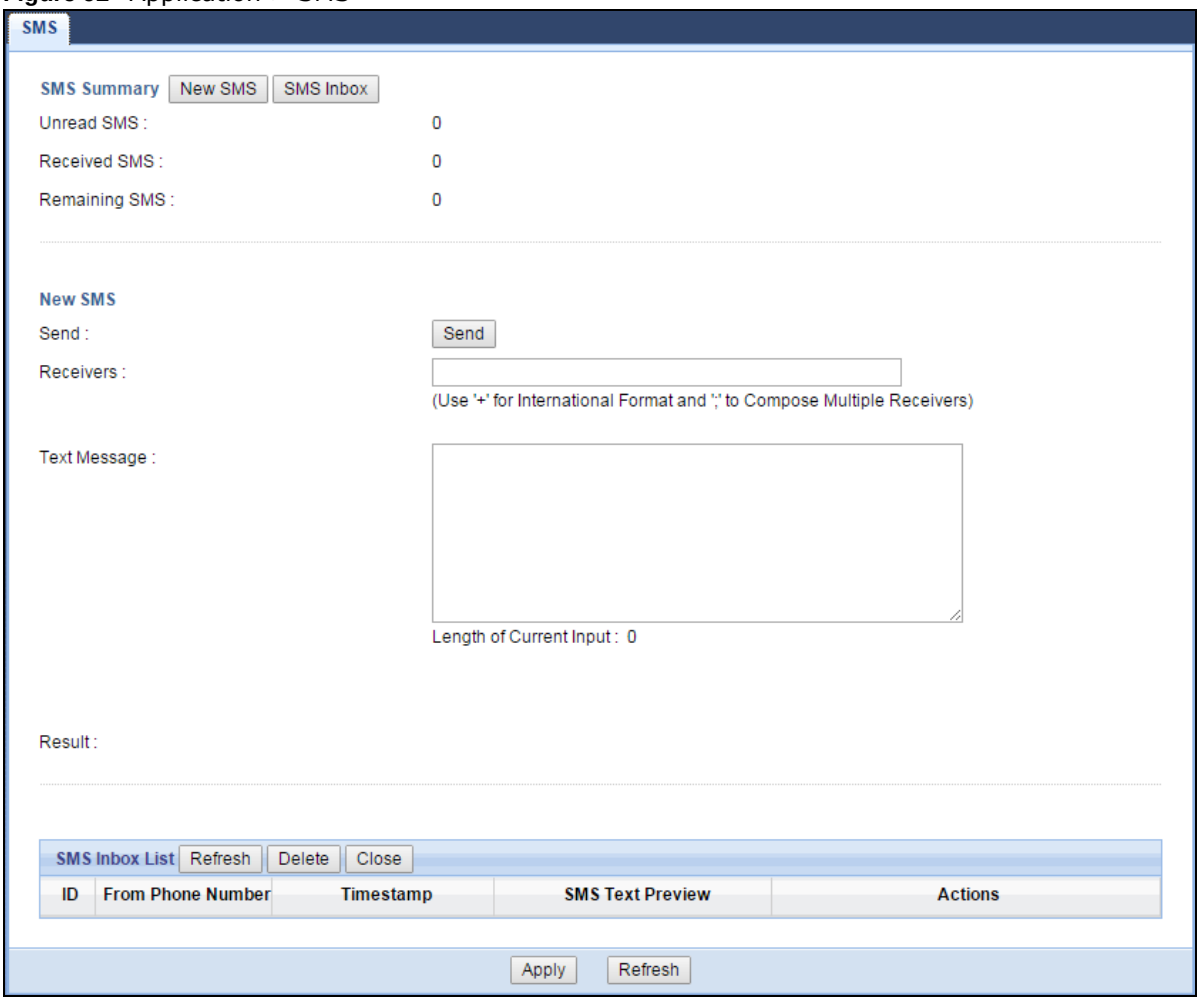
### 19.1.1 What You Can Do in this Chapter

- Use the **SMS** screen to send new messages and view messages received on the LTE3311 (Section 19.2 on page 140).

## 19.2 SMS Screen

Use this screen to send text messages using the LTE3311 and view messages received. To access this screen, click **Application > SMS**.

**Figure 92** Application > SMS




The following table describes the labels in this screen.

**Table 67** Application > SMS

| LABEL | DESCRIPTION |
|---|---|
| SMS Summary | Click **New SMS** to display the **New SMS** section.<br>Click **SMS Inbox** to display only the **SMS Inbox List**. |
| Unread SMS | This shows the number of unread text messages in the SMS in-box. |
| Received SMS | This shows the number of text messages that the LTE3311 received. |
| Remaining SMS | This shows the number of text messages that are to be sent. |
| New SMS | |
| Send | Click this button to send the new message. |
| Receivers | Enter the phone number to which you want to send a text message. |
| Text Message | Enter the message content. You can type up to 160 characters in one message. If the message exceeds 160 characters, more than one SMS will be sent. The maximum number of SMS that can be sent is 20 (1400 characters total). |
| Result | This shows whether the message is sent successfully. |
| SMS Inbox List | |
| Refresh | Click this button to update the list. |

**Table 67** Application > SMS (continued)

| LABEL | DESCRIPTION |
|---|---|
| Delete | |
| 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. |
| Apply | Click this button to save your changes to the LTE3311. |
| Refresh | Click this button to update the screen. |

# 20 NAS

## 20.1 Overview

This chapter shows you how to configure file sharing.

### 20.1.1 What You Can Do

- Use the **File Sharing** screen to allow file sharing via the LTE3311 using Windows Explorer, the workgroup name (Section 20.2.1 on page 144).
- Use the **FTP** screen to allow file sharing via the LTE3311 using FTP (Section 20.3 on page 145).

### 20.1.2 What You Need To Know

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

#### Workgroup name

This is the name given to a set of computers that are connected on a network and share resources such as a printer or files. Windows automatically assigns the workgroup name when you set up a network.

#### Samba

SMB is a client-server protocol used by Microsoft Windows systems for sharing files, printers, and so on.

Samba is a free SMB server that runs on most Unix and Unix-like systems. It provides an implementation of an SMB client and server for use with non-Microsoft operating systems.

#### File Transfer Protocol

This is a method of transferring data from one computer to another over a network such as the Internet.

### 20.1.3 Before You Begin

Make sure the LTE3311 is connected to your network and turned on.

1 Connect the USB device to one of the LTE3311's USB ports.

2 The LTE3311 detects the USB device and makes its contents available for browsing. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.

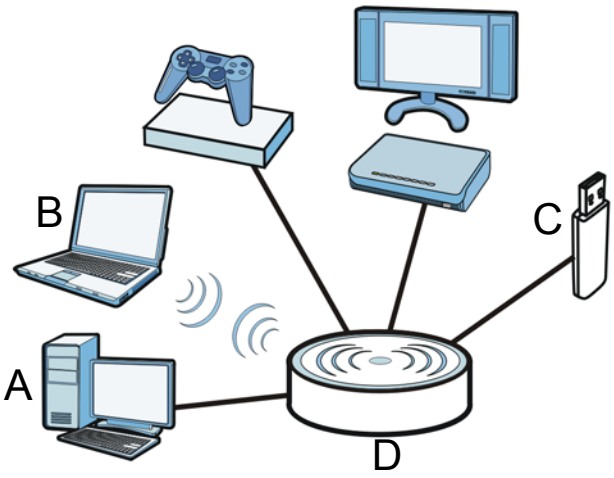
Note: If your USB device cannot be detected by the LTE3311, see the troubleshooting for suggestions.

# 20.2 File Sharing

You can also share files on a USB memory stick or hard drive connected to your LTE3311 with users on your network.

The following figure is an overview of the LTE3311's file-sharing server feature. Computers **A** and **B** can access files on a USB device (**C**) which is connected to the LTE3311 (**D**).

**Figure 93** File Sharing Overview



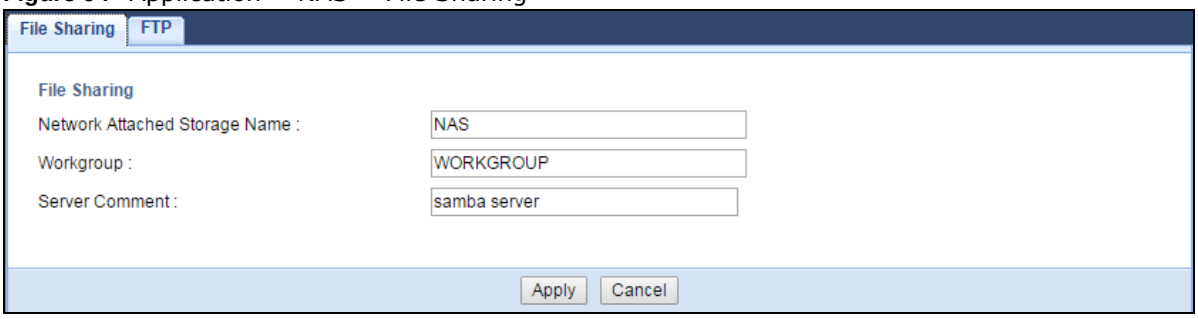

Note: The read and write performance may be affected by amount of file-sharing traffic on your network, type of connected USB device and your USB version (1.1 or 2.0).

## 20.2.1 Filing Sharing Screen

Use this screen to set up file-sharing via the LTE3311 using Windows Explorer or the workgroup name. You can also configure the workgroup name.

Click **Applications > NAS > File Sharing** to open the following screen.

**Figure 94** Application > NAS > File Sharing




The following table describes the labels in this screen.

**Table 68** Application > NAS > File Sharing

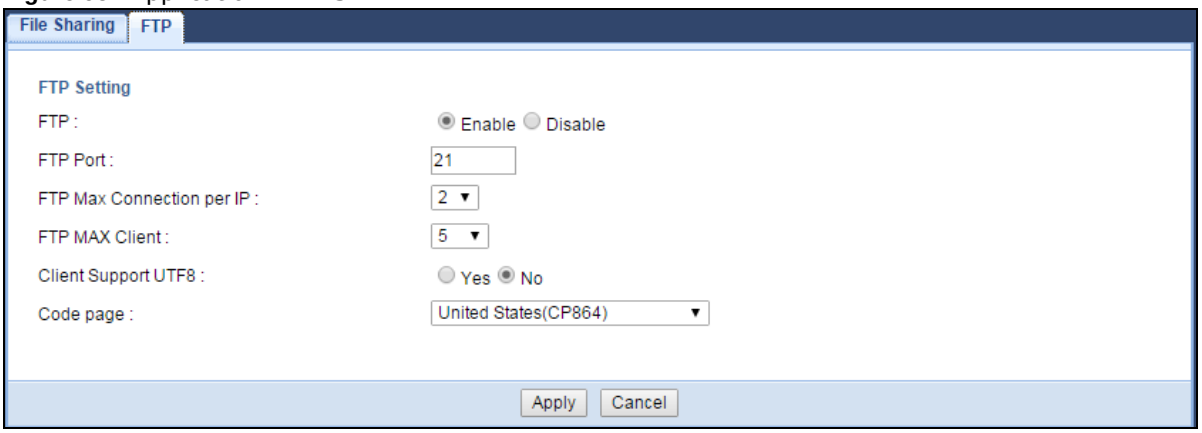
| LABEL | DESCRIPTION |
|---|---|
| File Sharing | |
| Network Attached Storage Name | Specify the name to identify the LTE3311 in a work group. |
| Work Group | You can add the LTE3311 to an existing or a new workgroup on your network. Enter the name of the workgroup which your LTE3311 automatically joins. You can set the LTE3311's workgroup name to be exactly the same as the workgroup name to which your computer belongs to.<br><br>Note: The LTE3311 will not be able to join the workgroup if your local area network has restrictions set up that do not allow devices to join a workgroup. In this case, contact your network administrator. |
| Server Comment | Enter the description of the LTE3311 in a work group. |
| Apply | Click **Apply** to save your changes back to the LTE3311. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

# 20.3 FTP Screen

Use this screen to set up file sharing via the LTE3311 using FTP.

Click **Application** > **NAS > FTP** to open the following screen.

**Figure 95** Application > NAS > FTP



The following table describes the labels in this screen.

**Table 69** Application > NAS > FTP

| LABEL | DESCRIPTION |
|---|---|
| FTP | Select to enable or disable the FTP server on the LTE3311 for file sharing using FTP. |
| FTP Port | You may change the server port number for FTP if needed, however you must use the same port number in order to use that service for file sharing. |
| FTP Max Connection per IP | Select the maximum number of FTP connections that are allowed from a single IP address. |
| FTP MAX Client | Select the maximum number of FTP clients that are allowed to connect to the FTP server. |
| Client Support UTF8 | Set whether the FTP clients support UTF-8 encoding. |
| Code page | If you select **No** in the **Client Support UTF8** field, select a code page being used for the connection. |
| Apply | Click **Apply** to save your changes back to the LTE3311. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

## 20.3.1 Example of Accessing Your Shared Files From a Computer

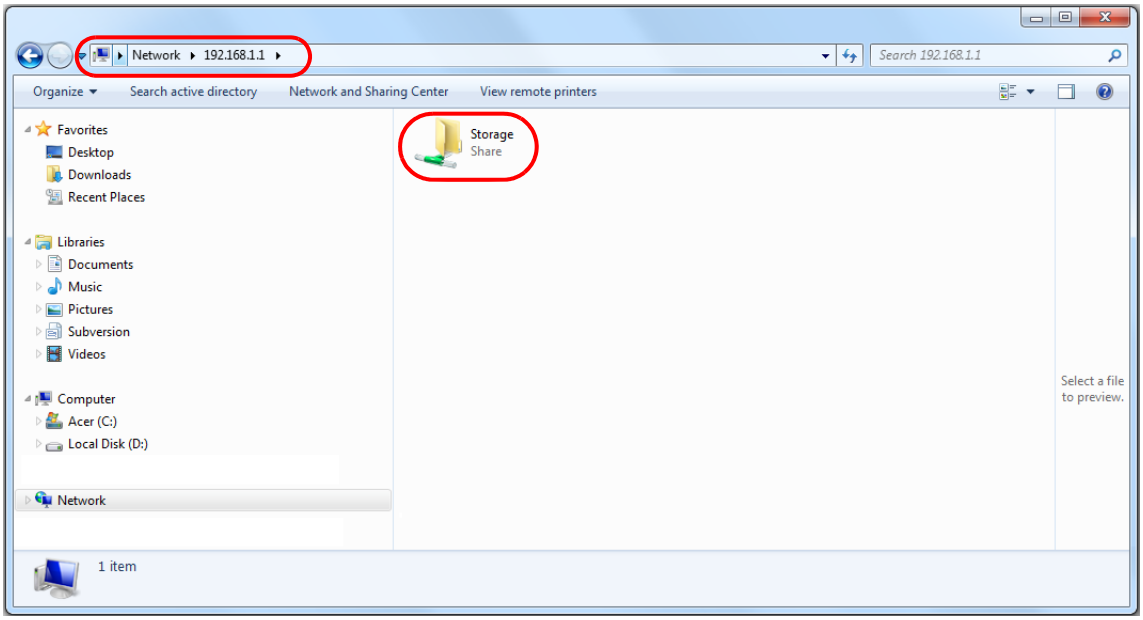
You can use Windows Explorer or FTP to access the USB storage devices connected to the LTE3311.

### Use Windows Explorer to Share Files

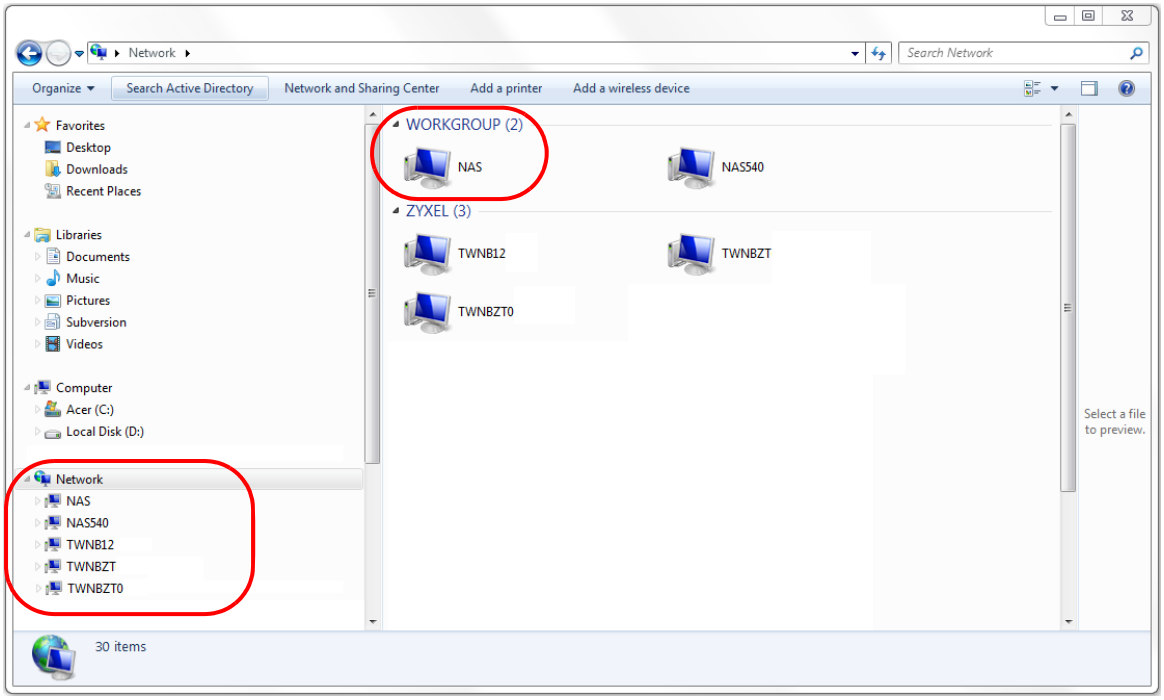
Open Windows Explorer to access the connected USB device using either Windows Explorer browser or by browsing to your workgroup.

Note: This example shows you how to use Microsoft’s Windows 7 to browse your shared files. Refer to your operating system’s documentation for how to browse your file structure.

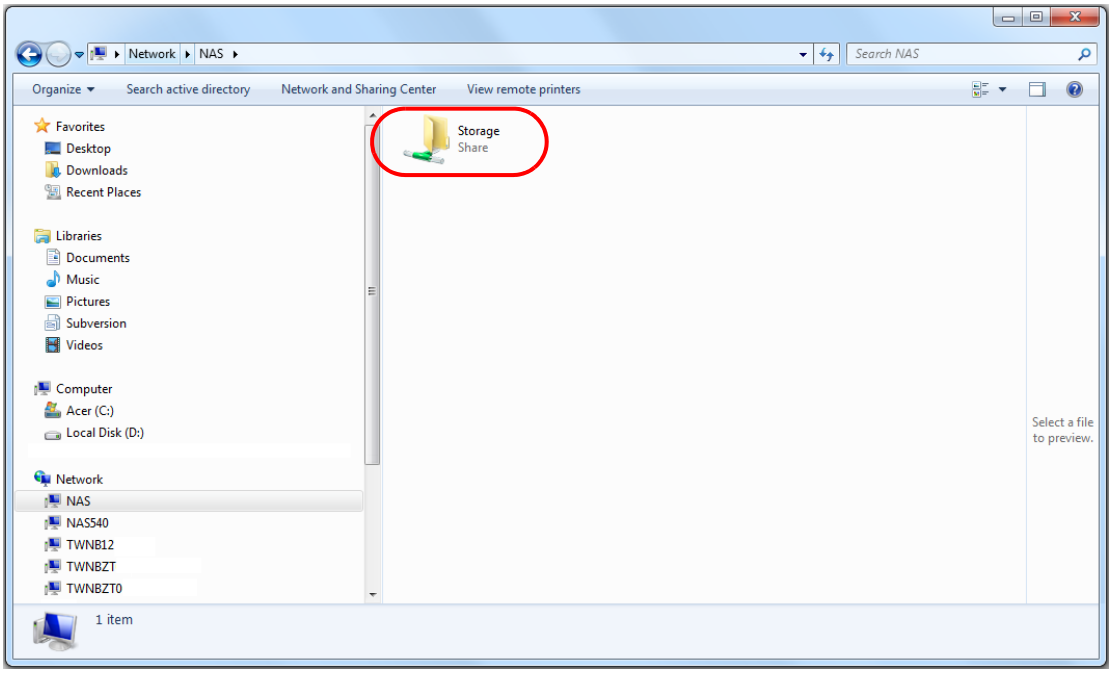
1 In Windows Explorer's address bar type a double backslash "\\" followed by the IP address of the LTE3311 (the default IP address of the LTE3311 is 192.168.1.1) and press [ENTER].




