# LTE6101

*LTE Outdoor Gateway*

# User's Guide



## Default Login Details

| | |
|---|---|
| Web Address | http://192.168.1.1 |
| Admin's User Name and Password | admin / 1234 |
| Guest's User Name and Password | user / 1234 |

Edition 1, 1/2013

ZyXEL

www.zyxel.com

**IMPORTANT!**

Graphics in this book may differ slightly from the product due to differences in operating systems, operating system versions, or if you installed updated firmware/software for your device. 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 LTE Device and access the Web Configurator wizards. (See the wizard real time help for information on configuring each screen.) It also contains a connection diagram and package contents list.

Note: It is recommended you use the Web Configurator to configure the LTE Device.

# Contents Overview

**User's Guide ..... 11**

Introduction ..... 13
Introducing the Web Configurator ..... 19

**Technical Reference ..... 25**

Connection Status and System Info ..... 27
Broadband ..... 33
Wireless ..... 41
Home Networking ..... 67
Routing ..... 73
Quality of Service (QoS) ..... 77
Network Address Translation (NAT) ..... 87
Dynamic DNS ..... 95
Firewall ..... 97
MAC Filter ..... 107
Parental Control ..... 109
VPN ..... 113
Logs ..... 127
Traffic Status ..... 129
User Account ..... 133
Remote MGMT ..... 135
System ..... 137
Time Setting ..... 139
Log Setting ..... 141
Firmware Upgrade ..... 143
Backup/Restore ..... 145
Diagnostic ..... 149
Troubleshooting ..... 151

# Table of Contents

**Contents Overview** ..... **3**

**Table of Contents** ..... **5**

**Part I: User's Guide** ..... **11**

**Chapter 1**
**Introduction** ..... **13**

1.1 Overview ..... 13
1.2 Applications for the LTE Device ..... 13
1.2.1 Internet Access ..... 13
1.2.2 Wireless Connection ..... 13
1.3 The WLAN Button ..... 14
1.4 Ways to Manage the LTE Device ..... 15
1.5 Good Habits for Managing the LTE Device ..... 15
1.6 LEDs (Lights) ..... 15
1.7 The RESET Button ..... 16

**Chapter 2**
**Introducing the Web Configurator** ..... **19**

2.1 Overview ..... 19
2.1.1 Accessing the Web Configurator ..... 19
2.2 The Web Configurator Layout ..... 21
2.2.1 Title Bar ..... 21
2.2.2 Main Window ..... 22
2.2.3 Traffic Status ..... 22
2.2.4 User Account ..... 22
2.2.5 Navigation Panel ..... 23

**Part II: Technical Reference** ..... **25**

**Chapter 3**
**Connection Status and System Info** ..... **27**

3.1 Overview ..... 27
3.2 The Connection Status Screen ..... 27
3.3 The System Info Screen ..... 29

**Chapter 4**
**Broadband ..... 33**

4.1 Overview ..... 33
4.1.1 What You Can Do in this Chapter ..... 33
4.1.2 What You Need to Know ..... 33
4.1.3 Before You Begin ..... 34
4.2 The Broadband Screen ..... 34
4.2.1 Edit Internet Connection ..... 35
4.3 The SIM Screen ..... 36
4.3.1 PUK Code Screen ..... 36
4.4 Technical Reference ..... 37

**Chapter 5**
**Wireless ..... 41**

5.1 Overview ..... 41
5.1.1 What You Can Do in this Chapter ..... 41
5.1.2 Wireless Network Overview ..... 41
5.1.3 Before You Begin ..... 43
5.2 The Wireless General Screen ..... 43
5.2.1 No Security ..... 45
5.2.2 Basic (Static WEP/Shared WEP Encryption) ..... 45
5.2.3 More Secure (WPA(2)-PSK) ..... 47
5.2.4 WPA(2) Authentication ..... 48
5.3 The More AP Screen ..... 49
5.3.1 Edit More AP ..... 50
5.4 The WPS Screen ..... 51
5.5 The WMM Screen ..... 52
5.6 Scheduling Screen ..... 54
5.7 Technical Reference ..... 54
5.7.1 Additional Wireless Terms ..... 55
5.7.2 Wireless Security Overview ..... 55
5.7.3 Signal Problems ..... 57
5.7.4 BSS ..... 58
5.7.5 MBSSID ..... 58
5.7.6 WiFi Protected Setup (WPS) ..... 59

**Chapter 6**
**Home Networking ..... 67**

6.1 Overview ..... 67
6.1.1 What You Can Do in this Chapter ..... 67
6.1.2 What You Need To Know ..... 67
6.2 The LAN Setup Screen ..... 69
6.3 The Static DHCP Screen ..... 70

6.3.1 Before You Begin ..... 70
6.4 The UPnP Screen ..... 71

**Chapter 7**
**Routing ..... 73**

7.1 Overview ..... 73
7.2 Configuring Static Route ..... 74
7.2.1 Add/Edit Static Route ..... 75

**Chapter 8**
**Quality of Service (QoS) ..... 77**

8.1 Overview ..... 77
8.1.1 What You Can Do in this Chapter ..... 77
8.1.2 What You Need to Know ..... 77
8.2 The QoS General Screen ..... 78
8.3 The Queue Setup Screen ..... 79
8.3.1 Add/Edit a QoS Queue ..... 80
8.4 The Class Setup Screen ..... 80
8.4.1 Add/Edit QoS Class ..... 82
8.5 The QoS Monitor Screen ..... 84
8.6 QoS Technical Reference ..... 85
8.6.1 DiffServ ..... 85

**Chapter 9**
**Network Address Translation (NAT) ..... 87**

9.1 Overview ..... 87
9.1.1 What You Can Do in this Chapter ..... 87
9.1.2 What You Need To Know ..... 87
9.2 The Port Forwarding Screen ..... 88
9.2.1 The Port Forwarding Screen ..... 89
9.2.2 The Port Forwarding Edit Screen ..... 90
9.3 The DMZ Screen ..... 91
9.4 The Sessions Screen ..... 91
9.5 Technical Reference ..... 92
9.5.1 NAT Definitions ..... 92
9.5.2 What NAT Does ..... 92
9.5.3 How NAT Works ..... 93