2 You can also access files via the LTE3311 by browsing to the workgroup folder using the folder tree on the left side of the screen. It is located under **Network**. In this example the LTE3311's name in a work group is the default "NAS" and the workgroup name is the default "WORKGROUP".



3 The screen changes and shows you the folder for the USB storage device connected to your LTE3311. Double-click the folder to display the contents in it.



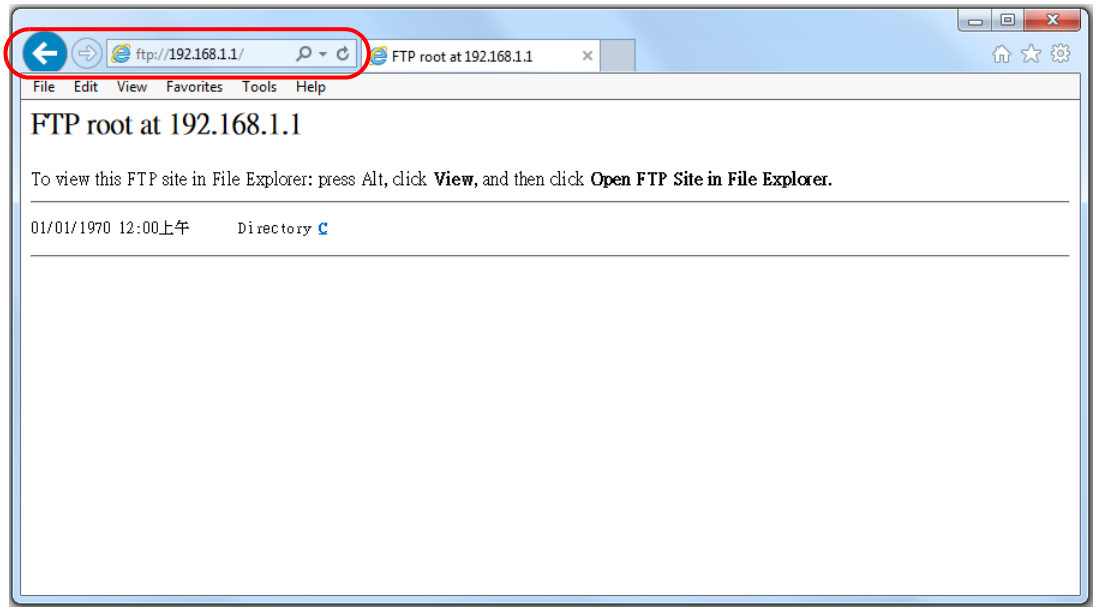

## Use FTP to Share Files

You can use FTP to access the USB storage device connected to the LTE3311. In this example, we use the web browser to share files via FTP from the LAN. The way or screen you log into the FTP server (on the LTE3311) varies depending on your FTP client. See your FTP client documentation for more information.

You should have enabled file sharing in the **Application** > **NAS** > **FTP** screen.

1 In your web browser's address or URL bar type "ftp://" followed by the IP address of the LTE3311 (the default LAN IP address of the LTE3311 is 192.168.1.1) and click **Go** or press [ENTER].

2 The screen changes and shows you the folder for the USB storage device connected to your LTE3311. Double-click the folder to display the contents in it.



# 21

# Bandwidth Management

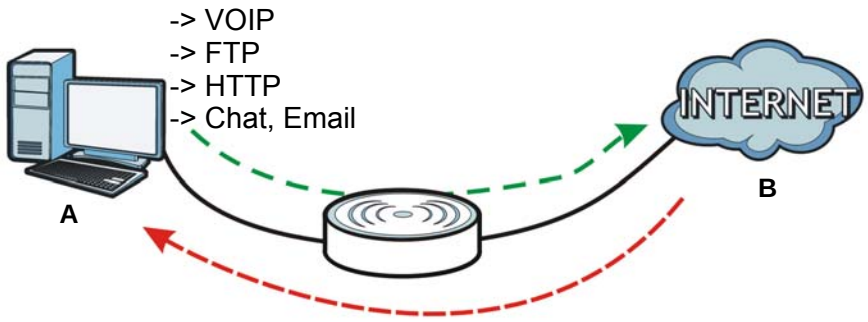
## 21.1 Overview

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 96** 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).

## 21.2 What You Can Do

- Use the **General** screen to enable bandwidth management and assign bandwidth values (Section 21.4 on page 151).
- Use the **Advanced** screen to configure bandwidth managements rule for the services and applications (Section 21.5 on page 152).

# 21.3 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 21.5 on page 152).

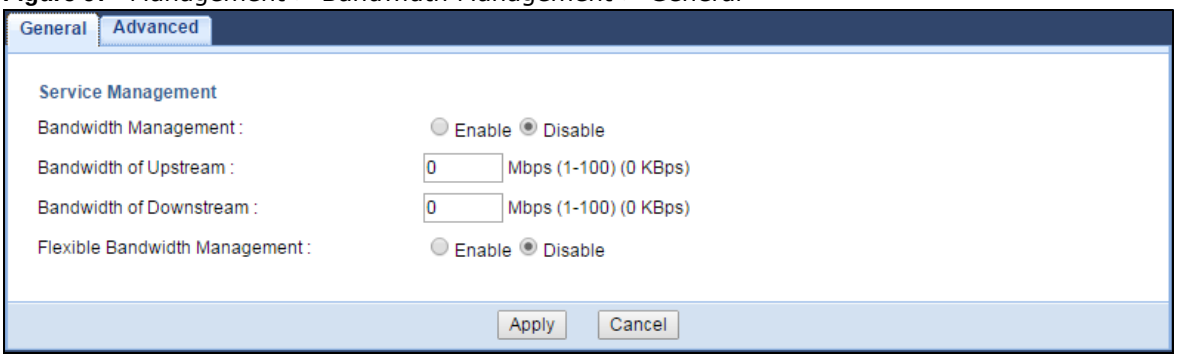
The sum of the bandwidth allotments that apply to the LAN interface (WAN to LAN, WAN to WLAN) must be less than or equal to the downstream bandwidth that you configure in the **Bandwidth Management > General** screen (Section 21.5 on page 152).

# 21.4 General Screen

Use this screen to have the LTE3311 apply bandwidth management.

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

**Figure 97** Management > Bandwidth Management > General




The following table describes the labels in this screen.

**Table 70** Management > Bandwidth Management > General

| LABEL | DESCRIPTION |
|---|---|
| Enable Bandwidth Management | This field allows you to have LTE3311 apply bandwidth management.<br>Enable bandwidth management to give traffic that matches a bandwidth rule priority over traffic that does not match a bandwidth rule.<br>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.<br>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.<br>This is traffic from WAN to LAN/WLAN. |
| 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. |
| Apply | Click **Apply** to save your customized settings. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

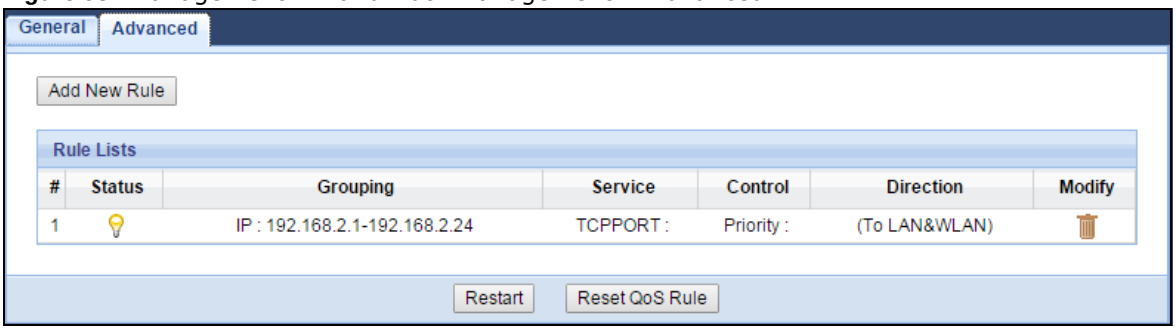
# 21.5 Advanced Screen

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 LTE3311. Additionally, you can define the IP addresses and port for a service or application.

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

**Figure 98** Management > Bandwidth Management > Advanced




The following table describes the labels in this screen.

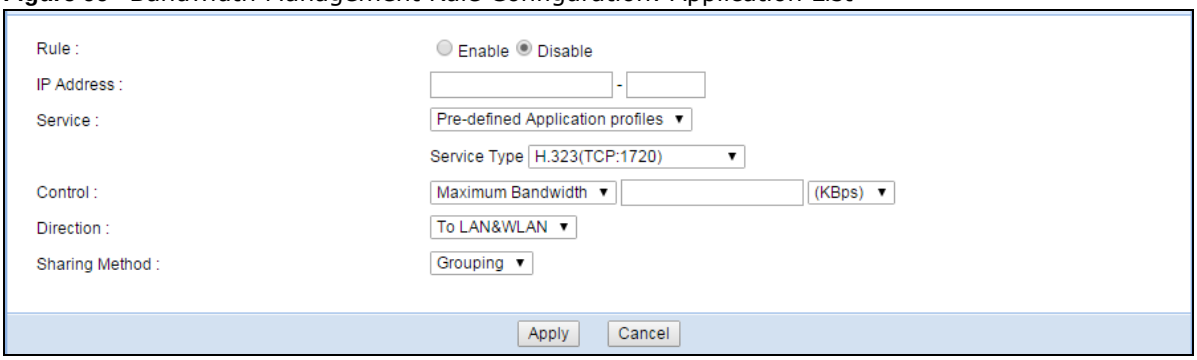
**Table 71** Management > Bandwidth Management > Advanced

| 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. |
| # | 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. |
| 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. |

## 21.5.1 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 99** Bandwidth Management Rule Configuration: Application List




The following table describes the labels in this screen.

**Table 72** 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.<br>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 LTE3311 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).<br>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.<br>Select **To WAN** to apply the rule to traffic from LAN/WLAN to WAN.<br>Select **Both** to apply the rule to traffic traveling in either direction. |
| Sharing Method | This field is available only when you set **Control** to **Maximum Bandwidth** or **Minimum Bandwidth**.<br>Select **Grouping** to have all IP addresses in the rule share the specified bandwidth.<br>Select **Single** and each IP address in the rule can have the specified bandwidth. |
| Apply | Click **Apply** to save your customized settings. |
| Cancel | Click **Cancel** to exit this screen without saving. |

See Appendix D on page 216 for commonly used services and port numbers.

# 22

# Universal Plug-and-Play (UPnP)

## 22.1 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.

## 22.2 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.

### 22.2.1 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.

### 22.2.2 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 LTE3311 allows multicast messages on the LAN only.

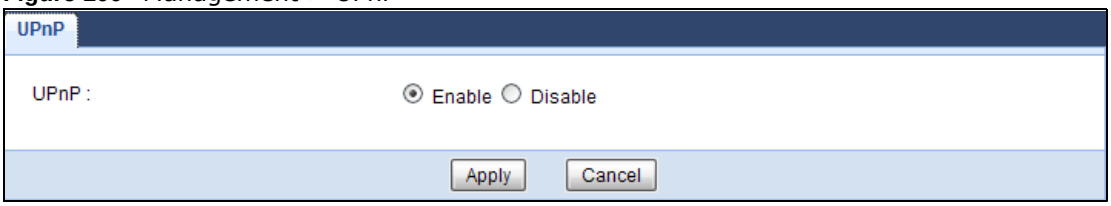
All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

# 22.3 UPnP Screen

Use this screen to enable UPnP on your LTE3311.

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

**Figure 100** Management > UPnP




The following table describes the fields in this screen.

**Table 73** 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 LTE3311's IP address (although you must still enter the password to access the web configurator). |
| Apply | Click **Apply** to save the setting to the LTE3311. |
| Cancel | Click **Cancel** to return to the previously saved settings. |

# 22.4 Technical Reference

The sections show examples of using UPnP.

## 22.4.1 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 LTE3311.

Make sure the computer is connected to a LAN port of the LTE3311. Turn on your computer and the LTE3311.

### 22.4.1.1 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 101** Network Connections


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

**Figure 102** Internet Connection Properties


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

**Figure 103** Internet Connection Properties: Advanced Settings

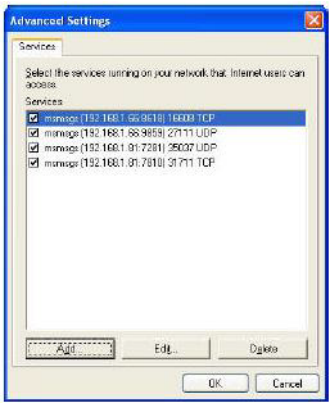
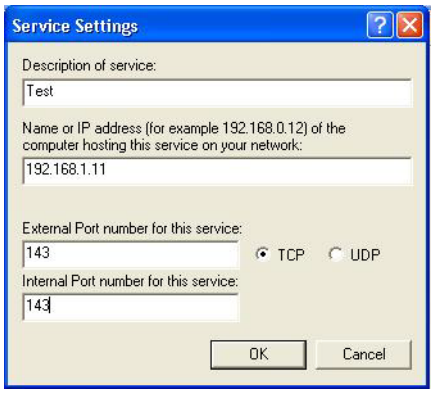


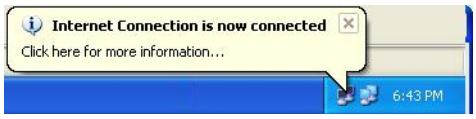
**Figure 104** Internet Connection Properties: Advanced Settings: Add




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

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

**Figure 105** System Tray Icon




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

**Figure 106** Internet Connection Status


## 22.4.2 Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the LTE3311 without finding out the IP address of the LTE3311 first. This comes helpful if you do not know the IP address of the LTE3311.

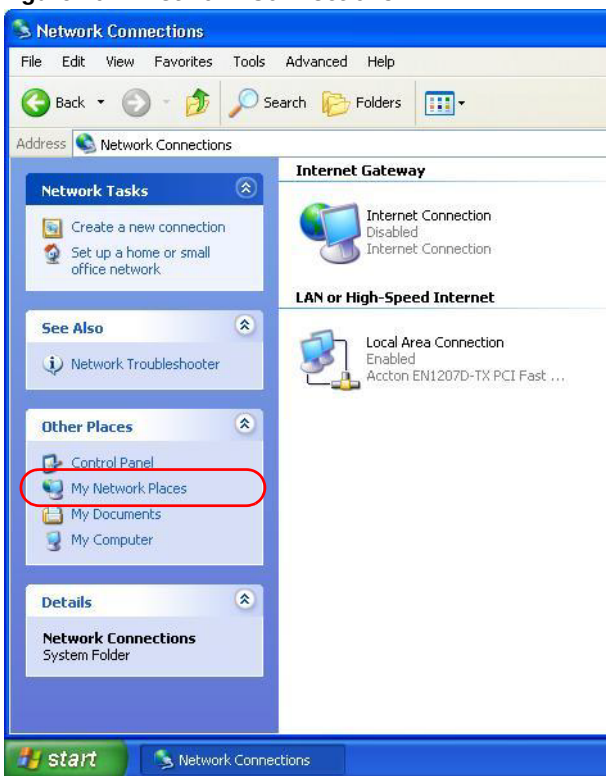
Follow the steps below to access the web configurator.

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

2 Double-click **Network Connections**.

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

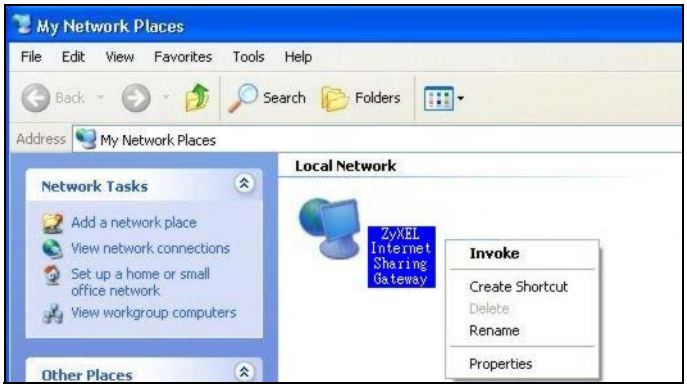
**Figure 107** Network Connections




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

5 Right-click on the icon for your LTE3311 and select **Invoke**. The web configurator login screen displays.

**Figure 108** Network Connections: My Network Places




6 Right-click on the icon for your LTE3311 and select **Properties**. A properties window displays with basic information about the LTE3311.

**Figure 109** Network Connections: My Network Places: Properties: Example

# 23

# TR-069

## 23.1 Overview

This chapter explains how to configure the LTE3311's TR-069 auto-configuration settings.

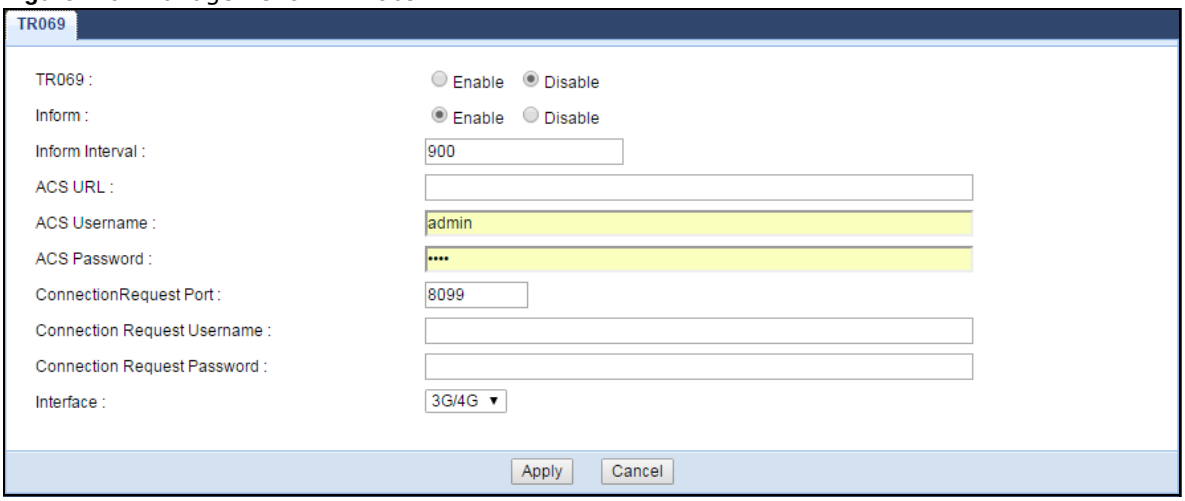
## 23.2 TR-069 Screen

TR-069 defines how Customer Premise Equipment (CPE), for example your LTE3311, 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 LTE3311, modify settings, perform firmware upgrades as well as monitor and diagnose the LTE3311. 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 **Management > TR-069** to open the following screen. Use this screen to configure your LTE3311 to be managed by an ACS.

**Figure 110** Management > TR-069



The following table describes the fields in this screen.

**Table 74** Maintenance > TR-069

| LABEL | DESCRIPTION |
|---|---|
| TR069 | Select **Enable** to allow the LTE3311 to be managed remotely by an ACS via TR-069. Otherwise, select **Disable**. |
| Inform | Select **Enable** for the LTE3311 to send periodic inform via TR-069 on the WAN. Otherwise, select **Disable**. |
| Inform Interval | Enter the time interval (in seconds) at which the LTE3311 sends information to the auto-configuration server. |
| ACS URL | Enter the URL or IP address of the auto-configuration server. |
| ACS Username | Enter the TR-069 user name for authentication with the auto-configuration server. |
| ACS Password | Enter the TR-069 password for authentication with the auto-configuration server. |
| Connection Request Port | Enter the port number for TR-069 connection requests. |
| Connection Request Username | Enter the connection request user name.<br>When the ACS makes a connection request to the LTE3311, this user name is used to authenticate the ACS. |
| Connection Request Password | Enter the connection request password.<br>When the ACS makes a connection request to the LTE3311, this password is used to authenticate the ACS. |
| Interface | Select a WAN interface through which the TR-069 traffic passes. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 24

# Maintenance

## 24.1 Overview

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

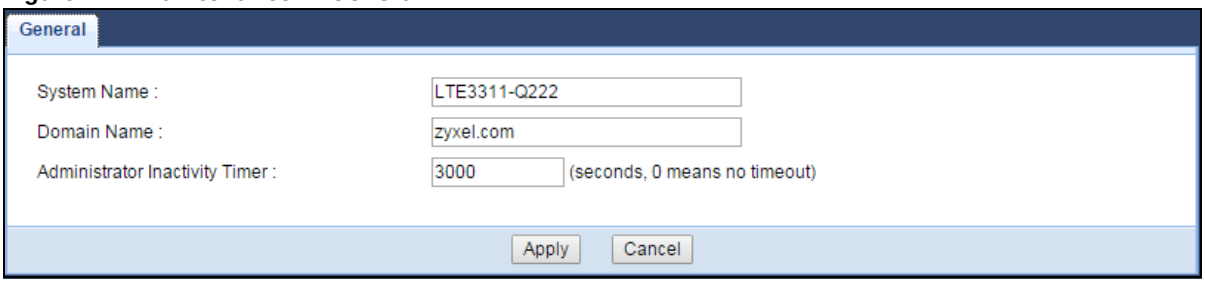
## 24.2 What You Can Do

- Use the **General** screen to set the timeout period of the management session (Section 24.3 on page 162).
- Use the **Account** screen to change your LTE3311's system password (Section 24.4 on page 163).
- Use the **Time** screen to change your LTE3311's time and date (Section 24.5 on page 164).
- Use the **Firmware Upgrade** screen to upload firmware to your LTE3311 (Section 24.6 on page 166).
- Use the **Backup / Restore** screen to view information related to factory defaults, backup configuration, and restoring configuration (Section 24.7 on page 167).
- Use the **Restart** screen to reboot the LTE3311 without turning the power off (Section 24.8 on page 169).

## 24.3 General Screen

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

**Figure 111** Maintenance > General



The following table describes the labels in this screen.

**Table 75** Maintenance > General

| LABEL | DESCRIPTION |
|---|---|
| System Name | System Name is a unique name to identify the LTE3311 in an Ethernet network. |
| Domain Name | Enter the domain name you want to give to the LTE3311. |
| 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). |
| Apply | Click **Apply** to save your changes back to the LTE3311. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

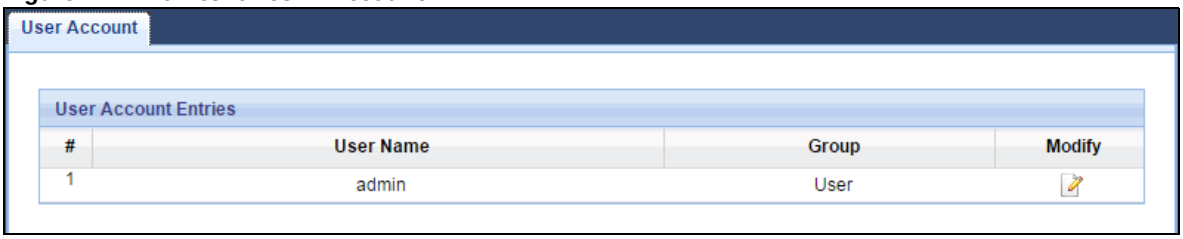
# 24.4 Account Screen

It is strongly recommended that you change your LTE3311's system password.

If you forget your LTE3311's password (or IP address), you will need to reset the device. See Section 24.8 on page 169 for details.

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

**Figure 112** Maintenance > Account




The following table describes the labels in this screen.

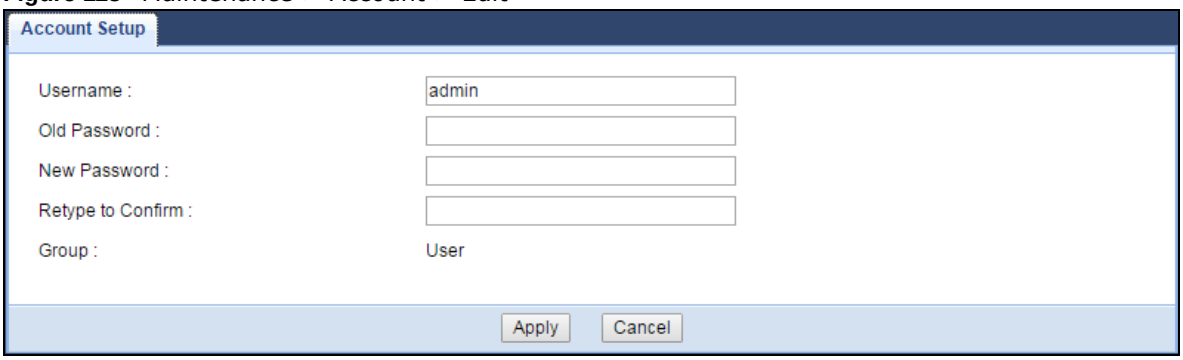
**Table 76** Maintenance > Account

| 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. |

## 24.4.1 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 113** Maintenance > Account > Edit




The following table describes the labels in this screen.

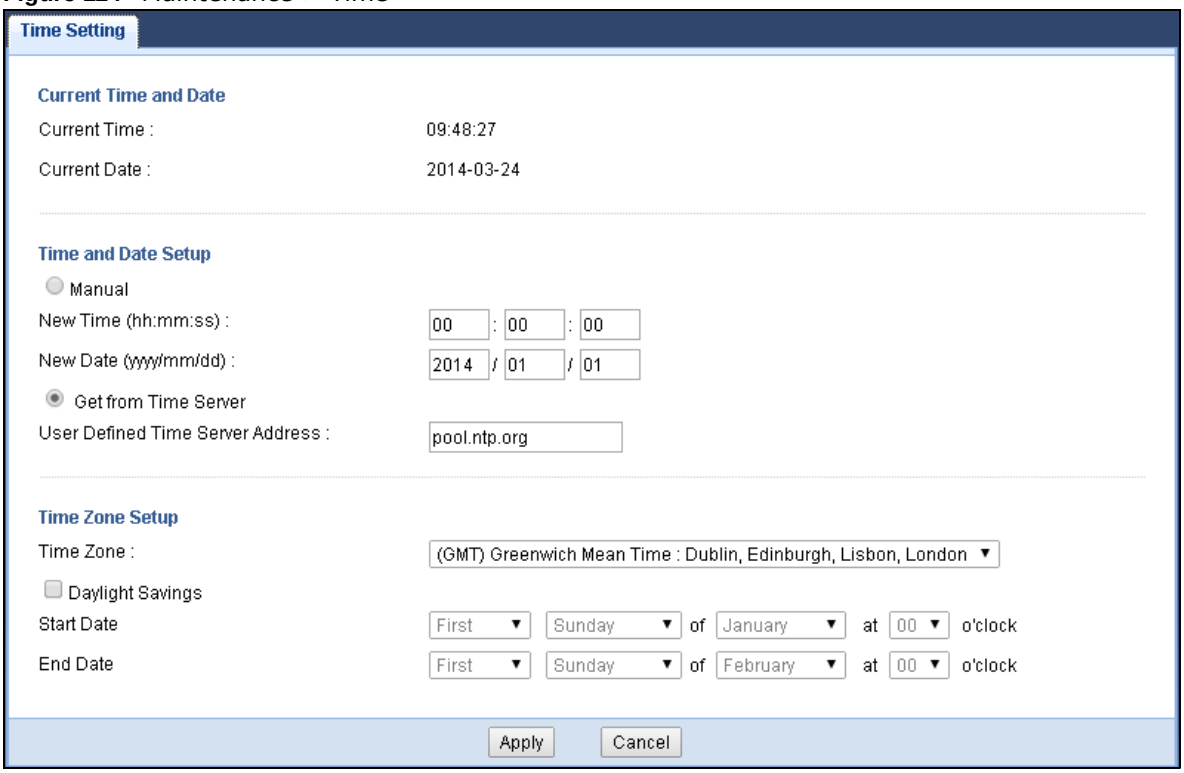
**Table 77** Maintenance > Account > Edit

| 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 (up to 30 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type. |
| Retype to Confirm | Type the new password again in this field. |
| Group | This shows the type of login account. |
| Apply | Click **Apply** to save your changes back to the LTE3311. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

# 24.5 Time Setting Screen

Use this screen to configure the LTE3311's time based on your local time zone. To change your LTE3311's time and date, click **Maintenance** > **Time**. The screen appears as shown.

**Figure 114** Maintenance > Time




The following table describes the labels in this screen.

**Table 78** Maintenance > Time

| LABEL | DESCRIPTION |
|---|---|
| Current Time and Date | |
| Current Time | This field displays the time of your LTE3311.<br><br>Each time you reload this page, the LTE3311 synchronizes the time with the time server. |
| Current Date | This field displays the date of your LTE3311.<br><br>Each time you reload this page, the LTE3311 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<br><br>(hh:mm:ss) | This field displays the last updated time from the time server or the last time configured manually.<br><br>When you select **Manual**, enter the new time in this field and then click **Apply**. |
| New Date<br><br>(yyyy/mm/dd) | This field displays the last updated date from the time server or the last date configured manually.<br><br>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 LTE3311 get the time and date from the time server you specified below. |

**Table 78** Maintenance > Time (continued)

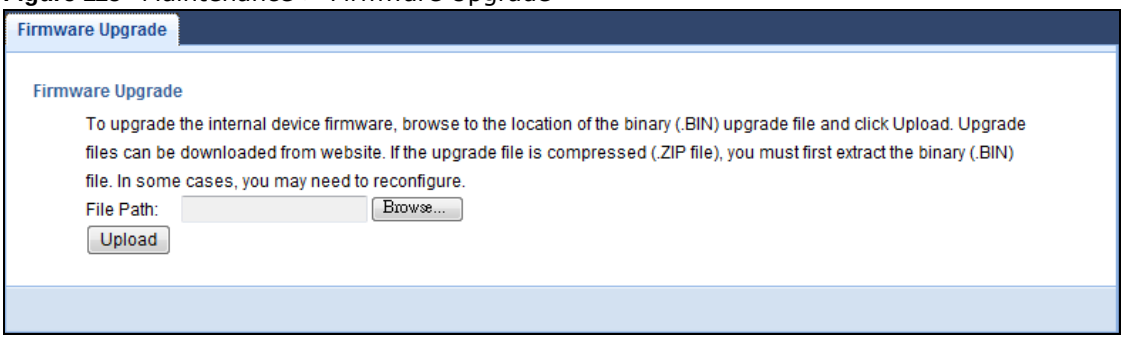
| LABEL | DESCRIPTION |
|---|---|
| User Defined Time Server Address | Select **User Defined Time Server Address** and enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information. |
| Time Zone Setup | |
| 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.<br><br>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:<br><br>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.<br><br>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:<br><br>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.<br><br>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). |
| Apply | Click **Apply** to save your changes back to the LTE3311. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

# 24.6 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 LTE3311.

**Figure 115** Maintenance > Firmware Upgrade




The following table describes the labels in this screen.

**Table 79** Maintenance > Firmware Upgrade

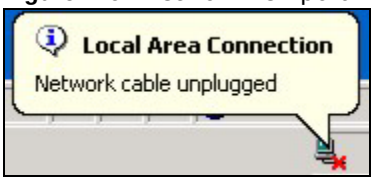
| LABEL | DESCRIPTION |
|---|---|
| File Path | Type in the location of the file you want to upload in this field or click **Browse...** to find it. |
| Browse... | Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload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

Note: Do not turn off the LTE3311 while firmware upload is in progress!

After you see the **Firmware Upload In Process** screen, wait two minutes before logging into the LTE3311 again.

The LTE3311 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

**Figure 116** Network Temporarily Disconnected




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

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

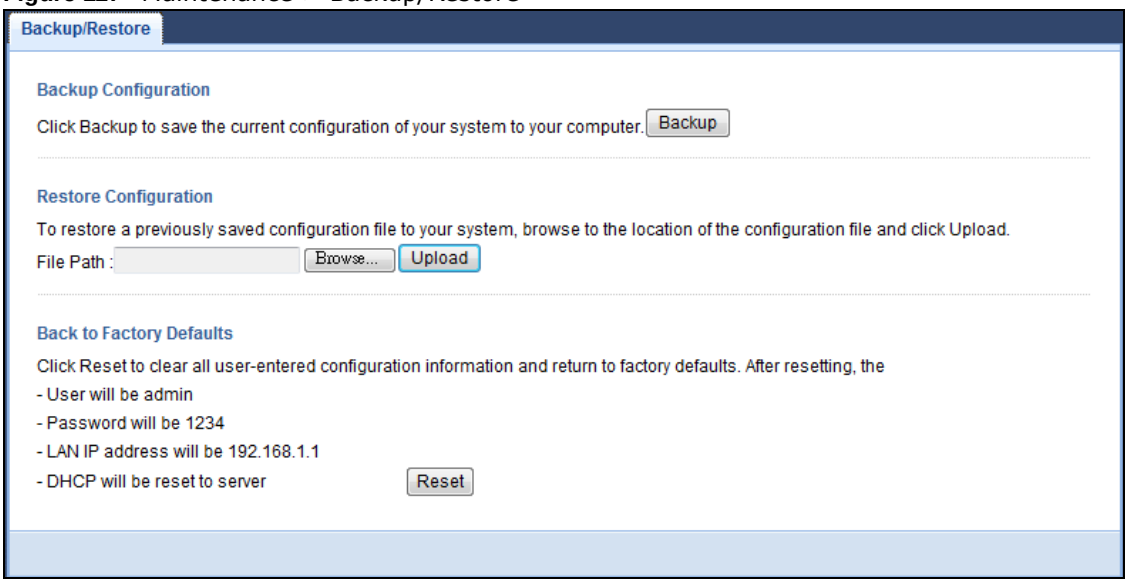
# 24.7 Configuration Backup/Restore Screen

Backup configuration allows you to back up (save) the LTE3311's current configuration to a file on your computer. Once your LTE3311 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 LTE3311.

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

**Figure 117** Maintenance > Backup/Restore




The following table describes the labels in this screen.

**Table 80** Maintenance > Backup/Restore

| LABEL | DESCRIPTION |
|---|---|
| Backup | Click **Backup** to save the LTE3311's current configuration to your computer. |
| File Path | Type in the location of the file you want to upload in this field or click **Browse...** to find it. |
| Browse... | Click **Browse...** to find the 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.<br><br>Note: Do not turn off the LTE3311 while configuration file upload is in progress.<br><br>After you see a "configuration upload successful" screen, you must then wait one minute before logging into the LTE3311 again. The LTE3311 automatically restarts in this time causing a temporary network disconnect.<br><br>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 LTE3311 to its factory defaults.<br><br>You can also press the **RESET** button on the rear panel to reset the factory defaults of your LTE3311. Refer to the chapter about introducing the Web Configurator for more information on the **RESET** button. |

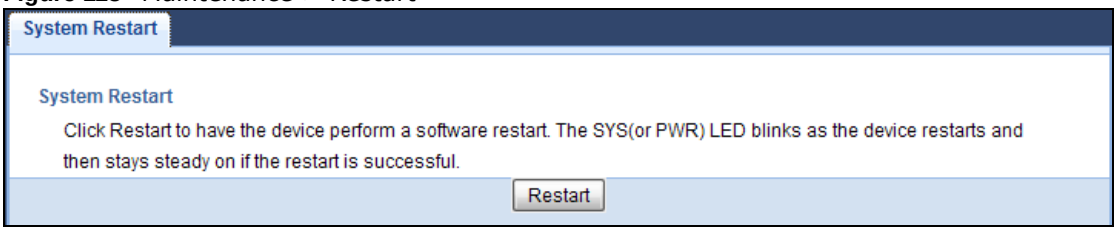
Note: If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default LTE3311 IP address (192.168.1.1). See Appendix C on page 190 for details on how to set up your computer's IP address.

# 24.8 Restart Screen

System restart allows you to reboot the LTE3311 without turning the power off.

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

**Figure 118** Maintenance > Restart




Click **Restart** to have the LTE3311 reboot. This does not affect the LTE3311's configuration.

# 25

# Troubleshooting

## 25.1 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
- LTE3311 Access and Login
- Internet Access
- Wireless Connections

## 25.2 Power, Hardware Connections, and LEDs

### The LTE3311 does not turn on. None of the LEDs turn on.

1. Make sure you are using the power adaptor or cord included with the LTE3311.
2. Make sure the power adaptor or cord is connected to the LTE3311 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 LTE3311.
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 1.8 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 LTE3311.
5. If the problem continues, contact the vendor.

# 25.3 LTE3311 Access and Login

## I don't know the IP address of my LTE3311.

1 The default IP address of the LTE3311 is **192.168.1.1**.

2 If you changed the IP address and have forgotten it, you might get the IP address of the LTE3311 by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the LTE3311 (it depends on the network), so enter this IP address in your Internet browser.

3 Reset your LTE3311 to change all settings back to their default. This means your current settings are lost. See Section 1.5 on page 14 for information on resetting your LTE3311.

## I forgot the password.

1 The default password is **1234**.

2 If this does not work, you have to reset the device to its factory defaults. See Section 1.5 on page 14.

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

1 Make sure you are using the correct IP address.

- The default IP address of the LTE3311 is **192.168.1.1**.
- If you changed the IP address (Section 8.4 on page 85), use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I don't know the IP address of my LTE3311.

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

3 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled. See Appendix B on page 181.

4 Make sure your computer is in the same subnet as the LTE3311. (If you know that there are routers between your computer and the LTE3311, skip this step.)

- If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See Section 8.4 on page 85.
- If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the LTE3311. See Section 8.4 on page 85.

5 Reset the device to its factory defaults, and try to access the LTE3311 with the default IP address. See Section 1.5 on page 14.

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

**Advanced Suggestions**

- Try to access the LTE3311 using another service, such as Telnet. If you can access the LTE3311, check the firewall rules to find out why the LTE3311 does not respond to HTTP.
- If your computer is connected to the **WAN** port or is connected wirelessly, use a computer that is connected to a **LAN**/**ETHERNET** port.

I can see the **Login** screen, but I cannot log in to the LTE3311.

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 LTE3311.

4 If this does not work, you have to reset the device to its factory defaults. See Section 1.5 on page 14.

## 25.4 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.

I cannot access the Internet anymore. I had access to the Internet (with the LTE3311), but my Internet connection is not available anymore.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.8 on page 16.
2. Reboot the LTE3311.
3. 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. Look at the LEDs, and check Section 1.8 on page 16. If the LTE3311 is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
2. Check the signal strength. If the signal strength is low, try moving the LTE3311 closer to the ISP's base station if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).
3. Reboot the LTE3311.
4. If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

   **Advanced Suggestion**

   - Check the settings for QoS. If it is disabled, you might consider activating it.

## 25.5 Wireless Connections

I cannot access the LTE3311 or ping any computer from the WLAN.

1. Make sure the wireless LAN is enabled on the LTE3311.
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 LTE3311.
4. Make sure your computer (with a wireless adapter installed) is within the transmission range of the LTE3311.

5 Check that both the LTE3311 and the wireless adapter on your computer are using the same wireless and wireless security settings.

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

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

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

The following factors may cause interference:

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

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

- Move your wireless device closer to the AP if the signal strength is low.
- Reduce wireless interference that may be caused by other wireless networks or surrounding wireless electronics such as cordless phones.
- Place the AP where there are minimum obstacles (such as walls and ceilings) between the AP and the wireless client.
- Reduce the number of wireless clients connecting to the same AP simultaneously, or add additional APs if necessary.
- Try closing some programs that use the Internet, especially peer-to-peer applications. If the wireless client is sending or receiving a lot of information, it may have too many programs open that use the Internet.
- Position the antennas for best reception. If the AP is placed on a table or floor, point the antennas upwards. If the AP is placed at a high position, point the antennas downwards. Try pointing the antennas in different directions and check which provides the strongest signal to the wireless clients.