**Chapter 10**
**Dynamic DNS ..... 95**

10.1 Overview ..... 95
10.1.1 What You Need To Know ..... 95
10.2 The Dynamic DNS Screen ..... 96

**Chapter 11**
**Firewall ..... 97**

11.1 Overview ..... 97
11.1.1 What You Can Do in this Chapter ..... 97
11.1.2 What You Need to Know ..... 98
11.2 The General Screen ..... 99
11.3 The Services Screen ..... 100
11.3.1 The Add New Services Entry Screen ..... 100
11.4 The Access Control Screen ..... 101
11.4.1 The Add New ACL Rule/Edit Screen ..... 102
11.5 The DoS Screen ..... 103
11.6 Firewall Technical Reference ..... 104
11.6.1 Guidelines For Enhancing Security With Your Firewall ..... 104
11.6.2 Security Considerations ..... 104

**Chapter 12**
**MAC Filter ..... 107**

12.1 Overview ..... 107
12.1.1 What You Need to Know ..... 107
12.2 The MAC Filter Screen ..... 107

**Chapter 13**
**Parental Control ..... 109**

13.1 Overview ..... 109
13.2 The Parental Control Screen ..... 109
13.2.1 Add/Edit a Parental Control Rule ..... 110

**Chapter 14**
**VPN ..... 113**

14.1 Overview ..... 113
14.2 IPSec VPN ..... 113
14.2.1 The General Screen ..... 113
14.2.2 IPSec VPN: Add ..... 115
14.2.3 The Monitor Screen ..... 119
14.3 Technical Reference ..... 120
14.3.1 IPSec Architecture ..... 120
14.3.2 Encapsulation ..... 121
14.3.3 IKE Phases ..... 122
14.3.4 Negotiation Mode ..... 122
14.3.5 IPSec and NAT ..... 123
14.3.6 VPN, NAT, and NAT Traversal ..... 123
14.3.7 ID Type and Content ..... 124
14.3.8 Pre-Shared Key ..... 125

14.3.9 Diffie-Hellman (DH) Key Groups ..... 126

**Chapter 15**
**Logs ..... 127**

15.1 Overview ..... 127
15.1.1 What You Can Do in this Chapter ..... 127
15.1.2 What You Need To Know ..... 127
15.2 The System Log Screen ..... 128

**Chapter 16**
**Traffic Status ..... 129**

16.1 Overview ..... 129
16.1.1 What You Can Do in this Chapter ..... 129
16.2 The WAN Status Screen ..... 129
16.3 The LAN Status Screen ..... 130
16.4 The NAT Status Screen ..... 131

**Chapter 17**
**User Account ..... 133**

17.1 Overview ..... 133
17.2 The User Account Screen ..... 133

**Chapter 18**
**Remote MGMT ..... 135**

18.1 Overview ..... 135
18.1.1 What You Need to Know ..... 135
18.2 The Remote MGMT Screen ..... 135

**Chapter 19**
**System ..... 137**

19.1 Overview ..... 137
19.1.1 What You Need to Know ..... 137
19.2 The System Screen ..... 137

**Chapter 20**
**Time Setting ..... 139**

20.1 Overview ..... 139
20.2 The Time Setting Screen ..... 139

**Chapter 21**
**Log Setting ..... 141**

21.1 Overview ..... 141
21.2 The Log Setting Screen ..... 141

**Chapter 22**
**Firmware Upgrade ..... 143**

22.1 Overview ..... 143
22.2 The Firmware Upgrade Screen ..... 143

**Chapter 23**
**Backup/Restore ..... 145**

23.1 Overview ..... 145
23.2 The Backup/Restore Screen ..... 145
23.3 The Reboot Screen ..... 147

**Chapter 24**
**Diagnostic ..... 149**

24.1 Overview ..... 149
24.2 The Ping/TraceRoute Screen ..... 149

**Chapter 25**
**Troubleshooting ..... 151**

25.1 Overview ..... 151
25.2 Power, Hardware Connections, and LEDs ..... 151
25.3 LTE Device Access and Login ..... 152
25.4 Internet Access ..... 153
25.5 Wireless Internet Access ..... 154
25.6 UPnP ..... 155

Appendix A IP Addresses and Subnetting ..... 157

Appendix B Setting Up Your Computer's IP Address ..... 167

Appendix C Pop-up Windows, JavaScript and Java Permissions ..... 197

Appendix D Common Services ..... 207

Appendix E Legal Information ..... 211

**Index ..... 215**

# PART I
# User's Guide

# 1 Introduction

## 1.1 Overview

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

See the chapter on product specifications for a full list of features.

## 1.2 Applications for the LTE Device

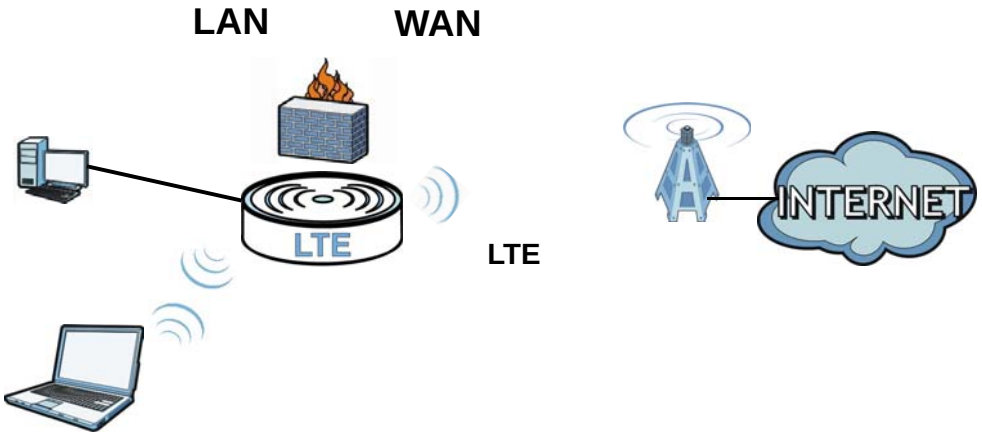
Here are some example uses for which the LTE Device is well suited.

### 1.2.1 Internet Access

Your LTE Device provides Internet access by connecting to an LTE network wirelessly.

Computers can connect to the LTE Device's **ETHERNET** ports.