## 25.6 Getting More Troubleshooting Help

Search for support information for your model at www.zyxel.com for more troubleshooting suggestions.

# A

# Customer Support

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

See *http://www.zyxel.com/homepage.shtml* and also *http://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml* for the latest information.

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

### Required Information

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

## Corporate Headquarters (Worldwide)

### Taiwan

- ZyXEL Communications Corporation
- http://www.zyxel.com

## Asia

### China

- ZyXEL Communications (Shanghai) Corp.
  ZyXEL Communications (Beijing) Corp.
  ZyXEL Communications (Tianjin) Corp.
- http://www.zyxel.cn

### India

- ZyXEL Technology India Pvt Ltd
- http://www.zyxel.in

### Kazakhstan

- ZyXEL Kazakhstan
- http://www.zyxel.kz

### Korea

- ZyXEL Korea Corp.
- http://www.zyxel.kr

### Malaysia

- ZyXEL Malaysia Sdn Bhd.
- http://www.zyxel.com.my

### Pakistan

- ZyXEL Pakistan (Pvt.) Ltd.
- http://www.zyxel.com.pk

### Philippines

- ZyXEL Philippines
- http://www.zyxel.com.ph

### Singapore

- ZyXEL Singapore Pte Ltd.
- http://www.zyxel.com.sg

### Taiwan

- ZyXEL Communications Corporation
- http://www.zyxel.com/tw/zh/

### Thailand

- ZyXEL Thailand Co., Ltd
- http://www.zyxel.co.th

### Vietnam

- ZyXEL Communications Corporation-Vietnam Office
- http://www.zyxel.com/vn/vi

## Europe

### Austria

- ZyXEL Deutschland GmbH
- http://www.zyxel.de

### Belarus

- ZyXEL BY
- http://www.zyxel.by

### Belgium

- ZyXEL Communications B.V.
- http://www.zyxel.com/be/nl/
- http://www.zyxel.com/be/fr/

### Bulgaria

- ZyXEL България
- http://www.zyxel.com/bg/bg/

### Czech Republic

- ZyXEL Communications Czech s.r.o
- http://www.zyxel.cz

### Denmark

- ZyXEL Communications A/S
- http://www.zyxel.dk

### Estonia

- ZyXEL Estonia
- http://www.zyxel.com/ee/et/

### Finland

- ZyXEL Communications
- http://www.zyxel.fi

### France

- ZyXEL France
- http://www.zyxel.fr

### Germany

- ZyXEL Deutschland GmbH
- http://www.zyxel.de

### Hungary

- ZyXEL Hungary & SEE
- http://www.zyxel.hu

### Italy

- ZyXEL Communications Italy
- http://www.zyxel.it/

### Latvia

- ZyXEL Latvia
- http://www.zyxel.com/lv/lv/homepage.shtml

### Lithuania

- ZyXEL Lithuania
- http://www.zyxel.com/lt/lt/homepage.shtml

### Netherlands

- ZyXEL Benelux
- http://www.zyxel.nl

### Norway

- ZyXEL Communications
- http://www.zyxel.no

### Poland

- ZyXEL Communications Poland
- http://www.zyxel.pl

### Romania

- ZyXEL Romania
- http://www.zyxel.com/ro/ro

### Russia

- ZyXEL Russia
- http://www.zyxel.ru

### Slovakia

- ZyXEL Communications Czech s.r.o. organizacna zlozka
- http://www.zyxel.sk

### Spain

- ZyXEL Communications ES Ltd
- http://www.zyxel.es

### Sweden

- ZyXEL Communications
- http://www.zyxel.se

### Switzerland

- Studerus AG

- http://www.zyxel.ch/

### Turkey

- ZyXEL Turkey A.S.
- http://www.zyxel.com.tr

### UK

- ZyXEL Communications UK Ltd.
- http://www.zyxel.co.uk

### Ukraine

- ZyXEL Ukraine
- http://www.ua.zyxel.com

## Latin America

### Argentina

- ZyXEL Communication Corporation
- http://www.zyxel.com/ec/es/

### Brazil

- ZyXEL Communications Brasil Ltda.
- https://www.zyxel.com/br/pt/

### Ecuador

- ZyXEL Communication Corporation
- http://www.zyxel.com/ec/es/

## Middle East

### Israel

- ZyXEL Communication Corporation
- http://il.zyxel.com/homepage.shtml

### Middle East

- ZyXEL Communication Corporation
- http://www.zyxel.com/me/en/

## North America

### USA

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

## Oceania

### Australia

- ZyXEL Communications Corporation
- http://www.zyxel.com/au/en/

## Africa

### South Africa

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

B

# Pop-up Windows, JavaScript and Java Permissions

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

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

Note: The screens used below belong to Internet Explorer version 6, 7 and 8. Screens for other Internet Explorer versions may vary.

## Internet Explorer Pop-up Blockers

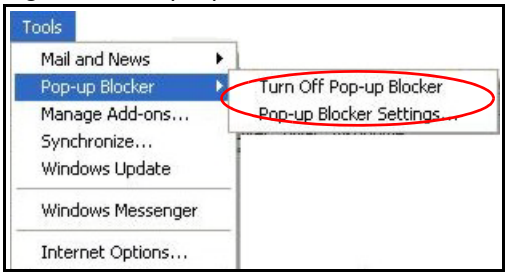
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

## Disable Pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

**Figure 119** Pop-up Blocker

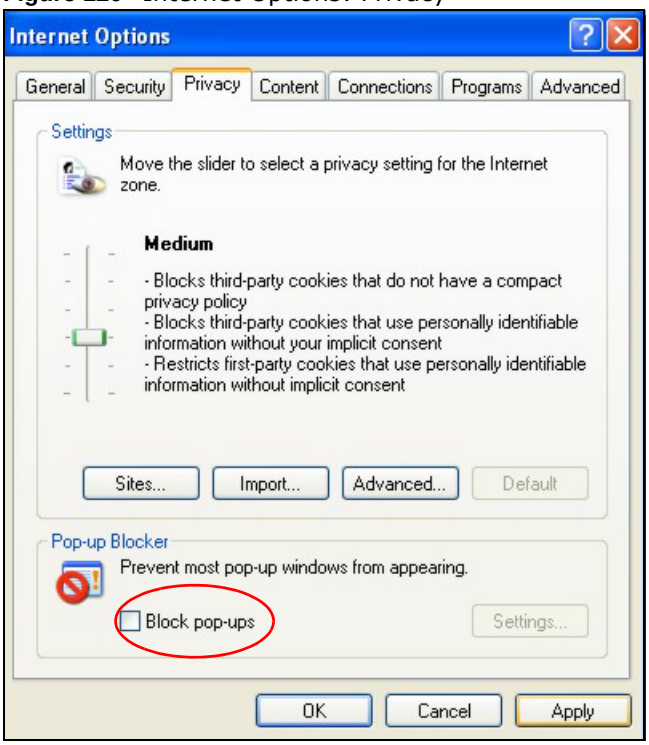



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

**Figure 120** Internet Options: Privacy




3 Click **Apply** to save this setting.

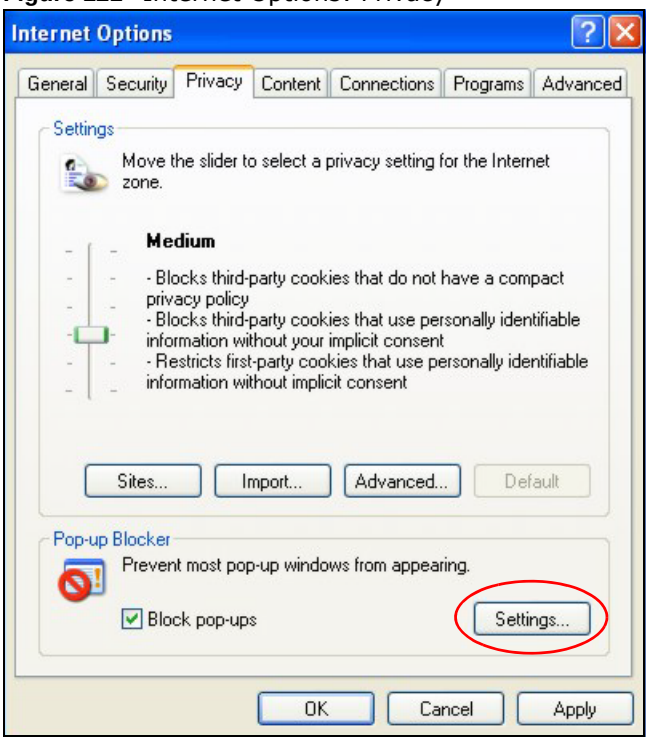
## Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings...**to open the **Pop-up Blocker Settings** screen.

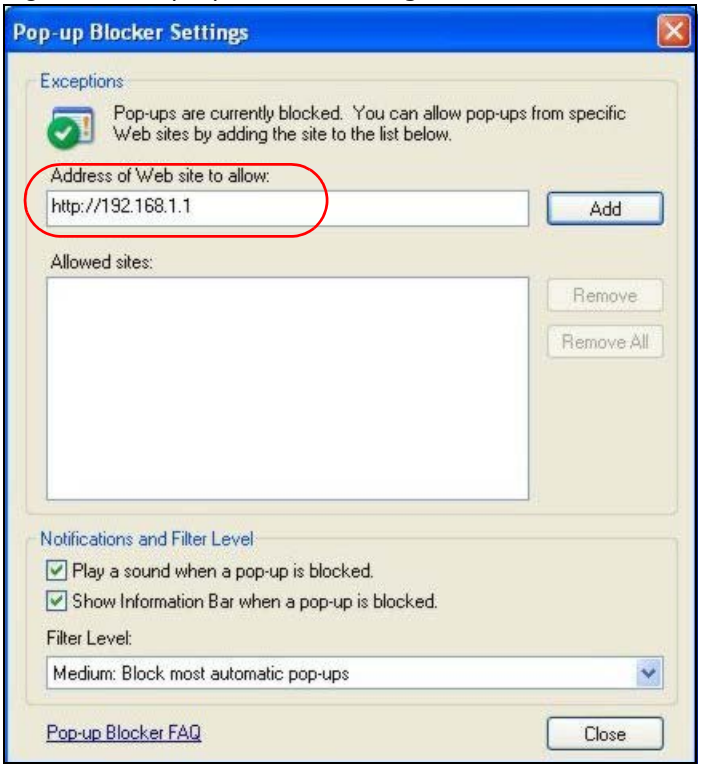
**Figure 121** Internet Options: Privacy




3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

**Figure 122** Pop-up Blocker Settings



5 Click **Close** to return to the **Privacy** screen.

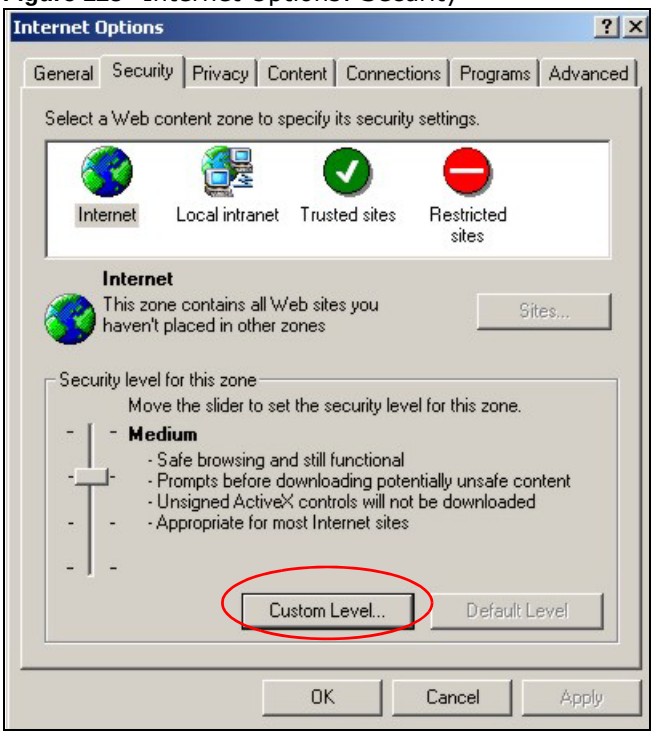
6 Click **Apply** to save this setting.

## JavaScript

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScript are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

**Figure 123** Internet Options: Security




2 Click the **Custom Level...** button.

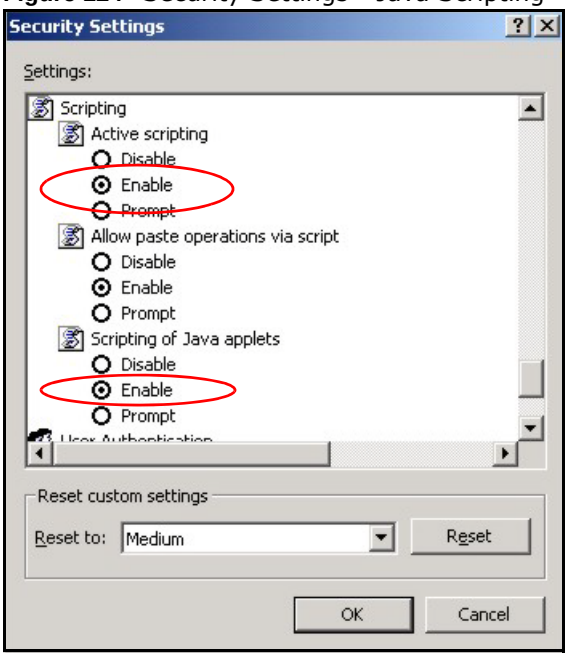
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

**Figure 124** Security Settings - Java Scripting




## Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

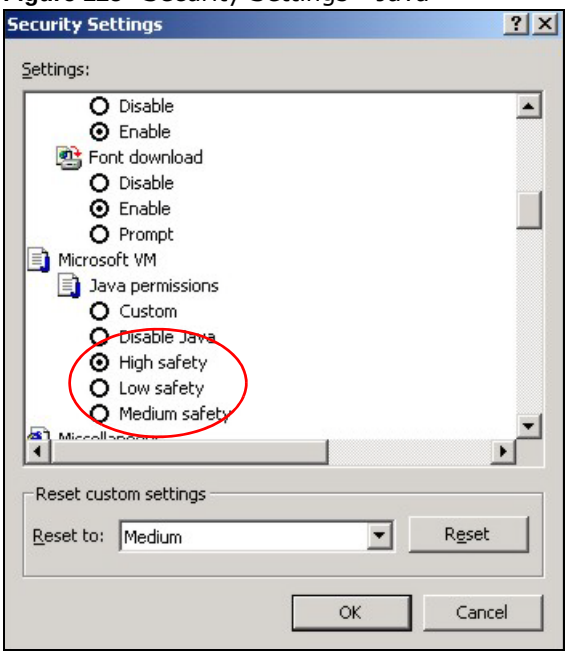
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

**Figure 125** Security Settings - Java



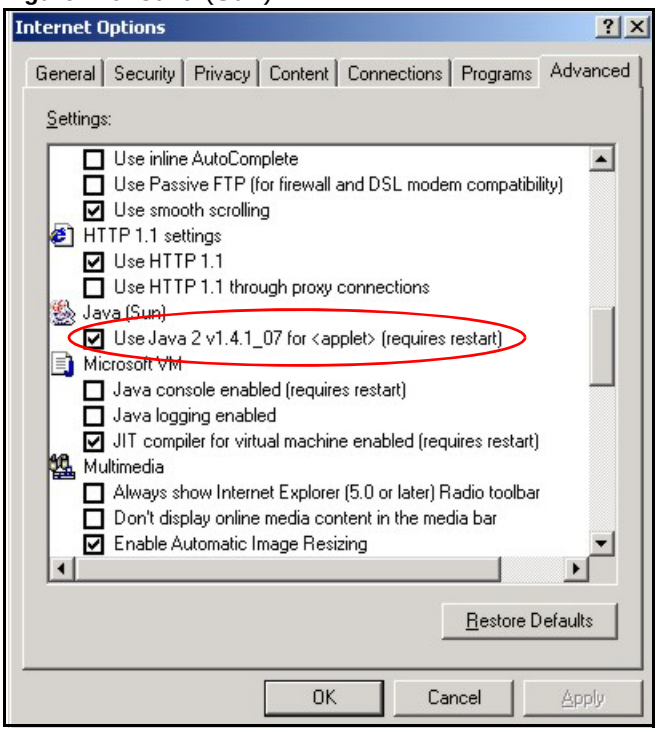

## JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

**Figure 126** Java (Sun)

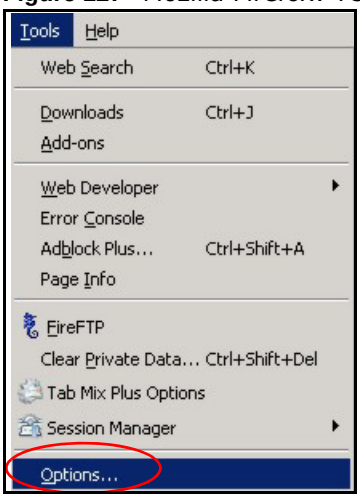


## Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary slightly. The steps below apply to Mozilla Firefox 3.0 as well.

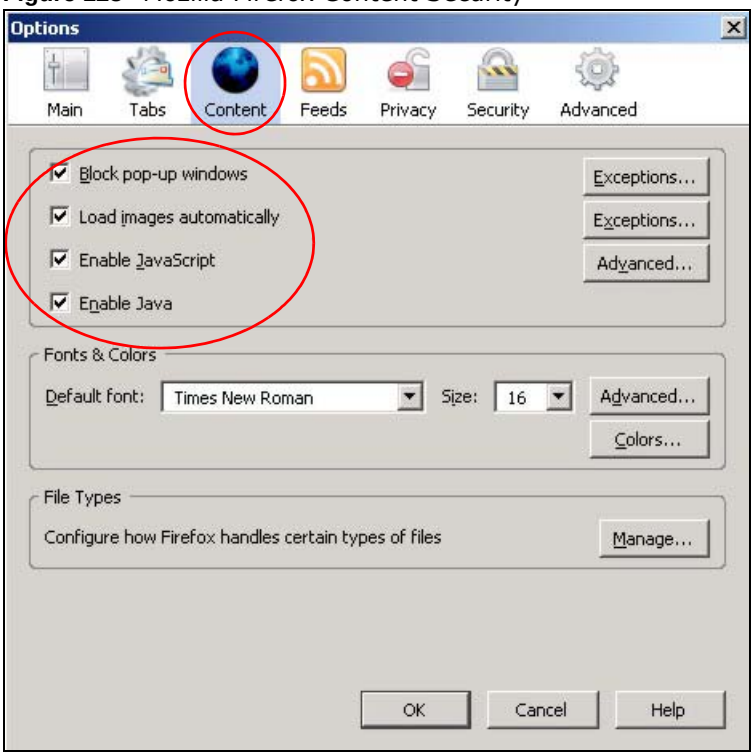
You can enable Java, Javascript and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

**Figure 127** Mozilla Firefox: TOOLS > Options




Click **Content** to show the screen below. Select the check boxes as shown in the following screen.

**Figure 128** Mozilla Firefox Content Security



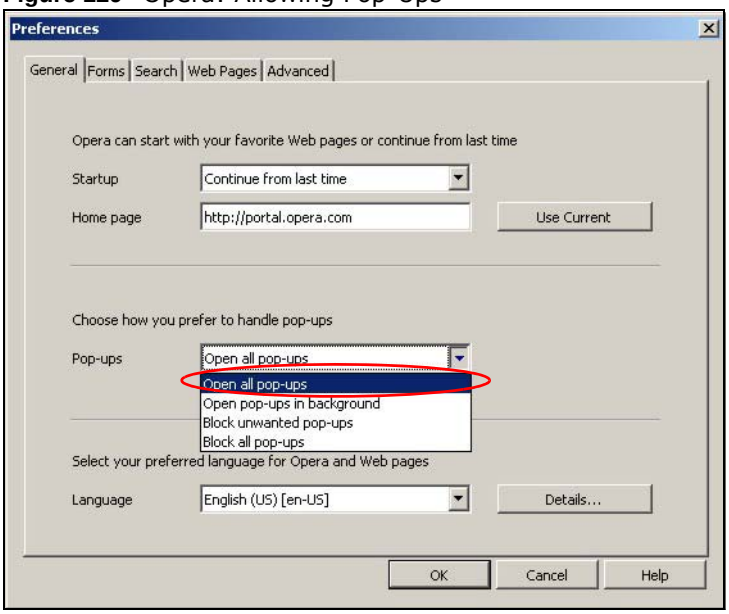
## Opera

Opera 10 screens are used here. Screens for other versions may vary slightly.

## Allowing Pop-Ups

From Opera, click **Tools**, then **Preferences**. In the **General** tab, go to **Choose how you prefer to handle pop-ups** and select **Open all pop-ups**.

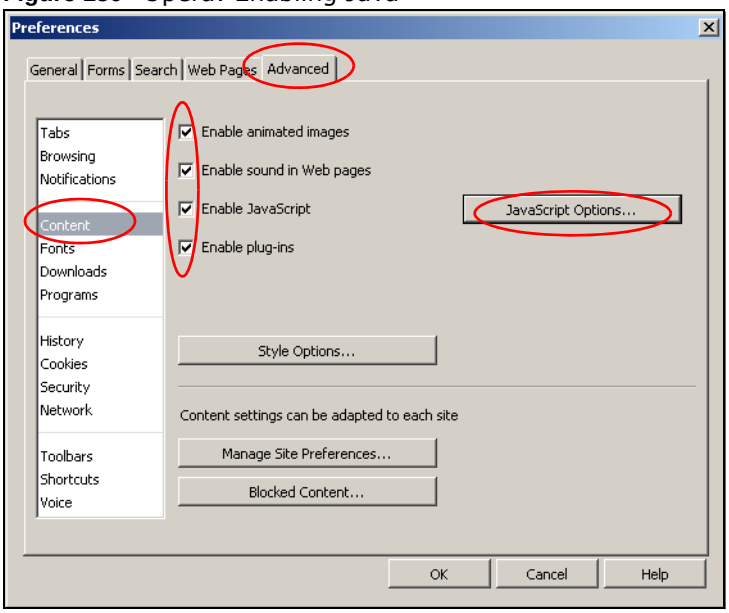
**Figure 129** Opera: Allowing Pop-Ups




## Enabling Java

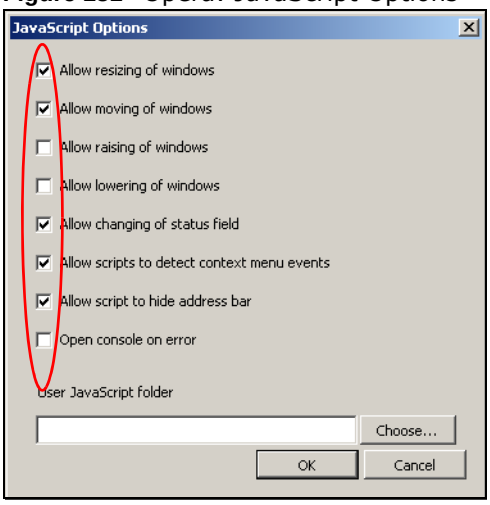
From Opera, click **Tools**, then **Preferences**. In the **Advanced** tab, select **Content** from the left-side menu. Select the check boxes as shown in the following screen.

**Figure 130** Opera: Enabling Java




To customize JavaScript behavior in the Opera browser, click **JavaScript Options**.

**Figure 131** Opera: JavaScript Options




Select the items you want Opera's JavaScript to apply.

C

# Setting Up Your Computer's IP Address

Note: Your specific LTE3301 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.

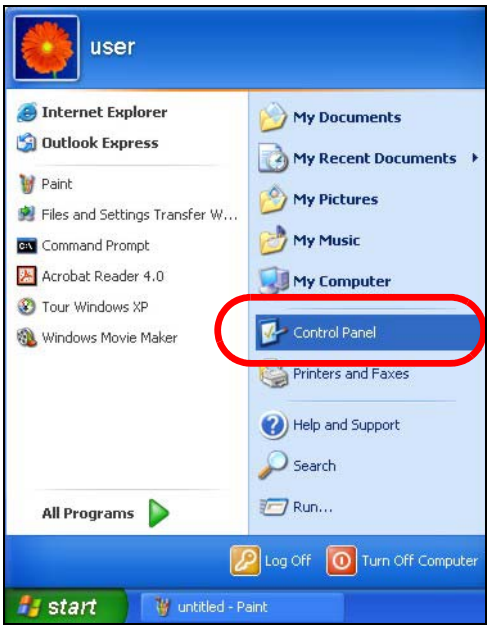
In this appendix, you can set up an IP address for:



## Windows XP/NT/2000

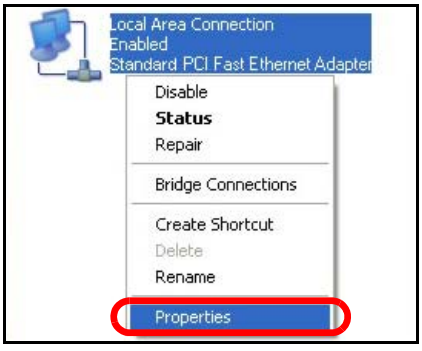
The following example uses the default Windows XP display theme but can also apply to Windows 2000 and Windows NT.

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

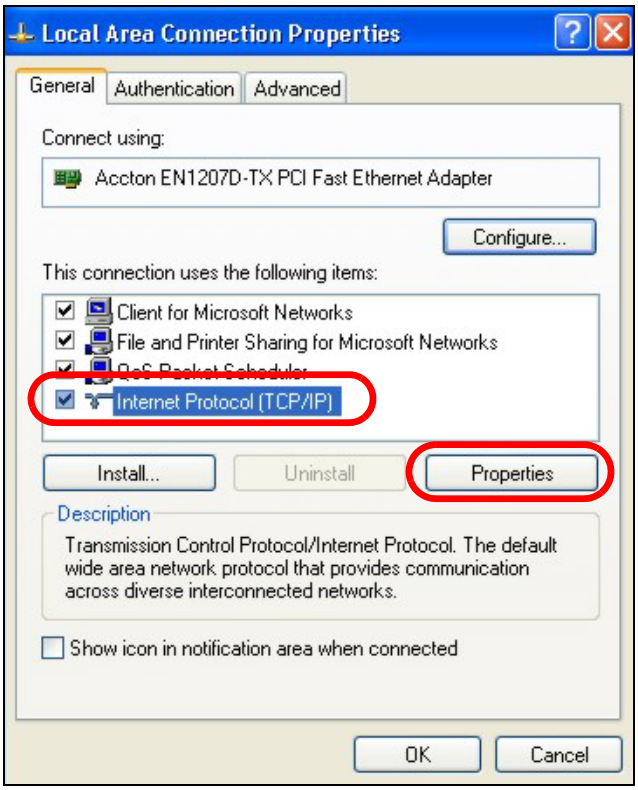



2 In the **Control Panel**, click the **Network Connections** icon.

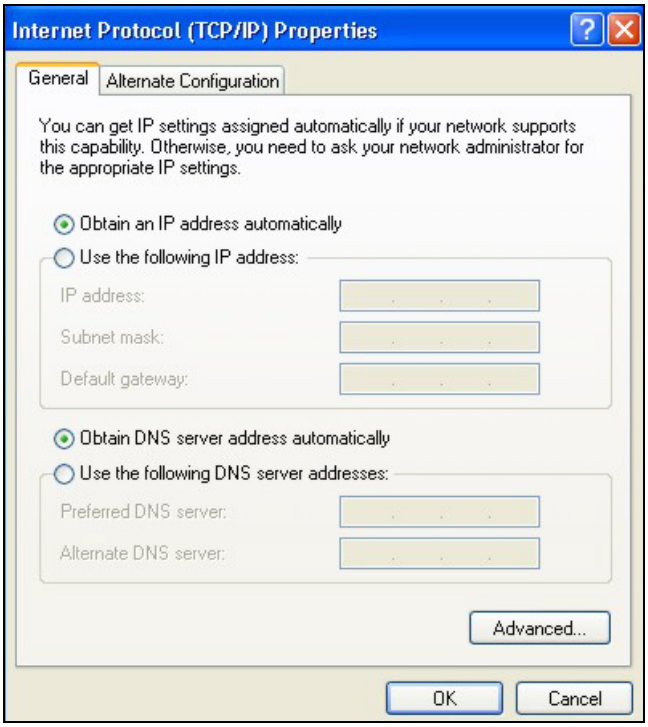

3 Right-click **Local Area Connection** and then select **Properties**.




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




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



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**.

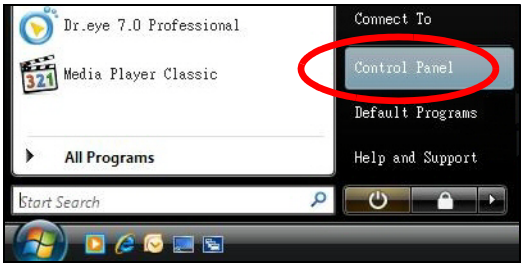
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

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.

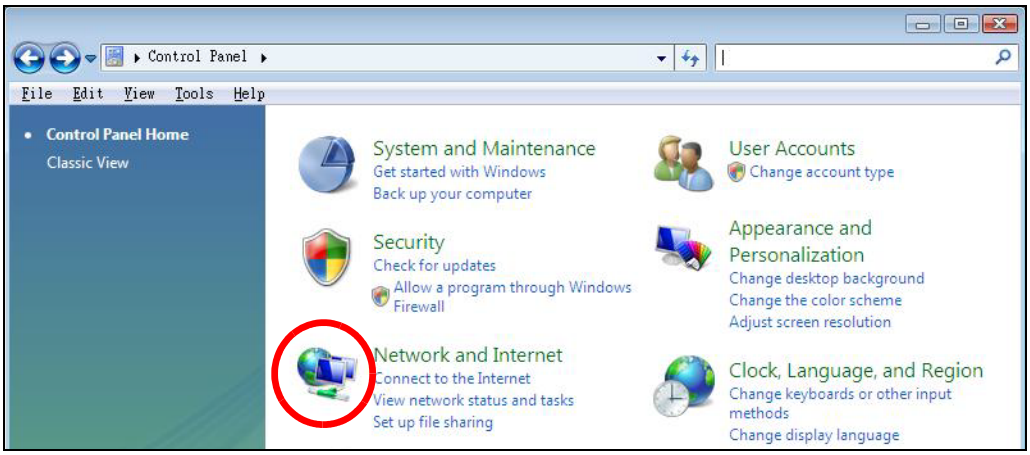
## Windows Vista

This section shows screens from Windows Vista Professional.

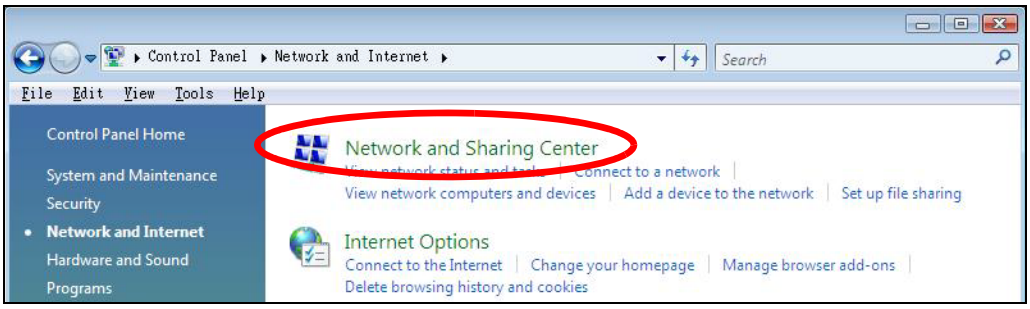
1 Click **Start** > **Control Panel**.



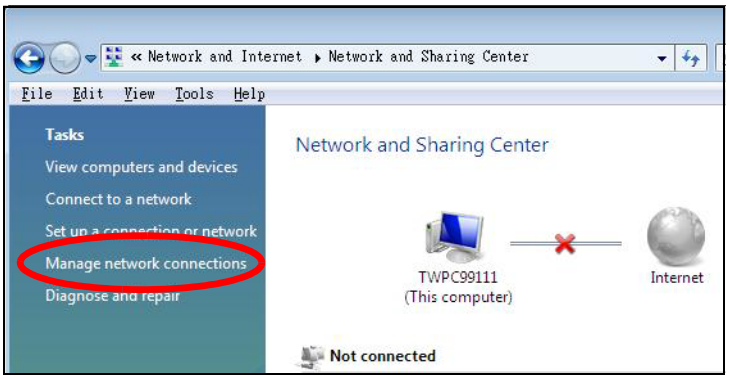

2 In the **Control Panel**, click the **Network and Internet** icon.



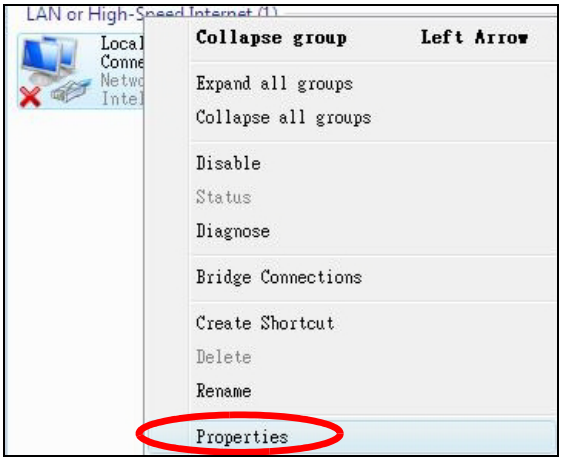
3 Click the **Network and Sharing Center** icon.




4 Click **Manage network connections**.

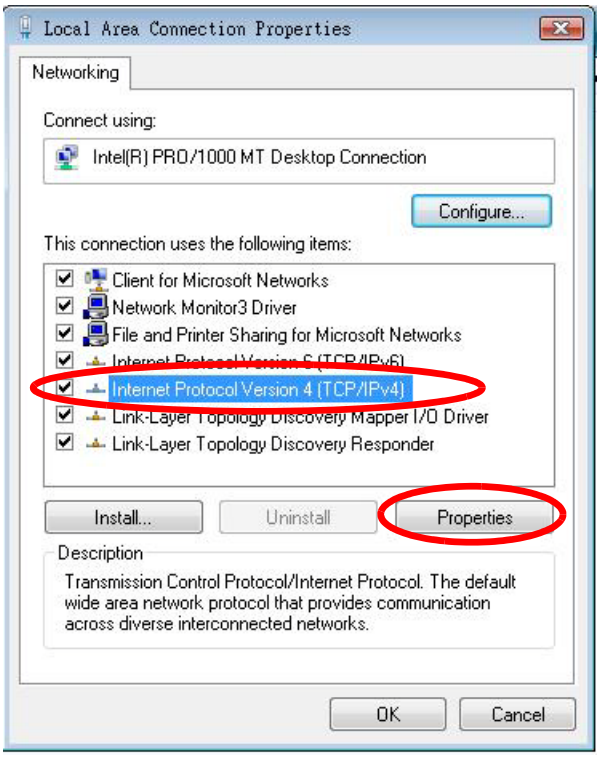



5 Right-click **Local Area Connection** and then select **Properties**.

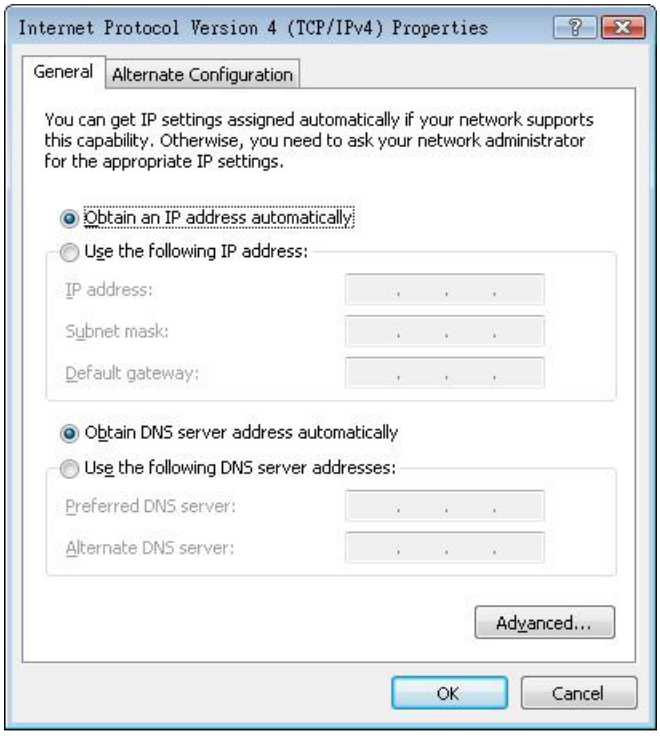



Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

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




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



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**.

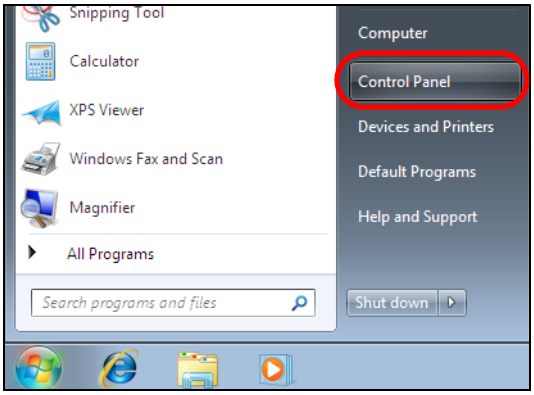
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

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.

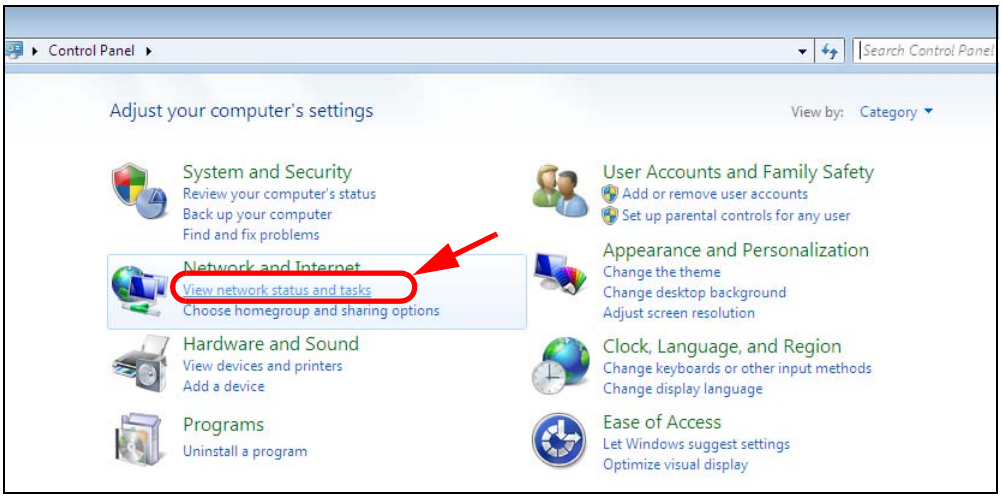
## Windows 7

This section shows screens from Windows 7 Enterprise.

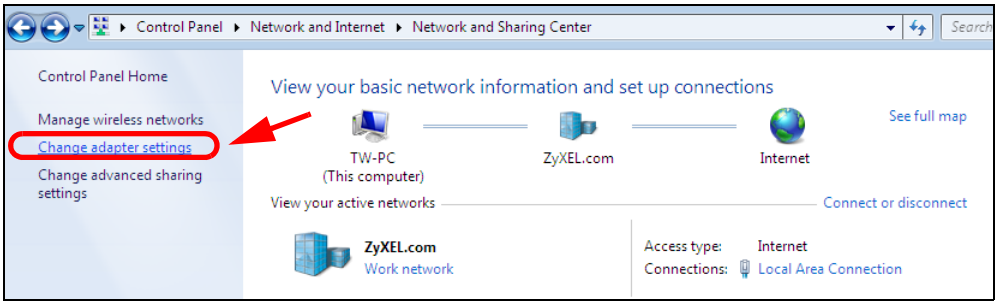
1 Click **Start** > **Control Panel**.