**Figure 1** LTE Device's Internet Access Application

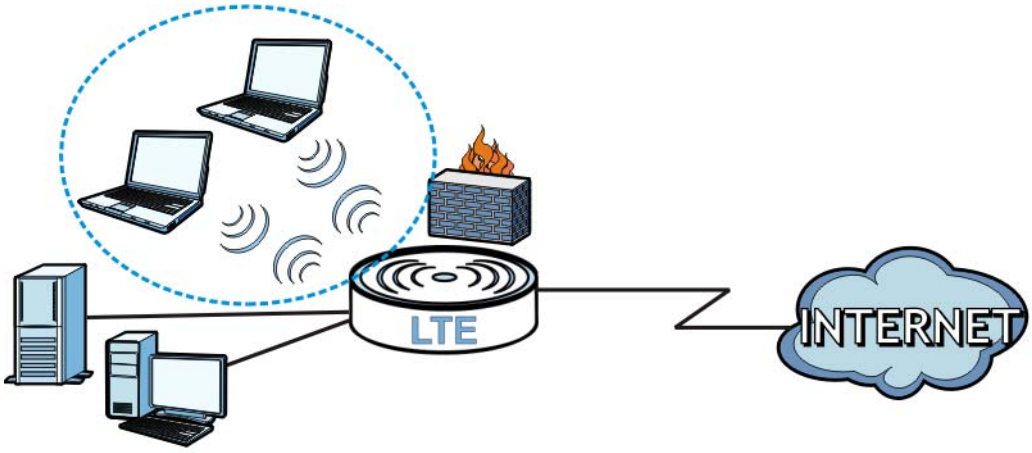



### 1.2.2 Wireless Connection

By default, the wireless LAN (WLAN) is enabled on the LTE Device. Once Wireless is enabled, IEEE 802.11b/g/n compliant clients can wirelessly connect to the LTE Device to access network

resources. You can set up a wireless network with WPS (WiFi Protected Setup) or manually add a client to your wireless network.

**Figure 2** Wireless Connection Application




# 1.3 The WLAN Button

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

## Turn the Wireless LAN On or Off

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

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

## Activate WPS

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

2 Press the **WIRELESS ON / OFF** button for more than five seconds and release it. Press the WPS button on another WPS-enabled device within range of the LTE Device. The **WLAN / WPS** LED should flash while the LTE Device sets up a WPS connection with the wireless device.

You must activate WPS in the LTE Device and in another wireless device within two minutes of each other. See Section 5.7.6 on page 59 for more information.

# 1.4 Ways to Manage the LTE Device

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

# 1.5 Good Habits for Managing the LTE Device

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

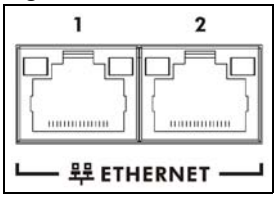
- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration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

# 1.6 LEDs (Lights)

The following graphic displays the labels of the LEDs.

**Figure 3** LEDs on the Top of the Device


**Figure 4** LEDs on the Ethernet Ports



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

**Table 1** LED Descriptions (From Left To Right)

| LED | COLOR | STATUS | DESCRIPTION |
|---|---|---|---|
| PWR/SYS | Green | On | The LTE Device is receiving power and ready for use. |
| | | Blinking | The LTE Device is booting up. |
| | Red | On | The LTE Device detected an error while self-testing, or there is a device malfunction. |
| | | Blinking | The LTE Device is upgrading the firmware. |
| | Off | | The LTE Device is not receiving power. |
| LTE | Green | On | The LTE Device has an LTE connection on the WAN. |
| | | Blinking | The LTE Device is searching for a frequency channel or is performing network entry. |
| | Off | | The LTE Device does not have an LTE connection on the WAN. |
| Signal Strength | | | The LTE LEDs display the Received Signal Strength Indication (RSSI) of the LTE connection. Three signals on at the same time means best signal quality, two means medium signal quality, and one means low signal quality. |
| | | No Signal LEDS | There is no LTE connection. |
| | Green | Signal 1 On | The signal strength is less than -90 dBm if signal 1 is on only. |
| | | Signal 2 On | The signal strength is between -90 dBm and -70 dBm if both signals 1 and 2 are on. |
| | | Signal 3 On | The signal strength is -70 dBm or greater if three signals are all on. |
| WLAN | Green | On | The wireless network is activated. |
| | | Blinking | The LTE Device is communicating with wireless clients. |
| | Orange | On | The LTE Device is setting up a WPS connection. |
| | Off | | The wireless network is not activated. |
| ETHERNET1 -2 | Yellow (Giga Ethernet) | On | The LTE Device has a successful 1000 Mbps Ethernet connection with a device on the Local Area Network (LAN). |
| | | Blinking | The LTE Device is sending or receiving data to/from the LAN at 1000 Mbps. |
| | Green (Fast Ethernet) | On | The LTE Device has a successful 10/100 Mbps Ethernet connection with a device on the Local Area Network (LAN). |
| | | Blinking | The LTE Device is sending or receiving data to/from the LAN at 10/100 Mbps. |
| | Off | | The LTE Device does not have an Ethernet connection with the LAN. |

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

# 1.7 The RESET Button

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the device to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the passwords will be reset to the defaults.

1 Make sure the **POWER** LED is on (not blinking).

2 To set the device back to the factory default settings, press the **RESET** button for 5 seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the device restarts.

# 2

# Introducing the Web Configurator

## 2.1 Overview

The web configurator is an HTML-based management interface that allows easy device setup and management via Internet browser. Use Internet Explorer 6.0 and later versions, Mozilla Firefox 3 and later versions, or Safari 2.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

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

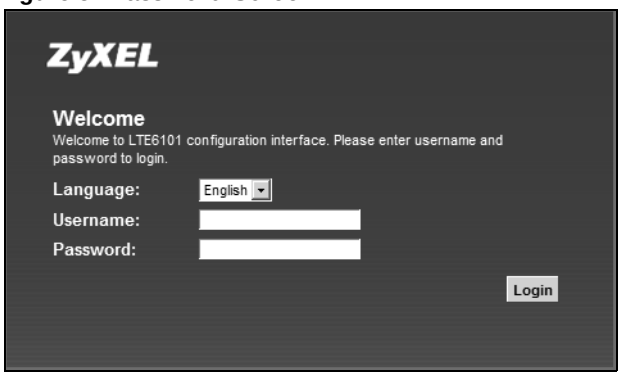
- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

See Appendix C on page 197 if you need to make sure these functions are allowed in Internet Explorer.

### 2.1.1 Accessing the Web Configurator

1. Make sure your LTE Device hardware is properly connected (refer to the Quick Start Guide).
2. Launch your web browser.
3. Type "192.168.1.1" as the URL.
4. A password screen displays. Type “admin” as the default Username and “1234” as the default password to access the device’s Web Configurator. Click **Login**. If you have changed the password, enter your password and click **Login**.