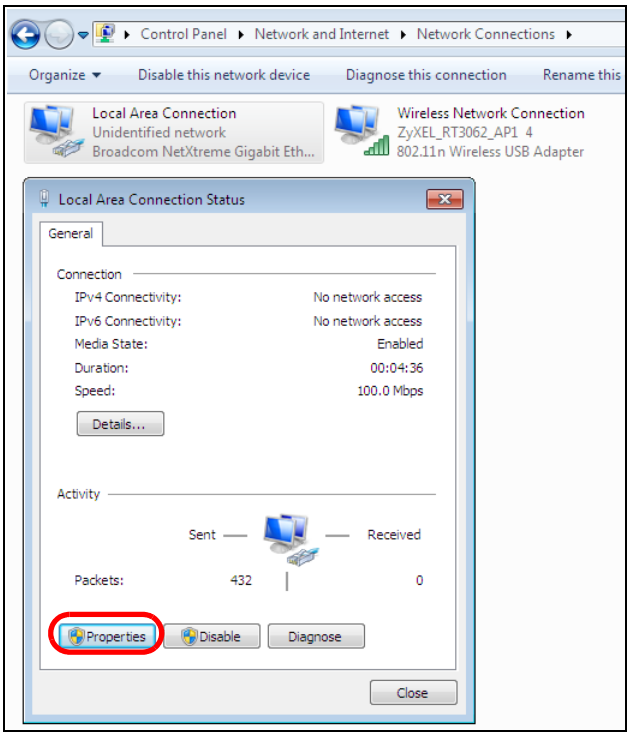

2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.




3 Click **Change adapter settings**.

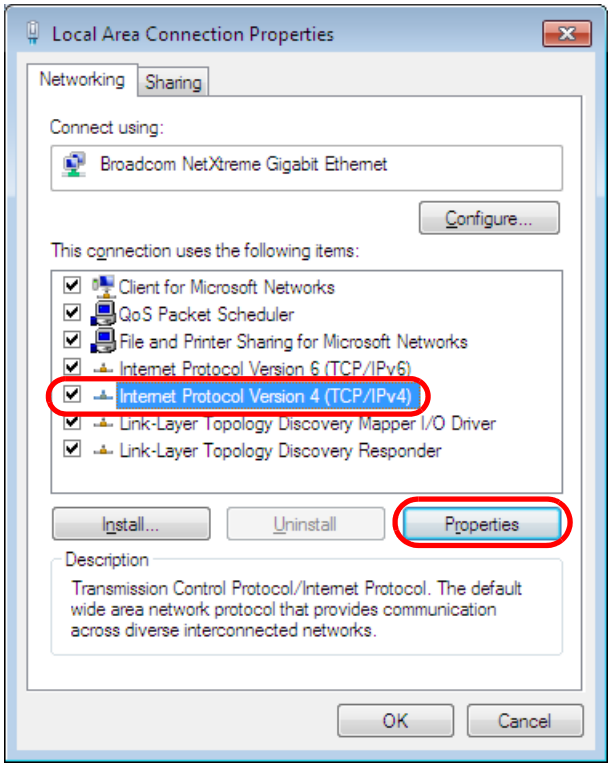



4 Double click **Local Area Connection** and then select **Properties**.

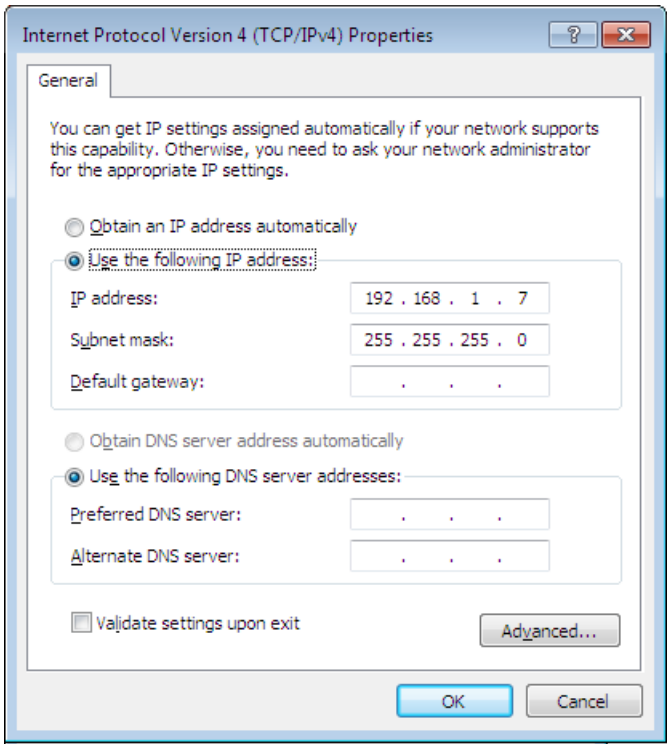


Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

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




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




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.

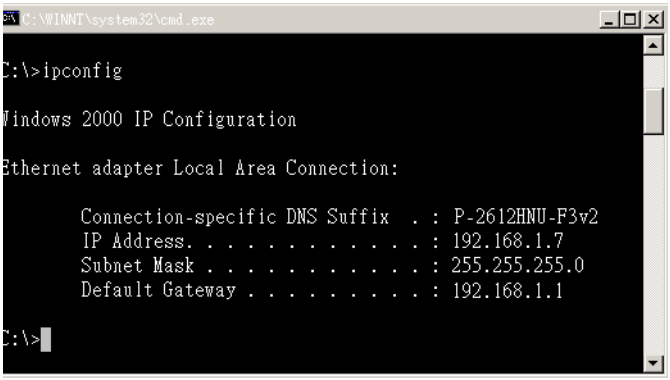
9 Click **OK** to close the **Local Area Connection Properties** window.

## Verifying Settings

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

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

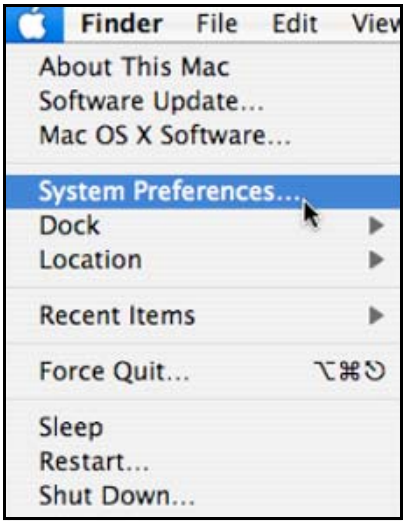
3 The IP settings are displayed as follows.




## Mac OS X: 10.3 and 10.4

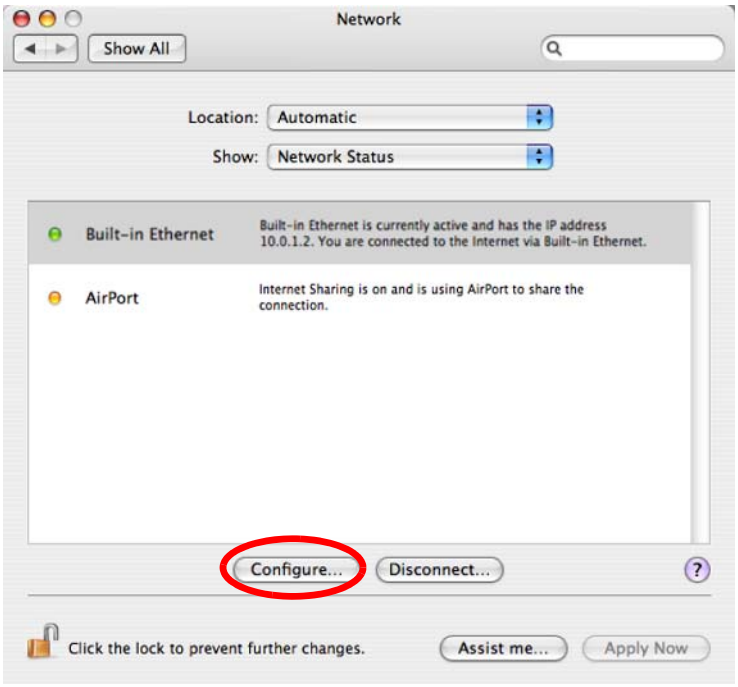
The screens in this section are from Mac OS X 10.4 but can also apply to 10.3.

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

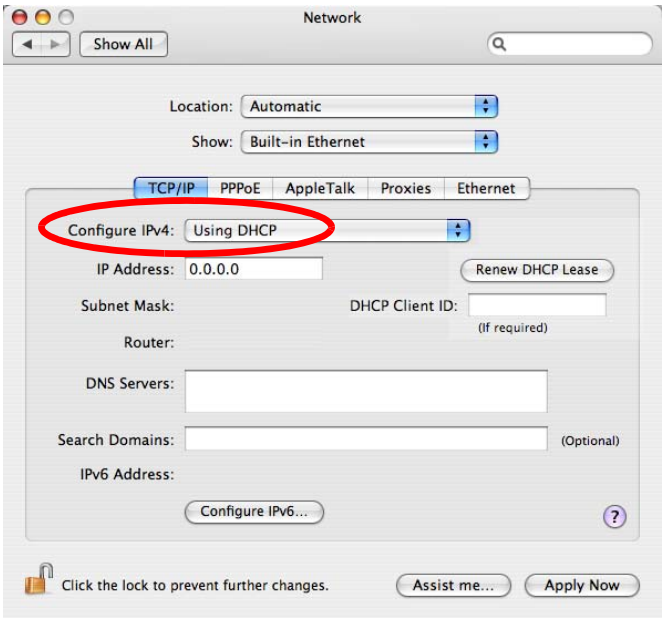



2 In the **System Preferences** window, click the **Network** icon.


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

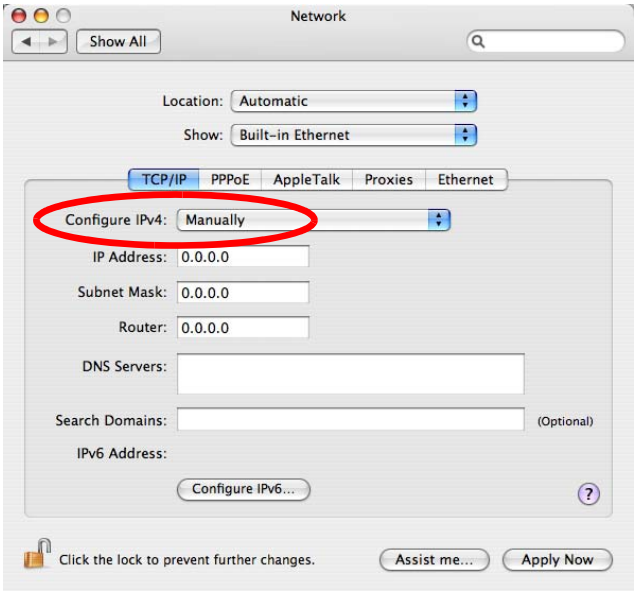



4 For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.




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.

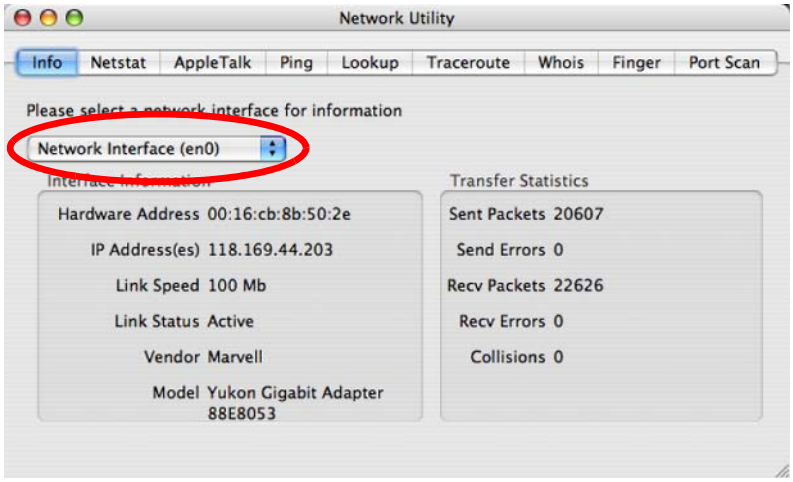



6 Click **Apply Now** and close the window.

## Verifying Settings

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

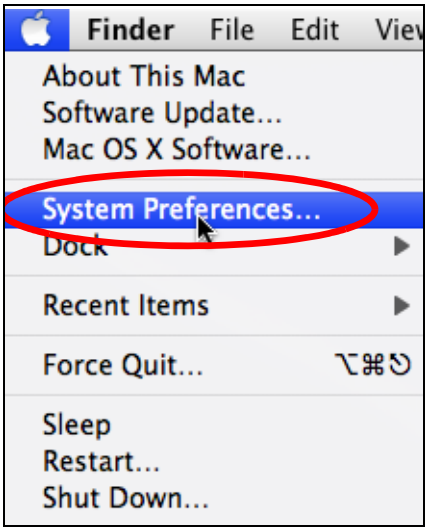
**Figure 132** Mac OS X 10.4: Network Utility




## Mac OS X: 10.5 and 10.6

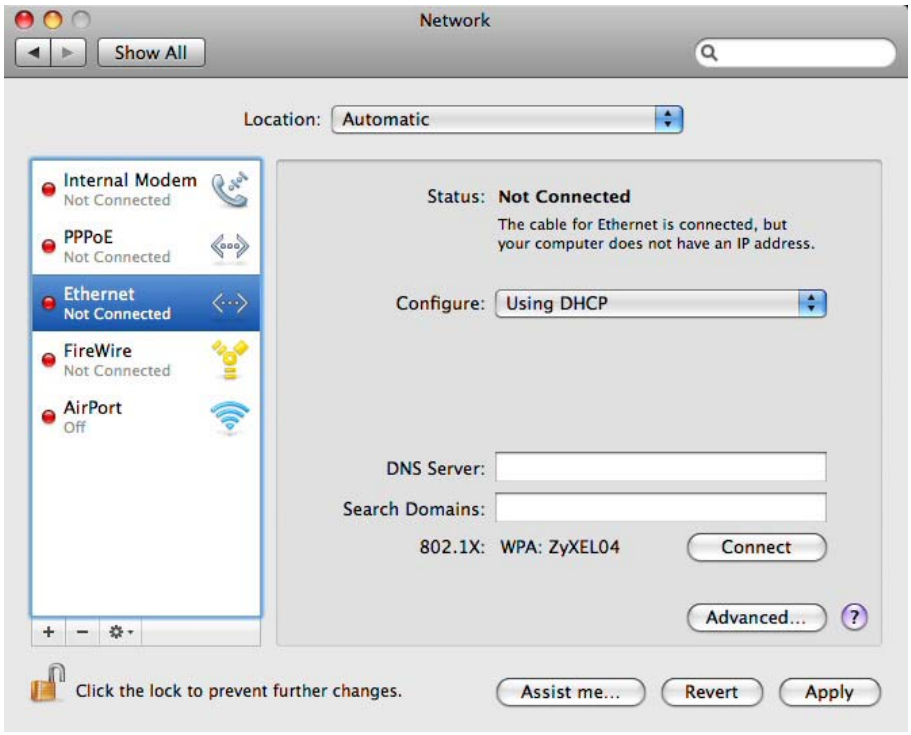
The screens in this section are from Mac OS X 10.5 but can also apply to 10.6.

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




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

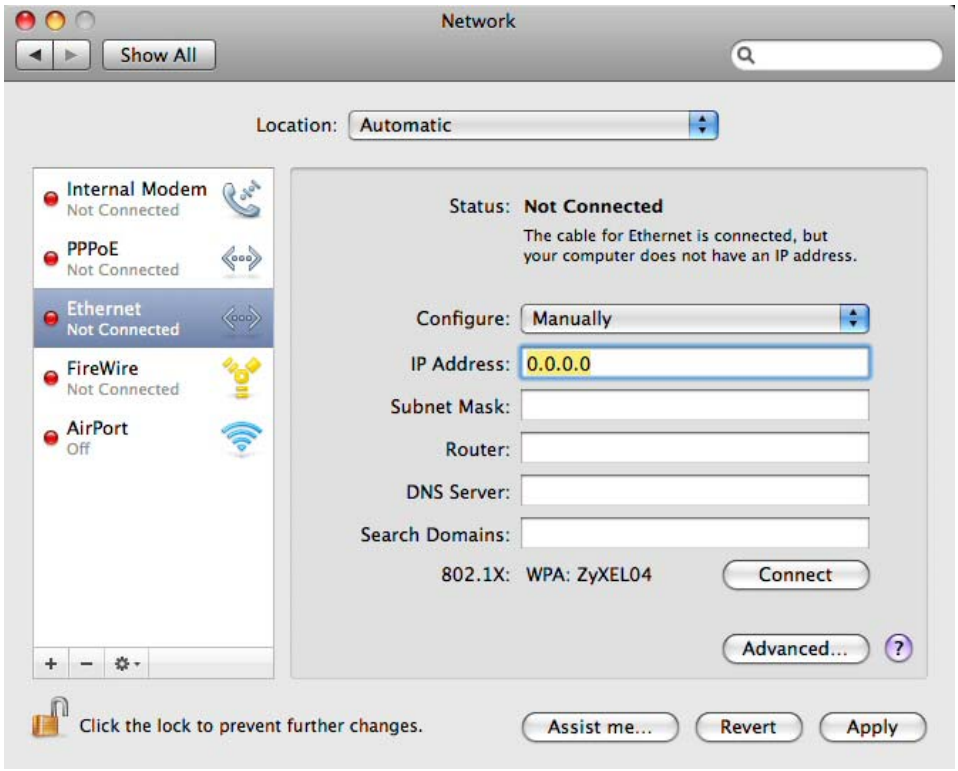

3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.




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 LTE3301.

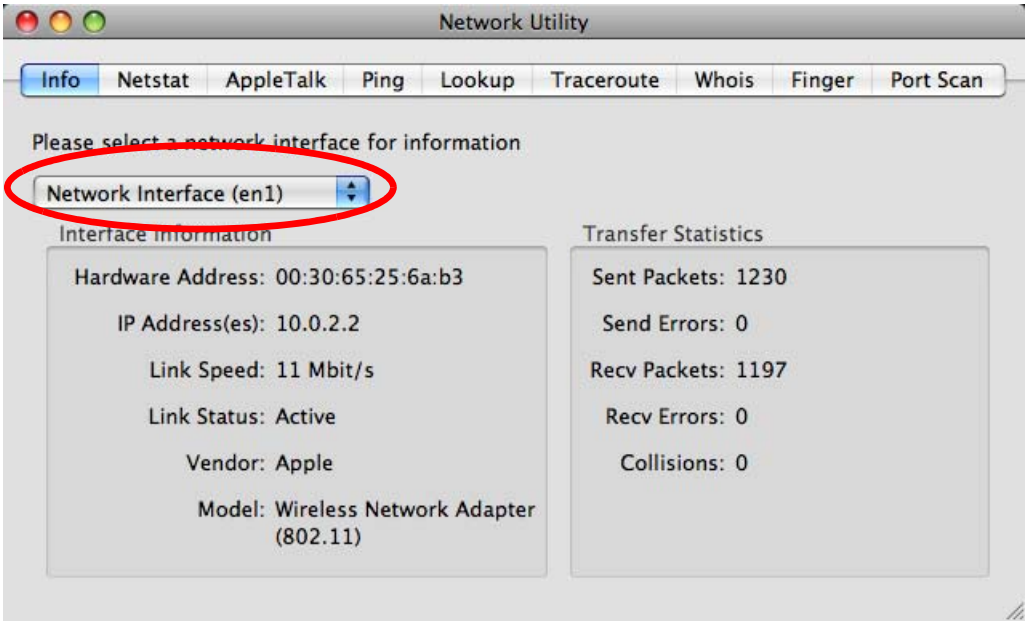



6 Click **Apply** and close the window.

## 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 133** Mac OS X 10.5: Network Utility



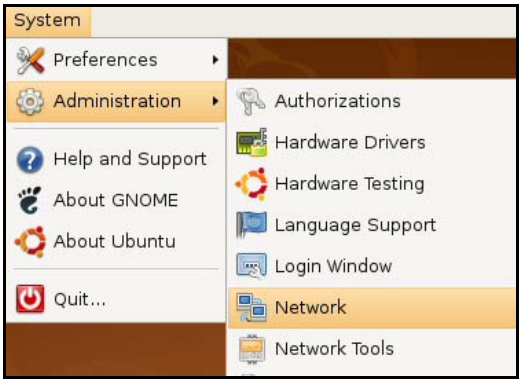

## Linux: Ubuntu 8 (GNOME)

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.