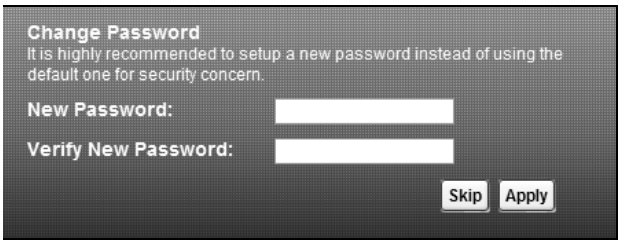
**Figure 5** Password Screen



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

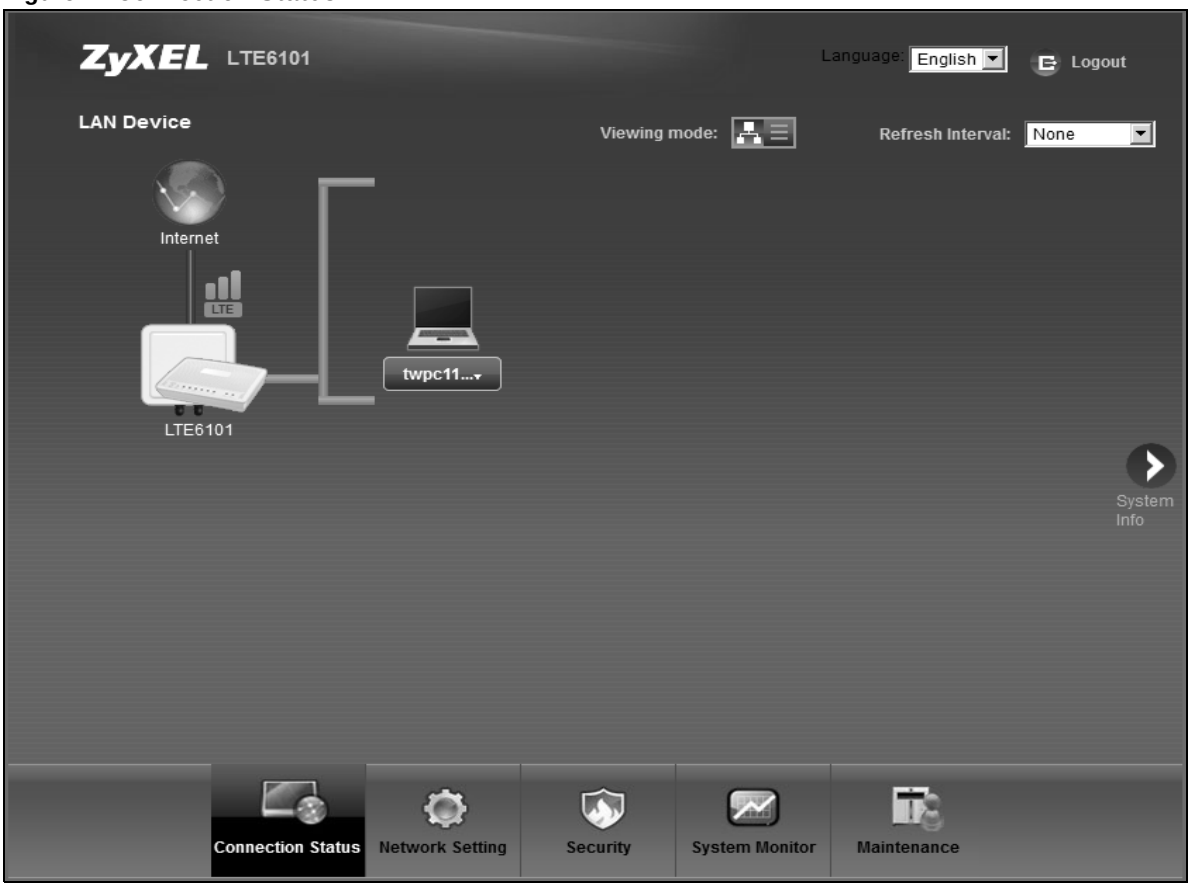
5 The following screen displays if you have not yet changed your password. It is strongly recommended you change the default password. Enter a new password, retype it to confirm and click **Apply**; alternatively click **Skip** to proceed to the main menu if you do not want to change the password now.