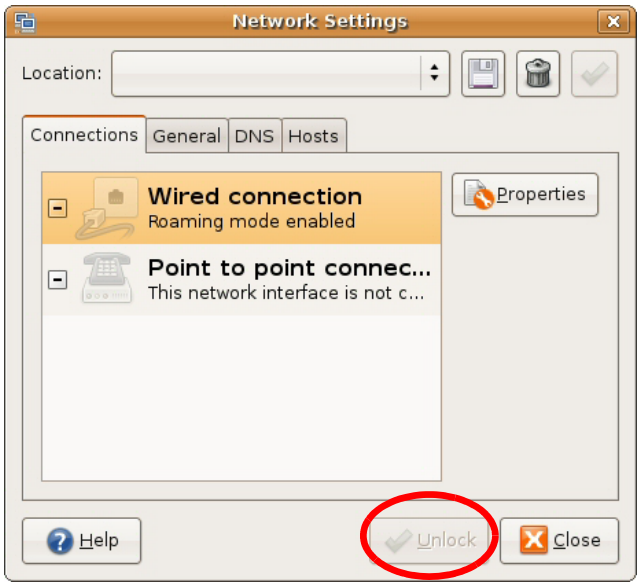
Note: Make sure you are logged in as the root administrator.

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

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

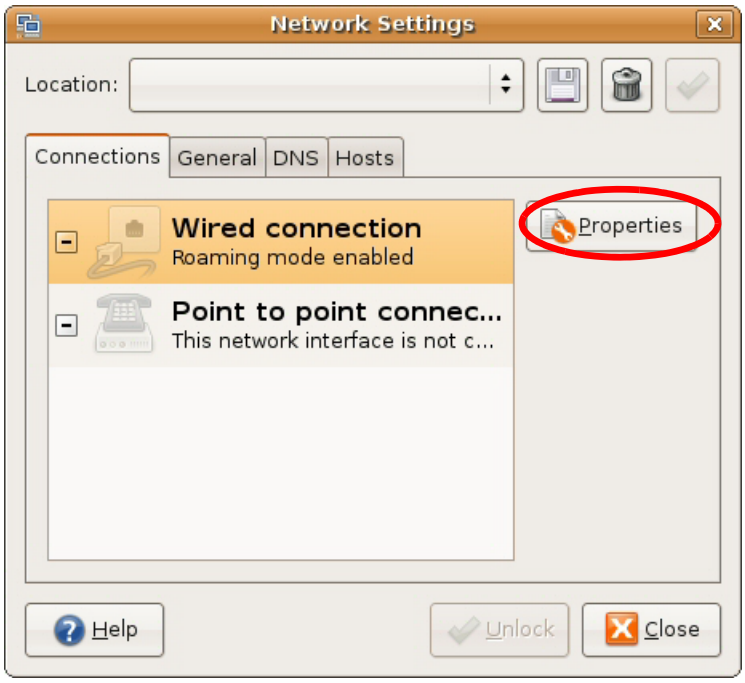



2 When the **Network Settings** window opens, click **Unlock** to open the **Authenticate** window. (By default, the **Unlock** button is greyed out until clicked.) You cannot make changes to your configuration unless you first enter your admin password.




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


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




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.

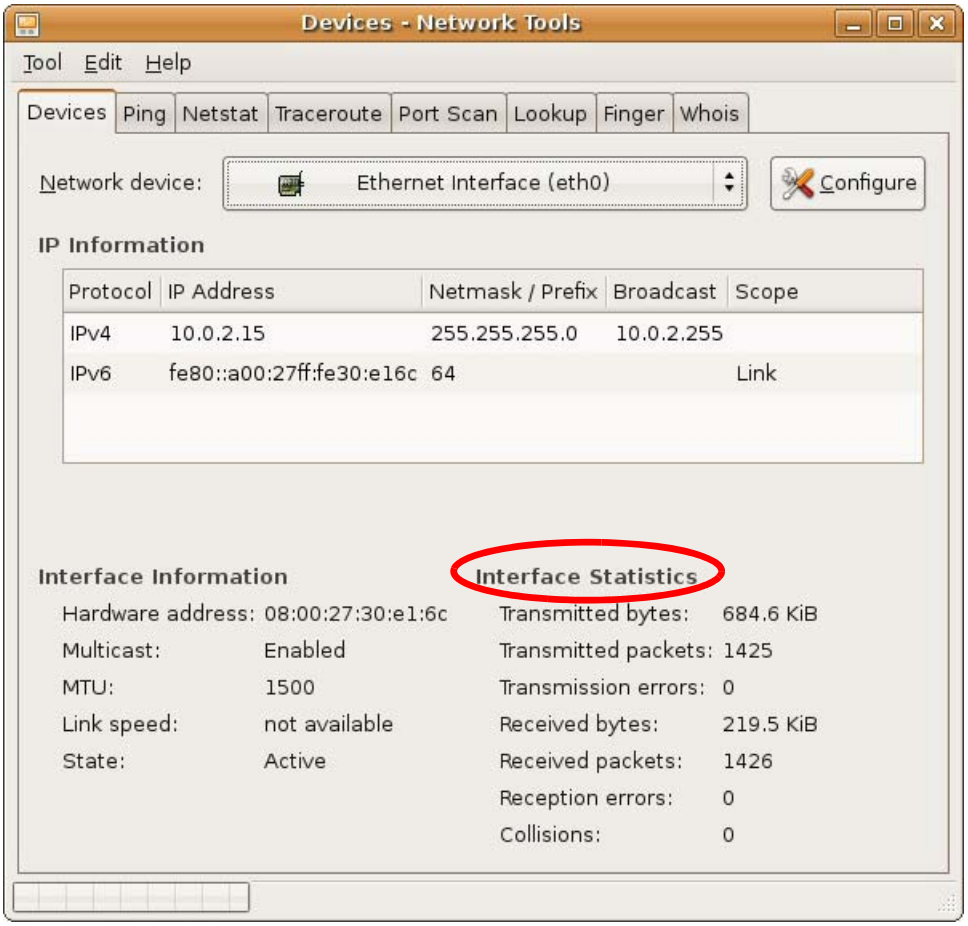
7 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Settings** window and then enter the DNS server information in the fields provided.


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 134** Ubuntu 8: Network Tools



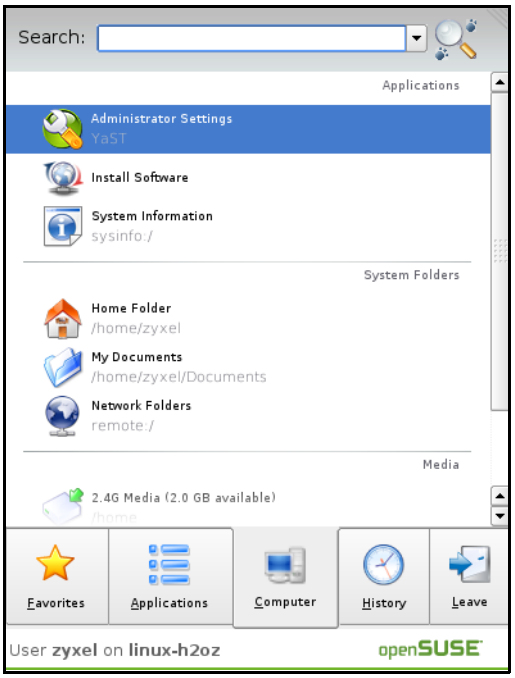

## Linux: openSUSE 10.3 (KDE)

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.

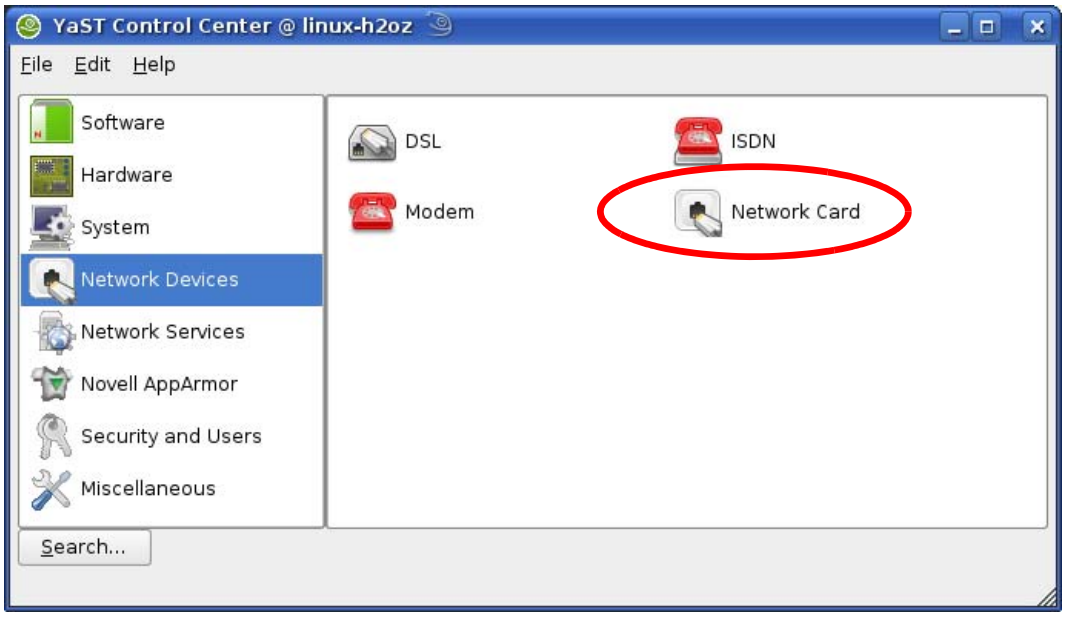
Follow the steps below to configure your computer IP address in the KDE:

1 Click **K Menu > Computer > Administrator Settings (YaST)**.

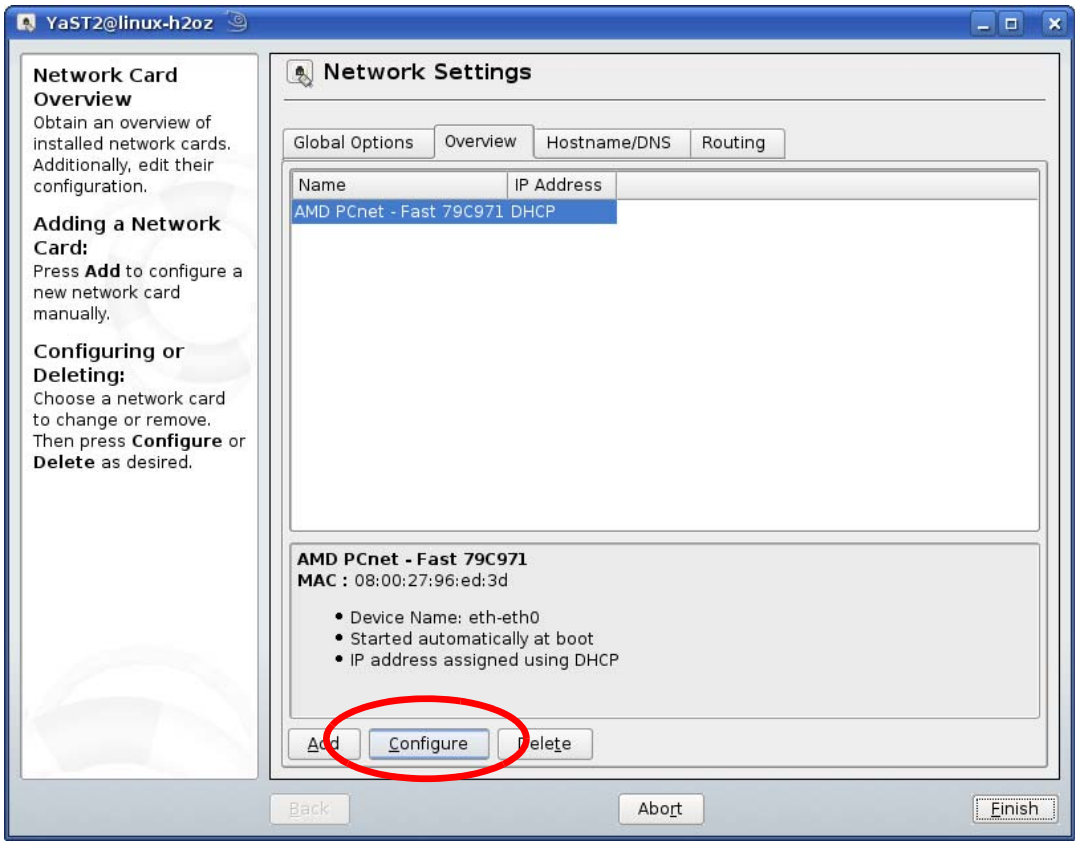



2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.


3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.

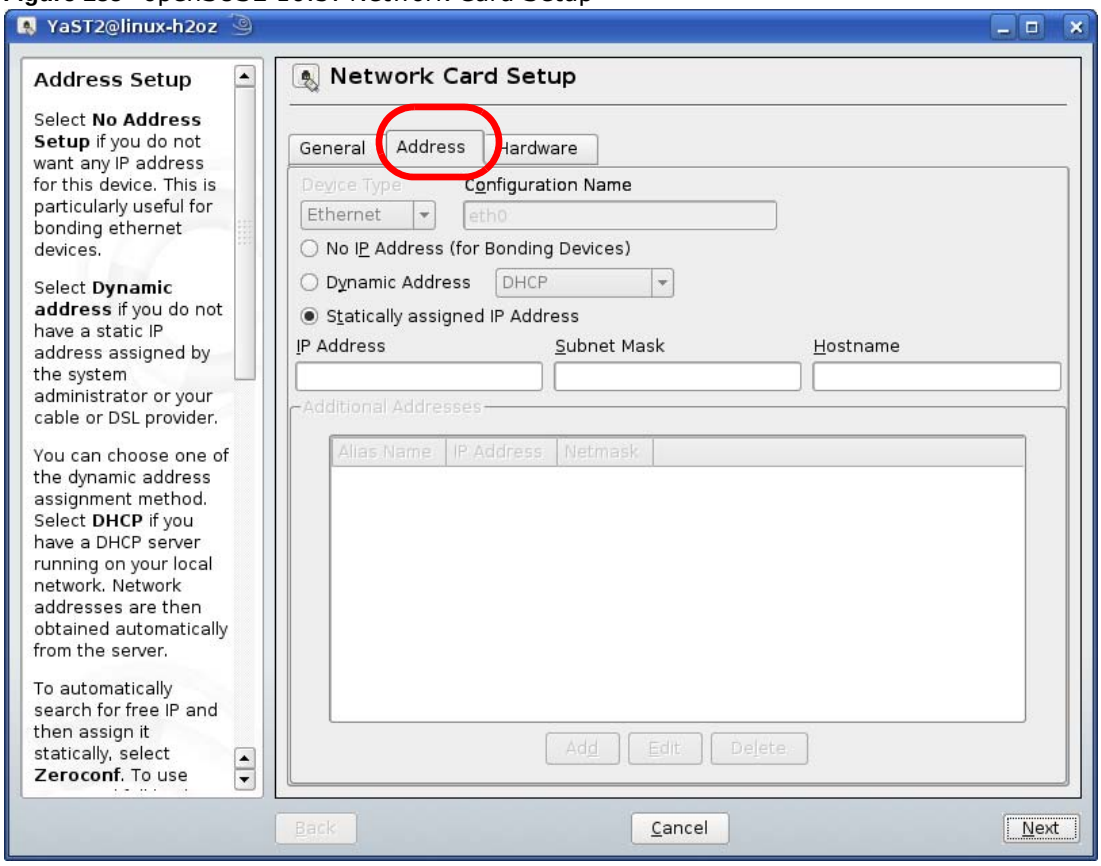



4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.




5 When the **Network Card Setup** window opens, click the **Address** tab

**Figure 135** openSUSE 10.3: Network Card Setup

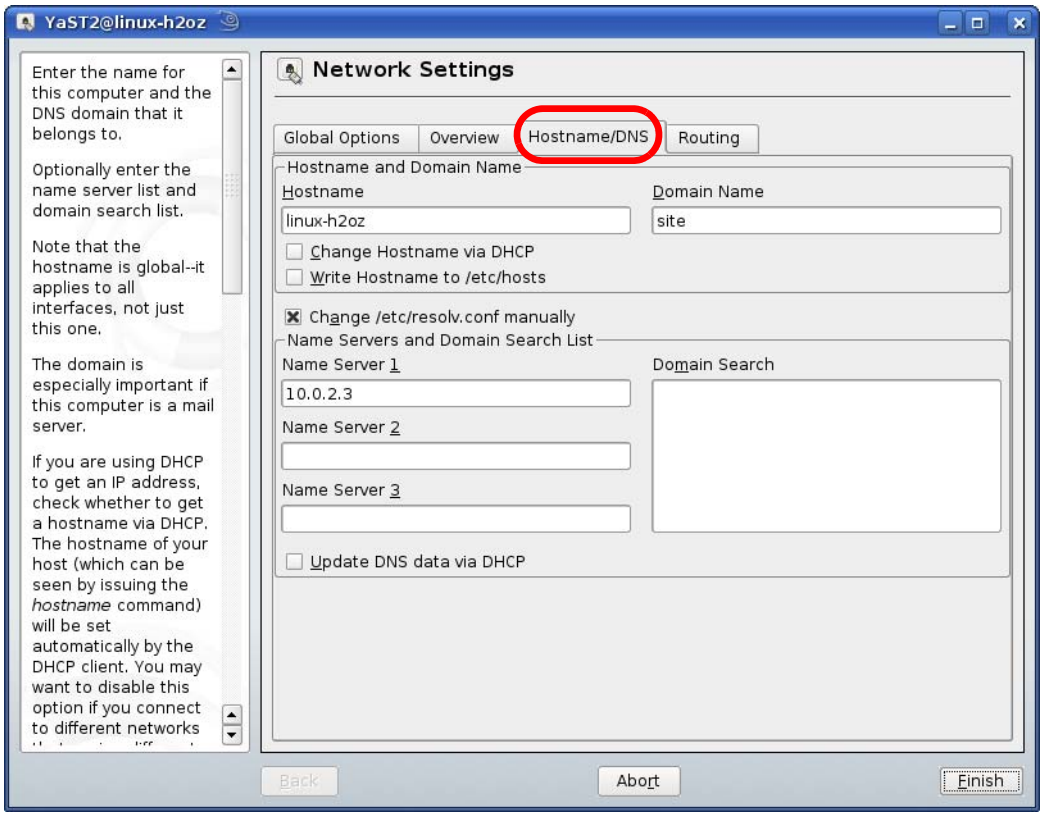



6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.

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.

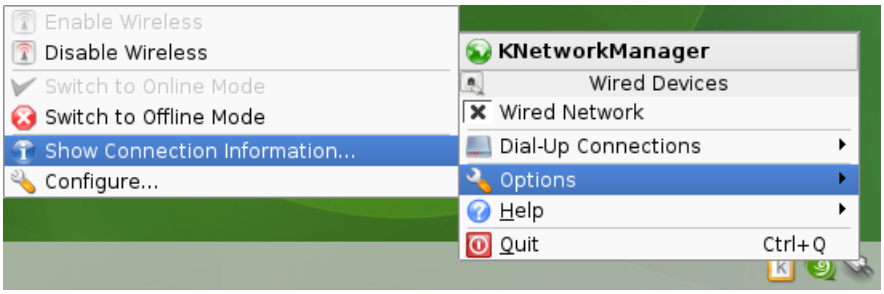



9 Click **Finish** to save your settings and close the window.

## Verifying Settings

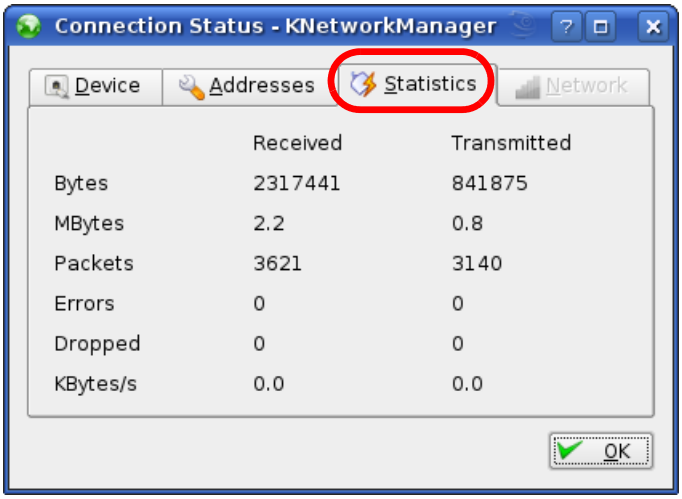
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

**Figure 136** 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 137** openSUSE: Connection Status - KNetwork Manager



# D

# 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 81** 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<br>UDP | 7648<br>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<br>TCP | 20<br>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. |

**Table 81** Commonly Used Services (continued)

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|---|---|---|---|
| HTTPS | TCP | 443 | HTTPS is a secured http session often used in e-commerce. |
| 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). |

**Table 81** Commonly Used Services (continued)

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|---|---|---|---|
| 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. |
| 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. |

E

# Legal Information

## Copyright

Copyright © 2016 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

### 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

ICAN ICES-3 (B)/NMB-3(B)

### 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 1999/5/EC (R&TTE Directive)

Compliance information for 2.4GHz and/or 5GHz wireless products relevant to the EU and other Countries following the EU Directive 1999/5/EC (R&TTE)

| | |
|---|---|
| Български (Bulgarian) | С настоящото ZyXEL декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 1999/5/ЕС. |
| 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 1999/5/CE. |
| Čeština (Czech) | ZyXEL tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/EC. |
| Dansk (Danish) | Undertegnede ZyXEL erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF. |
| Deutsch (German) | Hiermit erklärt ZyXEL, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EU befindet. |
| Eesti keel (Estonian) | Käesolevaga kinnitab ZyXEL seadme seadmed vastavust direktiivi 1999/5/EÜ 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 1999/5/ΕC. |
| English | Hereby, ZyXEL declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC. |
| Français (French) | Par la présente ZyXEL déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/EC. |
| Hrvatski (Croatian) | ZyXEL ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 1999/5/EC. |
| Íslenska (Icelandic) | Hér með lýsir, ZyXEL því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 1999/5/EC. |
| Italiano (Italian) | Con la presente ZyXEL dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE. |
| Latviešu valoda (Latvian) | Ar šo ZyXEL deklarē, ka iekārtas atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem. |
| Lietuvių kalba (Lithuanian) | Šiuo ZyXEL deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas. |
| Magyar (Hungarian) | Alulírott, ZyXEL nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EK irányelv egyéb elõírásainak. |
| Malti (Maltese) | Hawnhekk, ZyXEL, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC. |
| Nederlands (Dutch) | Hierbij verklaart ZyXEL dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EC. |
| Polski (Polish) | Niniejszym ZyXEL oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC. |
| Português (Portuguese) | ZyXEL declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/EC. |
| Română (Romanian) | Prin prezenta, ZyXEL declară că acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 1999/5/EC. |
| Slovenčina (Slovak) | ZyXEL týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/EC. |
| Slovenščina (Slovene) | ZyXEL izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/EC. |

| | |
|---|---|
| Suomi (Finnish) | ZyXEL vakuuttaa täten että laitteet tyyppinen laite on direktiivin 1999/5/EY 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 1999/5/EC. |
| Norsk (Norwegian) | Erklærer herved ZyXEL at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 1999/5/EF. |

This device is restricted to indoor use only when operating in the 5150 to 5350 MHz frequency range.

### National Restrictions

This product may be used in all EU countries (and other countries following the EU Directive 1999/5/EC) without any limitation except for the countries mentioned below:

Ce produit peut être utilisé dans tous les pays de l'UE (et dans tous les pays ayant transposés la directive 1999/5/CE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous:

Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttiva 1999/5/EC) senza nessuna limitazione, eccetto per i paesii menzionati di seguito:

Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der Richtlinie 1999/5/CE folgen) mit Außnahme der folgenden aufgeführten Staaten:

In the majority of the EU and other European countries, the 2.4GHz and 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 both the 2.4GHz and 5GHz wireless LANs.

The following countries have restrictions and/or requirements in addition to those given in the table labeled "*Overview of Regulatory Requirements for Wireless LANs*":.

Belgium

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.

Denmark

In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage.

I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.

Italy

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.

Latvia

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.

Notes:

1. Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 1999/5/EC 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 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.
- Do not obstruct the device ventilation slots, as insufficient airflow may harm your device.
- 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 < 12W, 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.

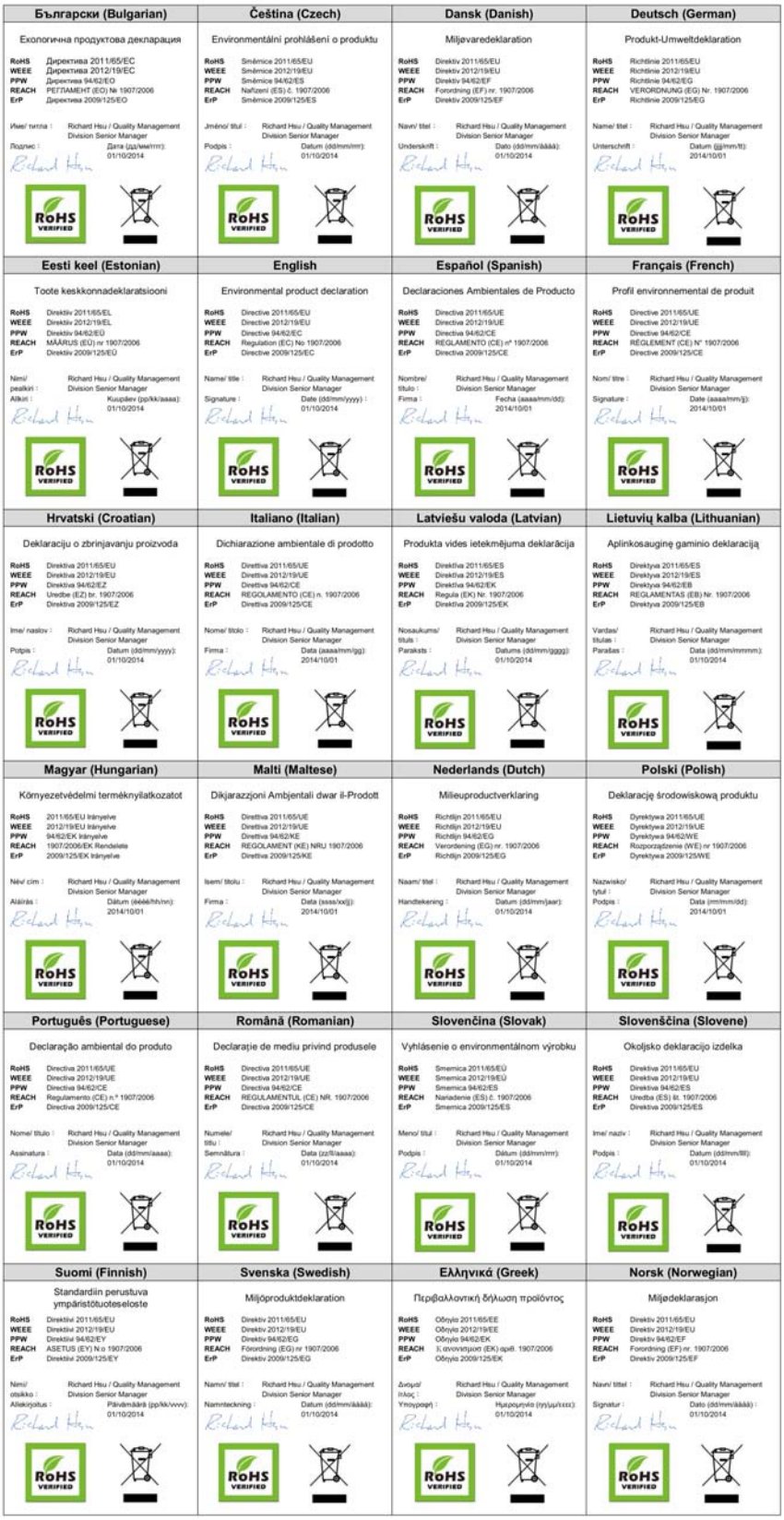
El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado 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.

## Environmental Product Declaration



**Български (Bulgarian)**

Екологична продуктова декларация

RoHS Директива 2011/65/EC
WEEE Директива 2012/19/EC
PPW Директива 94/62/EO
REACH РЕГЛАМЕНТ (ЕО) № 1907/2006
ErP Директива 2009/125/EO

Име/ титла : Richard Hsu / Quality Management Division Senior Manager
Подпис : Дата (дд/мм/гггг): 01/10/2014

**Čeština (Czech)**

Environmentální prohlášení o produktu

RoHS Směrnice 2011/65/EU
WEEE Směrnice 2012/19/EU
PPW Směrnice 94/62/ES
REACH Nařízení (ES) č. 1907/2006
ErP Směrnice 2009/125/ES

Jméno/ titul : Richard Hsu / Quality Management Division Senior Manager
Podpis : Datum (dd/mm/rrrr): 01/10/2014

**Dansk (Danish)**

Miljøvaredeklaration

RoHS Direktiv 2011/65/EU
WEEE Direktiv 2012/19/EU
PPW Direktiv 94/62/EF
REACH Forordning (EF) nr. 1907/2006
ErP Direktiv 2009/125/EF

Navn/ titel : Richard Hsu / Quality Management Division Senior Manager
Underskrift : Dato (dd/mm/åååå): 01/10/2014

**Deutsch (German)**

Produkt-Umweltdeklaration

RoHS Richtlinie 2011/65/EU
WEEE Richtlinie 2012/19/EU
PPW Richtlinie 94/62/EG
REACH VERORDNUNG (EG) Nr. 1907/2006
ErP Richtlinie 2009/125/EG

Name/ titel : Richard Hsu / Quality Management Division Senior Manager
Unterschrift : Datum (tt/mm/jj): 2014/10/01

**Eesti keel (Estonian)**

Toote keskkonnadeklaratsiooni

RoHS Direktiiv 2011/65/EL
WEEE Direktiiv 2012/19/EL
PPW Direktiiv 94/62/EÜ
REACH MÄÄRUS (EÜ) nr 1907/2006
ErP Direktiiv 2009/125/EÜ

Nimi/ ametikoht : Richard Hsu / Quality Management Division Senior Manager
Allkiri : Kuupäev (pp/kk/aaaa): 01/10/2014

**English**

Environmental product declaration

RoHS Directive 2011/65/EU
WEEE Directive 2012/19/EU
PPW Directive 94/62/EC
REACH Regulation (EC) No 1907/2006
ErP Directive 2009/125/EC

Name/ title : Richard Hsu / Quality Management Division Senior Manager
Signature : Date (dd/mm/yyyy) : 01/10/2014

**Español (Spanish)**

Declaraciones Ambientales de Producto

RoHS Directiva 2011/65/UE
WEEE Directiva 2012/19/UE
PPW Directiva 94/62/CE
REACH REGLAMENTO (CE) nº 1907/2006
ErP Directiva 2009/125/CE

Nombre/ título : Richard Hsu / Quality Management Division Senior Manager
Firma : Fecha (aaaa/mm/dd): 2014/10/01

**Français (French)**

Profil environnemental de produit

RoHS Directive 2011/65/UE
WEEE Directive 2012/19/UE
PPW Directive 94/62/CE
REACH RÈGLEMENT (CE) N° 1907/2006
ErP Directive 2009/125/CE

Nom/ titre : Richard Hsu / Quality Management Division Senior Manager
Signature : Date (aaaa/mm/jj): 2014/10/01

**Hrvatski (Croatian)**

Deklaraciju o zbrinjavanju proizvoda

RoHS Direktiva 2011/65/EU
WEEE Direktiva 2012/19/EU
PPW Direktiva 94/62/EZ
REACH Uredbe (EZ) br. 1907/2006
ErP Direktiva 2009/125/EZ

Ime/ naslov : Richard Hsu / Quality Management Division Senior Manager
Potpis : Datum (dd/mm/yyyy): 01/10/2014

**Italiano (Italian)**

Dichiarazione ambientale di prodotto

RoHS Direttiva 2011/65/UE
WEEE Direttiva 2012/19/UE
PPW Direttiva 94/62/CE
REACH REGOLAMENTO (CE) n. 1907/2006
ErP Direttiva 2009/125/CE

Nome/ titolo : Richard Hsu / Quality Management Division Senior Manager
Firma : Data (aaaa/mm/gg): 2014/10/01

**Latviešu valoda (Latvian)**

Produkta vides ietekmējuma deklarācija

RoHS Direktīva 2011/65/ES
WEEE Direktīva 2012/19/ES
PPW Direktīva 94/62/EK
REACH Regula (EK) Nr. 1907/2006
ErP Direktīva 2009/125/EK

Nosaukums/ tituls : Richard Hsu / Quality Management Division Senior Manager
Paraksts : Datums (dd/mm/gggg): 01/10/2014

**Lietuvių kalba (Lithuanian)**

Aplinkosauginę gaminio deklaraciją

RoHS Direktyva 2011/65/ES
WEEE Direktyva 2012/19/ES
PPW Direktyva 94/62/EB
REACH REGLAMENTAS (EB) Nr. 1907/2006
ErP Direktyva 2009/125/EB

Vardas/ titulas : Richard Hsu / Quality Management Division Senior Manager
Parašas : Data (dd/mm/mmmm): 01/10/2014

**Magyar (Hungarian)**

Környezetvédelmi terméknyilatkozatot

RoHS 2011/65/EU irányelve
WEEE 2012/19/EU irányelve
PPW 94/62/EK irányelve
REACH 1907/2006/EK Rendelete
ErP 2009/125/EK irányelve

Név/ cím : Richard Hsu / Quality Management Division Senior Manager
Aláírás : Dátum (éééé/hh/nn): 2014/10/01

**Malti (Maltese)**

Dikjarazzjoni Ambjentali dwar il-Prodott

RoHS Direttiva 2011/65/UE
WEEE Direttiva 2012/19/UE
PPW Direttiva 94/62/KE
REACH REGOLAMENT (KE) NRU 1907/2006
ErP Direttiva 2009/125/KE

Isem/ titolu : Richard Hsu / Quality Management Division Senior Manager
Firma : Data (sssa/xx/jj): 2014/10/01

**Nederlands (Dutch)**

Milieuproductverklaring

RoHS Richtlijn 2011/65/EU
WEEE Richtlijn 2012/19/EU
PPW Richtlijn 94/62/EG
REACH Verordening (EG) nr. 1907/2006
ErP Richtlijn 2009/125/EG

Naam/ titel : Richard Hsu / Quality Management Division Senior Manager
Handtekening : Datum (dd/mm/jaar): 01/10/2014

**Polski (Polish)**

Deklarację środowiskową produktu

RoHS Dyrektywa 2011/65/UE
WEEE Dyrektywa 2012/19/UE
PPW Dyrektywa 94/62/WE
REACH Rozporządzenie (WE) nr 1907/2006
ErP Dyrektywa 2009/125/WE

Nazwisko/ tytuł : Richard Hsu / Quality Management Division Senior Manager
Podpis : Data (rr/mm/dd): 2014/10/01

**Português (Portuguese)**

Declaração ambiental do produto

RoHS Directiva 2011/65/UE
WEEE Directiva 2012/19/UE
PPW Directiva 94/62/CE
REACH Regulamento (CE) n.º 1907/2006
ErP Directiva 2009/125/CE

Nome/ título : Richard Hsu / Quality Management Division Senior Manager
Assinatura : Data (dd/mm/aaaa): 01/10/2014

**Română (Romanian)**

Declarație de mediu privind produsele

RoHS Directiva 2011/65/UE
WEEE Directiva 2012/19/UE
PPW Directiva 94/62/CE
REACH REGLAMENTUL (CE) NR. 1907/2006
ErP Directiva 2009/125/CE

Numele/ titlu : Richard Hsu / Quality Management Division Senior Manager
Semnătura : Data (zz/ll/aaaa): 01/10/2014

**Slovenčina (Slovak)**

Vyhlásenie o environmentálnom výrobku

RoHS Smernica 2011/65/EÚ
WEEE Smernica 2012/19/EÚ
PPW Smernica 94/62/ES
REACH Nariadenie (ES) č. 1907/2006
ErP Smernica 2009/125/ES

Meno/ titul : Richard Hsu / Quality Management Division Senior Manager
Podpis : Dátum (dd/mm/rrrr): 01/10/2014

**Slovenščina (Slovene)**

Okoljsko deklaracijo izdelka

RoHS Direktiva 2011/65/EU
WEEE Direktiva 2012/19/EU
PPW Direktiva 94/62/ES
REACH Uredba (ES) št. 1907/2006
ErP Direktiva 2009/125/ES

Ime/ naziv : Richard Hsu / Quality Management Division Senior Manager
Podpis : Datum (dd/mm/ll): 01/10/2014

**Suomi (Finnish)**

Standardiin perustuva ympäristötuoteseloste

RoHS Direktiivi 2011/65/EU
WEEE Direktiivi 2012/19/EU
PPW Direktiivi 94/62/EY
REACH ASETUS (EY) N:o 1907/2006
ErP Direktiivi 2009/125/EY

Nimi/ otsikko : Richard Hsu / Quality Management Division Senior Manager
Allekirjoitus : Päivämäärä (pp/kk/vvvv): 01/10/2014

**Svenska (Swedish)**

Miljöproduktdeklaration

RoHS Direktiv 2011/65/EU
WEEE Direktiv 2012/19/EU
PPW Direktiv 94/62/EG
REACH Förordning (EG) nr 1907/2006
ErP Direktiv 2009/125/EG

Namn/ titel : Richard Hsu / Quality Management Division Senior Manager
Namnteckning : Datum (dd/mm/åååå): 01/10/2014

**Ελληνικά (Greek)**

Περιβαλλοντική δήλωση προϊόντος

RoHS Οδηγία 2011/65/ΕΕ
WEEE Οδηγία 2012/19/ΕΕ
PPW Οδηγία 94/62/ΕΚ
REACH Κ ανανησμοσ (ΕΚ) αρθ. 1907/2006
ErP Οδηγία 2009/125/ΕΚ

Όνομα/ Τίτλος : Richard Hsu / Quality Management Division Senior Manager
Υπογραφή : Ημερομηνία (ηη/μμ/εεεε): 01/10/2014

**Norsk (Norwegian)**

Miljødeklarasjon

RoHS Direktiv 2011/65/EU
WEEE Direktiv 2012/19/EU
PPW Direktiv 94/62/EF
REACH Forordning (EF) nr. 1907/2006
ErP Direktiv 2009/125/EF

Navn/ tittel : Richard Hsu / Quality Management Division Senior Manager
Signatur : Dato (dd/mm/åååå) : 01/10/2014

## 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。

## Viewing Certifications

Go to http://www.zyxel.com to view this product's documentation and certifications.

## ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized ZyXEL local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

### Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

## Registration

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

## Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.

# Index

## A



## B



## C



## D



## E

## F



## G



## I



## J



## L



## M



## N

## O



## P



## Q



## R



## S

## T



## U



## V



## W