**Figure 6** Change Password Screen




6 The **Connection Status** screen appears.

**Figure 7** Connection Status

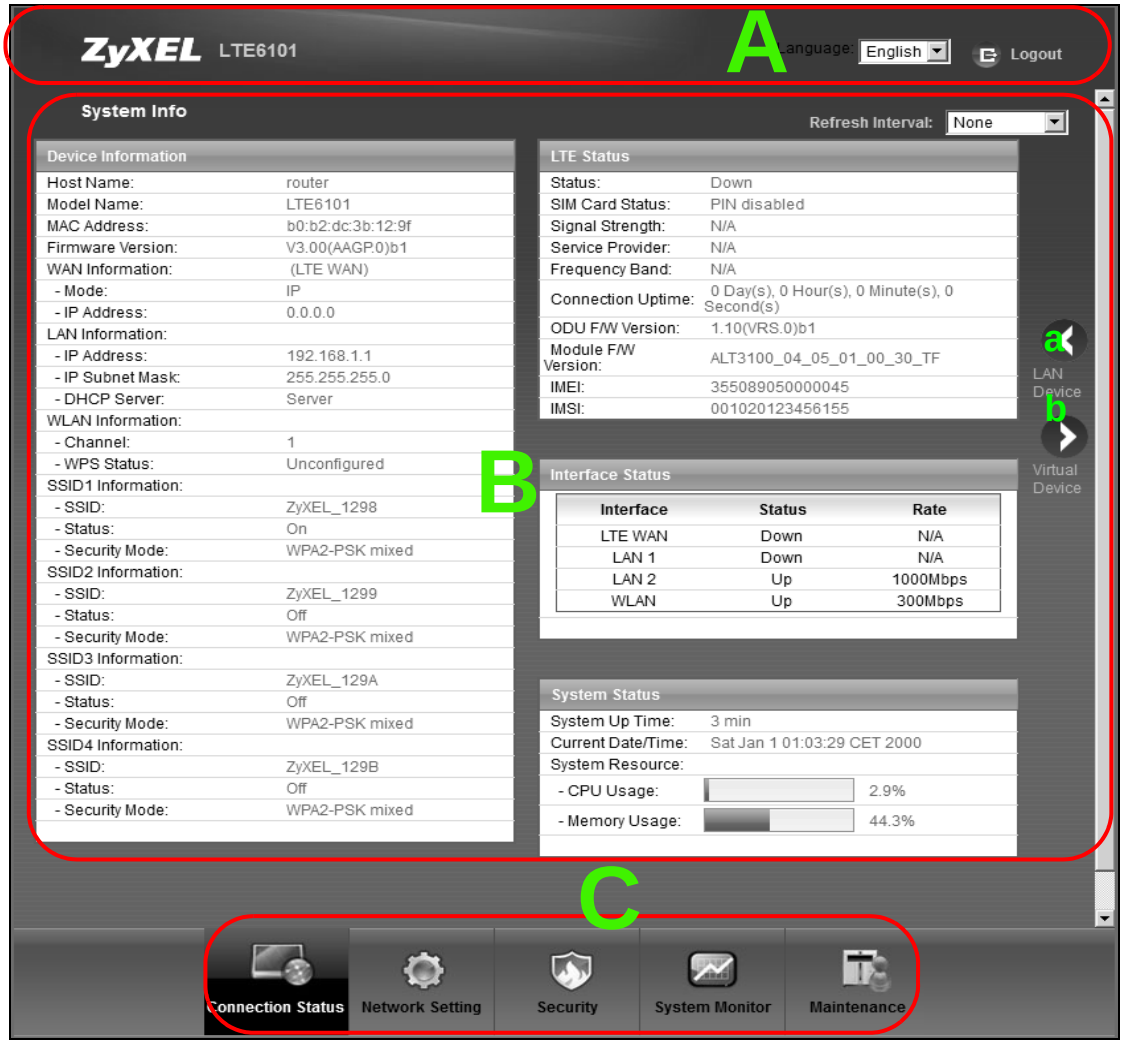



7 Click **System Info** to display the **System Info** screen, where you can view the LTE Device's interface and system information.

# 2.2 The Web Configurator Layout

Click **Connection Status > System Info** to show the following screen. (See Section 3.3 on page 29 for more information.)

**Figure 8** Web Configurator Layout




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

- **A** - title bar
- **B** - main window
- **C** - navigation panel

## 2.2.1 Title Bar

The title bar shows the following icon in the upper right corner.

Click this icon to log out of the web configurator.

## 2.2.2 Main Window

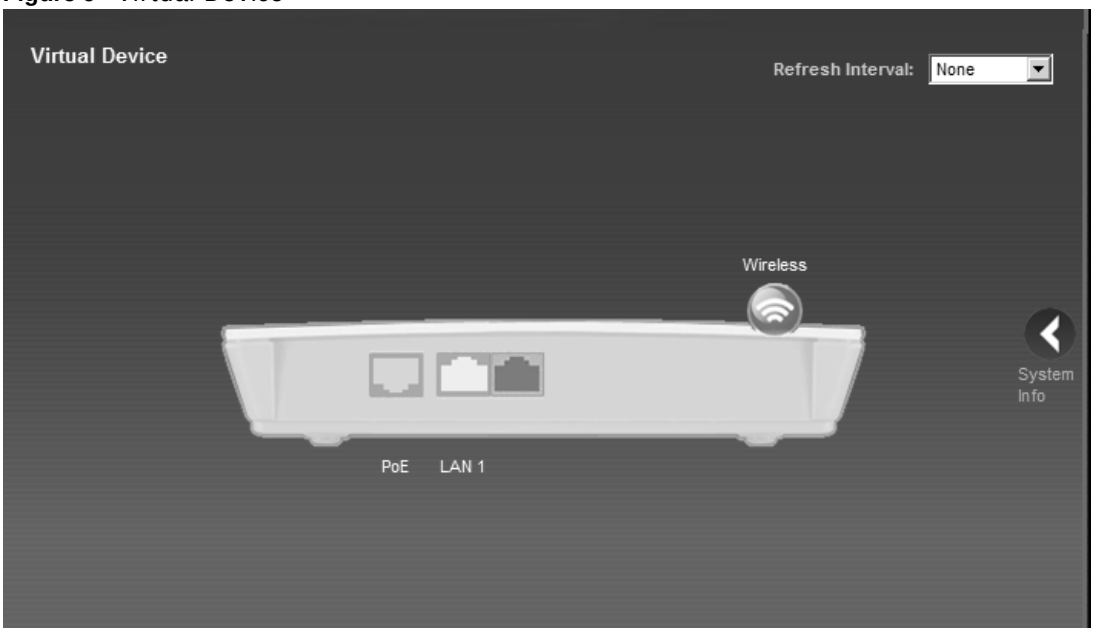
The main window displays information and configuration fields. It is discussed in the rest of this document.

After you click **System Info** on the **Connection Status** screen, the **System Info** screen is displayed. See Chapter 3 on page 29 for more information about the **System Info** screen.

If you click **LAN Device** on the **System Info** screen (**a** in Figure 8 on page 21), the **Connection Status** screen appears. See Chapter 3 on page 27 for more information about the **Connection Status** screen.

If you click **Virtual Device** on the **System Info** screen (**b** in Figure 8 on page 21), a visual graphic appears, showing the connection status of the LTE Device's ports. The connected ports are in color and disconnected ports are gray.

**Figure 9** Virtual Device




## 2.2.3 Traffic Status

Use the **Maintenance > Traffic Status** screens to look at network traffic status and statistics of the WAN, LAN interfaces and NAT. See Chapter 19 on page 137 for more information.

## 2.2.4 User Account

Use the **Maintenance > User Accounts** screen to configure system password for different user accounts. See Chapter 17 on page 133 for more information.

## 2.2.5 Navigation Panel

Use the menu items on the navigation panel to open screens to configure LTE Device features. The following table describes each menu item.

**Table 2** Navigation Panel Summary

| LINK | TAB | FUNCTION |
|---|---|---|
| Connection Status | | This screen shows the network status of the LTE Device and computers/devices connected to it. |
| Network Setting | | |
| Broadband | Broadband | Use this screen to view and modify your WAN interface. |
| | SIM | Use this screen to enter the PIN of your SIM card. |
| Wireless | General | Use this screen to turn the wireless connection on or off, specify the SSID(s) and configure the wireless LAN settings and WLAN authentication/security settings. |
| | More AP | Use this screen to configure multiple BSSs on the LTE Device. |
| | WPS | Use this screen to use WPS (Wi-Fi Protected Setup) to establish a wireless connection. |
| | WMM | Use this screen to enable or disable Wi-Fi MultiMedia (WMM). |
| | Scheduling | Use this screen to configure when the LTE Device enables or disables the wireless LAN. |
| Home Networking | LAN Setup | Use this screen to configure LAN TCP/IP settings, and other advanced properties. |
| | Static DHCP | Use this screen to assign specific IP addresses to individual MAC addresses. |
| | UPnP | Use this screen to enable the UPnP function. |
| Static Route | Static Route | Use this screen to view and set up static routes on the LTE Device. |
| QoS | General | Use this screen to enable QoS and decide allowable bandwidth using QoS. |
| | Queue Setup | Use this screen to configure QoS queue assignment. |
| | Class Setup | Use this screen to set up classifiers to sort traffic into different flows and assign priority and define actions to be performed for a classified traffic flow. |
| | Monitor | Use this screen to view each queue's statistics. |
| NAT | Port Forwarding | Use this screen to make your local servers visible to the outside world. |
| | DMZ | Use this screen to configure the IP address of the LTE Device's DMZ interface. |
| | Sessions | Use this screen to limit the number of NAT sessions a single client can establish. |
| Dynamic DNS | Dynamic DNS | Use this screen to allow a static hostname alias for a dynamic IP address. |
| Security | | |
| Firewall | General | Use this screen to activate/deactivate the firewall. |
| | Services | Use this screen to view and configure services. |
| | Access Control | Use this screen to view and configure filter rules for incoming and outgoing traffic. |
| | DoS | Use this screen to activate/deactivate Denial of Service (DoS) protection. |

**Table 2** Navigation Panel Summary (continued)

| LINK | TAB | FUNCTION |
|---|---|---|
| MAC Filter | MAC Filter | Use this screen to allow specific devices to access the LTE Device. |
| Parental Control | Parental Control | Use this screen to define time periods and days during which the LTE Device performs parental control and/or block web sites with the specific URL. |
| VPN | Setup | Use this screen to configure IPSec VPN connections. |
| | Monitor | Use this screen to view IPSec VPN connection status. |
| System Monitor | | |
| Log | System Log | Use this screen to view the system logs for the categories that you select. |
| Traffic Status | WAN | Use this screen to view the status of all network traffic going through the WAN port of the LTE Device. |
| | LAN | Use this screen to view the status of all network traffic going through the LAN ports of the LTE Device. |
| | NAT | Use this screen to view the status of NAT sessions on the LTE Device. |
| Maintenance | | |
| Users Account | Users Account | Use this screen to configure the passwords your user accounts. |
| Remote MGMT | Remote MGMT | Use this screen to enable specific traffic directions for network services. |
| System | System | Use this screen to configure the LTE Device's name, domain name, management inactivity time-out. |
| Time Setting | Time Setting | Use this screen to change your LTE Device's time and date. |
| Log Setting | Log Setting | Use this screen to select which logs and/or immediate alerts your device is to record. You can also set it to e-mail the logs to you. |
| Firmware Upgrade | Firmware Upgrade | Use this screen to upload firmware to your device. |
| Backup/ Restore | Backup/Restore | Use this screen to backup and restore your device's configuration (settings) or reset the factory default settings. |
| Reboot | Reboot | Use this screen to reboot the LTE Device without turning the power off. |
| Diagnostic | Ping/TraceRoute | Use this screen to test the connections to other devices. |

# PART II
# Technical Reference

The appendices provide general information. Some details may not apply to your LTE Device.

# 3

# Connection Status and System Info

## 3.1 Overview

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

Use the **System Info** screen to look at the current status of the device, system resources, interfaces (LAN, WAN).

If you click **Virtual Device** on the **System Info** screen, a visual graphic appears, showing the connection status of the LTE Device's ports. See Section 2.2.2 on page 22 for more information.

## 3.2 The Connection Status Screen

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

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

**Figure 10** Connection Status: Icon View

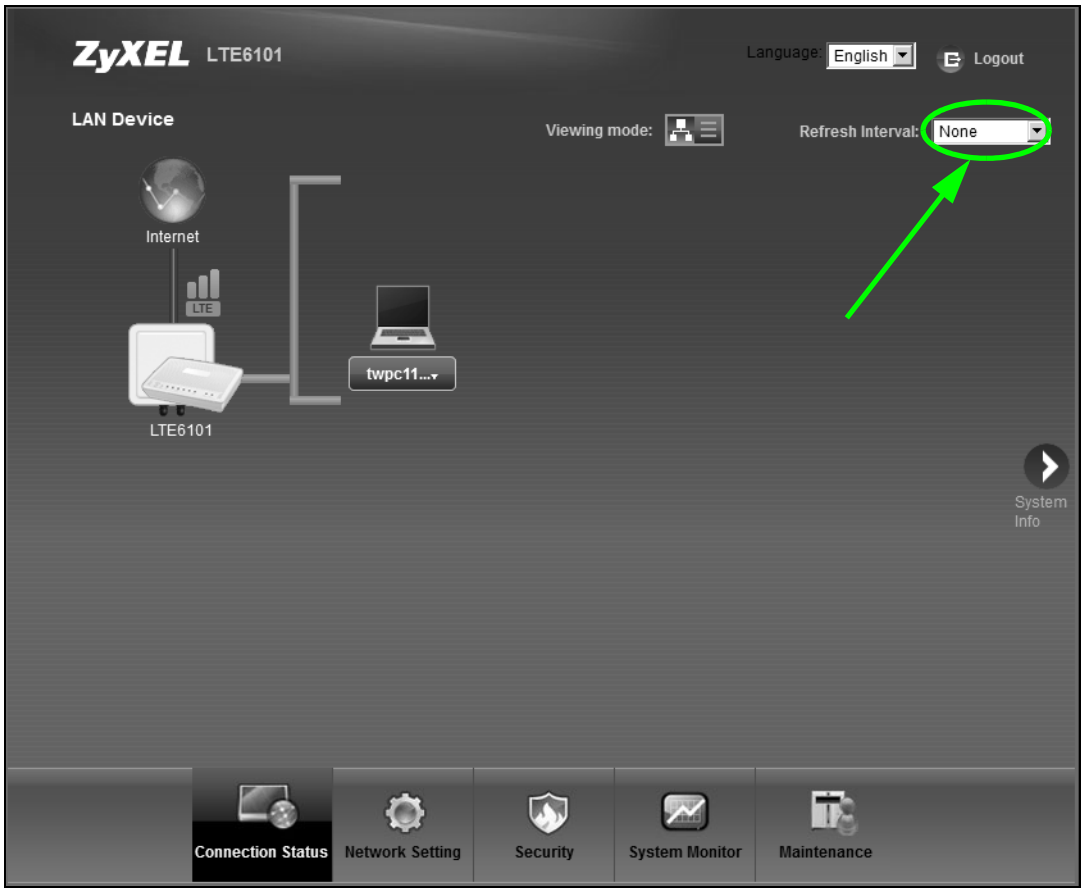
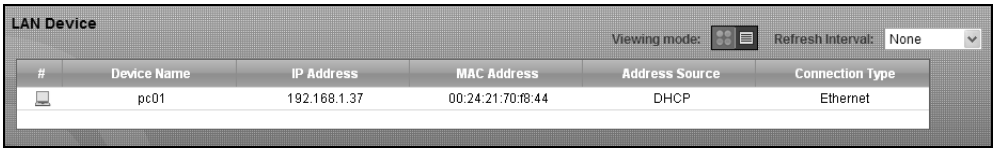



**Figure 11** Connection Status: List View




In **Icon View**, if you want to view information about a client, click the client's name and **Info**. Click the IP address if you want to change it. If you want to change the name or icon of the client, click **Change name/icon**.

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

# 3.3 The System Info Screen

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

**Figure 12** System Info Screen


Each field is described in the following table.

**Table 3** System Info Screen

| LABEL | DESCRIPTION |
|---|---|
| Language | Select the web configurator language from the drop-down list box. |
| Refresh Interval | Select how often you want the LTE Device to update this screen from the drop-down list box. |
| Device Information | |

**Table 3** System Info Screen (continued)

| LABEL | DESCRIPTION |
|---|---|
| Host Name | This field displays the LTE Device system name. It is used for identification. You can change this in the **Maintenance > System** screen's **Host Name** field. |
| Model Name | This is the model name of your device. |
| MAC Address | This is the MAC (Media Access Control) or Ethernet address unique to your LTE Device. |
| Software Version | This field displays the current version of the firmware inside the device. It also shows the date the firmware version was created. Go to the **Maintenance > Firmware Upgrade** screen to change it. |
| WAN Information | |
| Mode | This is the method of encapsulation used by your ISP. |
| IP Address | This field displays the current IP address of the LTE Device in the WAN. |
| LAN Information | |
| IP Address | This field displays the current IP address of the LTE Device in the LAN. |
| IP Subnet Mask | This field displays the current subnet mask in the LAN. |
| DHCP Server | This field displays what DHCP services the LTE Device is providing to the LAN. Choices are:<br>**Server** - The LTE Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN.<br>**None** - The LTE Device is not providing any DHCP services to the LAN. |
| WLAN Information | |
| Channel | This is the channel number used by the LTE Device now. |
| WPS Status | **Configured** displays when a wireless client has connected to the LTE Device or WPS is enabled and wireless or wireless security settings have been configured. **Unconfigured** displays if WPS is disabled or wireless security settings have not been configured. |
| SSID (1~4) Information | |
| SSID | This is the descriptive name used to identify the LTE Device in the wireless LAN. |
| Status | This shows whether or not the SSID is enabled (on). |
| Security Mode | This displays the type of security the LTE Device is using in the wireless LAN. |
| LTE Status | |
| Status | This displays **4G LTE** if there is an LTE connection, otherwise, it displays **Down**. |
| SIM Card Status | This displays the SIM card status:<br>**PIN disabled** - SIM card has no PIN code security.<br>**PIN required** - SIM card has PIN code security, but you didn't enter PIN code yet.<br>**PIN verified** - SIM card has PIN code security, and you entered the correct PIN code.<br>**PIN locked** - you entered an incorrect PIN code more than 10 times, so SIM card has been locked; call ISP for PUK (Pin Unlock Key) to unlock SIM card.<br>**SIM card locked call operator** - PUK (Pin Unlock Key) failed, so SIM card has been locked.<br>**No SIM Card** - you have not inserted a SIM card.<br>**SIM Card Error** - other SIM card error. |
| Signal Strength | This displays the strength of the LTE connection that the LTE Device has with the base station which is also known as eNodeB or eNB. |

**Table 3** System Info Screen (continued)

| LABEL | DESCRIPTION |
|---|---|
| Service Provider | This displays the service provider's name of the connected LTE network. |
| Frequency Band | This displays **LTE** if there is an LTE connection. |
| Connection Uptime | This displays how long the LTE connection has been available since it was last established successfully. |
| ODU F/W Version | This displays the firmware version of the outdoor unit. |
| Module F/W Version | This displays the firmware version of LTE module. |
| IMEI | This displays the LTE Device's International Mobile Equipment Identity number (IMEI). An IMEI is a unique ID used to identify a mobile device. |
| IMSI | This displays the International Mobile Subscriber Identity (IMSI) of the SIM card inserted in the outdoor unit. An IMSI is a unique ID used to identify a mobile subscriber in a mobile network. |
| Interface Status | |
| Interface | This column displays each interface the LTE Device has. |
| Status | This field indicates whether or not the LTE Device is using the interface.<br>For the LTE WAN interface, this field displays **Up** when the LTE Device is connected to an LTE network and **Down** when the LTE Device does not have an LTE connection.<br>For the LAN interface, this field displays **Up** when the LTE Device is using the interface and **Down** when the LTE Device is not using the interface. |
| Rate | For the LTE WAN interface, this displays **4G LTE** if there is an LTE connection.<br>For the LAN interface, this displays the port speed and duplex setting. |
| System Status | |
| System Up Time | This field displays how long the LTE Device has been running since it last started up. The LTE Device starts up when you plug it in, when you restart it (**Maintenance > Reboot**), or when you reset it (see Section 1.7 on page 16). |
| Current Date/Time | This field displays the current date and time in the LTE Device. You can change this in **Maintenance > Time Setting**. |
| System Resource | |
| CPU Usage | This field displays what percentage of the LTE Device's processing ability is currently used. When this percentage is close to 100%, the LTE Device is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications. |
| Memory Usage | This field displays what percentage of the LTE Device's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100%, the LTE Device is probably becoming unstable, and you should restart the device. See Chapter 23 on page 147, or turn off the device (unplug the power) for a few seconds. |

# 4

# Broadband

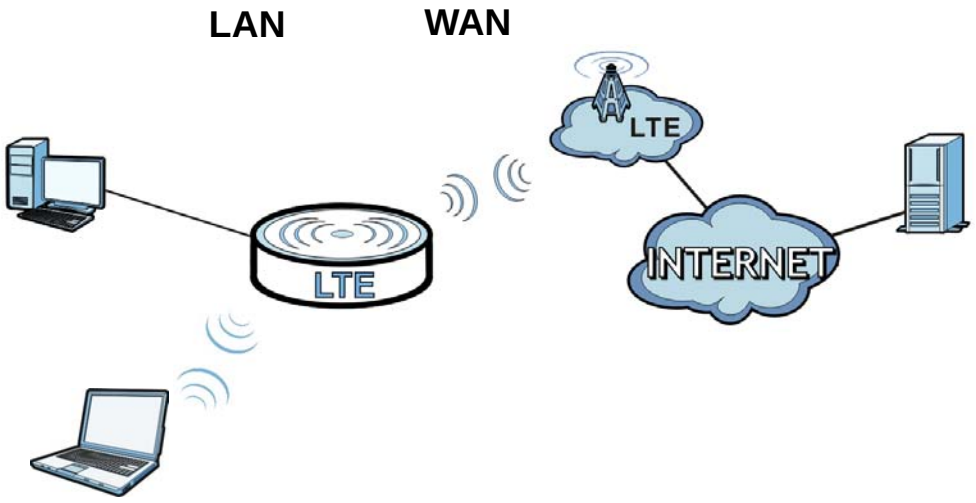
## 4.1 Overview

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

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

This LTE Device supports LTE connection for the WAN only.

**Figure 13** LAN and WAN




### 4.1.1 What You Can Do in this Chapter

- Use the **Broadband** screen to view or edit an LTE WAN interface. You can also configure the WAN settings on the LTE Device for Internet access (Section 4.2 on page 34).
- Use the **SIM** screen to enter the PIN of your SIM card (Section 4.3 on page 36).

### 4.1.2 What You Need to Know

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

### WAN IP Address

The WAN IP address is an IP address for the LTE Device, which makes it accessible from an outside network. It is used by the LTE Device to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the LTE Device tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es).

### APN

Access Point Name (APN) is a unique string which indicates an LTE network. An APN is required for LTE stations to enter the LTE network and then the Internet.

## 4.1.3 Before You Begin

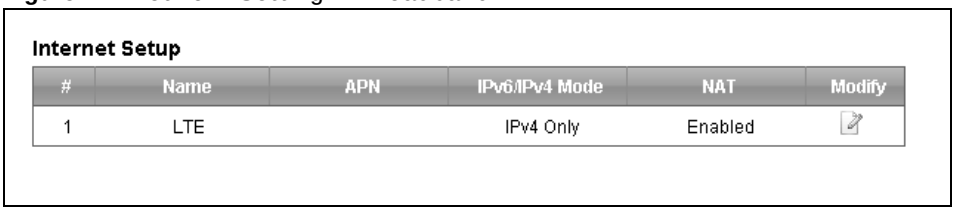
You may need to know your Internet access settings such as LTE APN, WAN IP address and SIM card's PIN code if the **INTERNET** light on your LTE Device is off. Get this information from your service provider.

# 4.2 The Broadband Screen

The LTE Device must have a WAN interface to allow users to use the LTE connection to access the Internet. Use the **Broadband** screen to view or modify a WAN interface.

Click **Network Setting > Broadband**. The following screen opens.

**Figure 14** Network Setting > Broadband




The following table describes the fields in this screen.

**Table 4** Network Setting > Broadband

| LABEL | DESCRIPTION |
|---|---|
| Internet Setup | |
| Name | This is the service name of the connection. |
| APN | This is the name of the LTE network to which the LTE Device will connect. |
| IPv6/IPv4 Mode | This shows whether the connection uses IPv6 or IPv4. |

**Table 4** Network Setting > Broadband (continued)

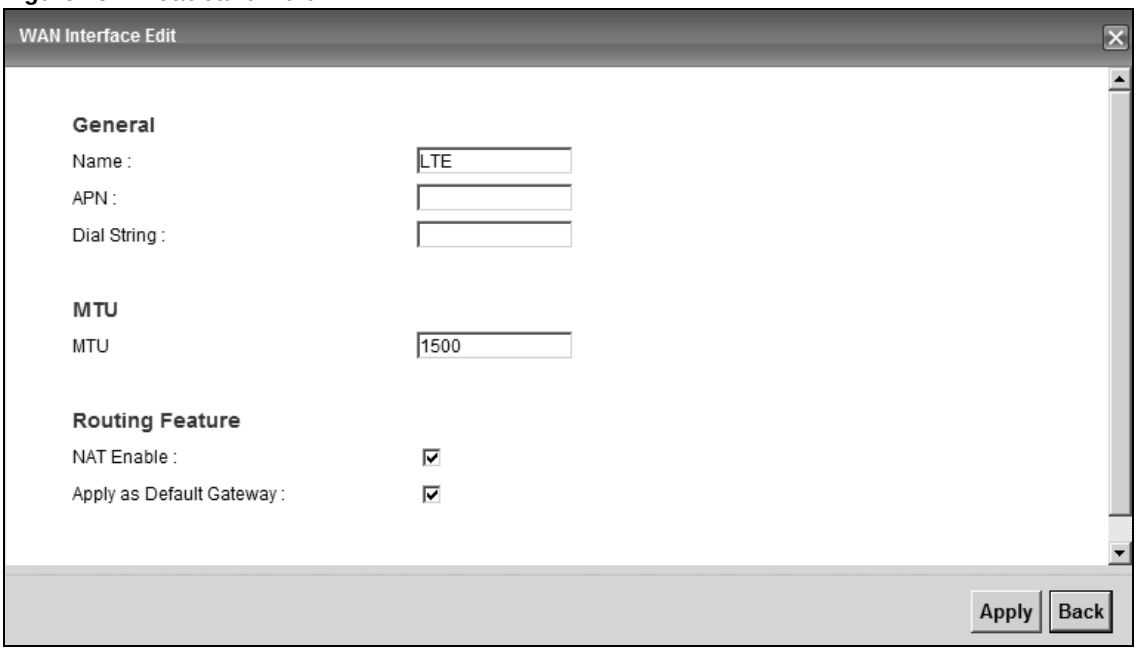
| LABEL | DESCRIPTION |
|---|---|
| NAT | This shows whether NAT is activated or not for this connection. NAT is not available when the connection uses the bridging service. |
| Modify | Click the **Edit** icon to configure the connection.<br>Click the **Delete** icon to delete this connection from the Device. A window displays asking you to confirm that you want to delete the connection. |

## 4.2.1 Edit Internet Connection

Use this screen to configure a WAN connection.

Click the **Edit** icon next to the LTE connection, the screen displays as shown next.

**Figure 15** Broadband Edit




The following table describes the fields in this screen.

**Table 5** Broadband Edit

| LABEL | DESCRIPTION |
|---|---|
| Name | Specify the name for this WAN interface. |
| APN | Enter the Access Point Name (APN) of an LTE network, which your service provider gave you. |
| Dial String | Enter the dial string for the ISP. |
| MTU | The Maximum Transmission Unit (MTU) defines the size of the largest packet allowed on an interface or connection. Enter the MTU for this WAN interface in this field. |
| NAT Enable | Select this to activate NAT on the WAN. |
| Apply as Default Gateway | Select this option to have the LTE Device use the WAN interface of this connection as the system default gateway. |

**Table 5** Broadband Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save your changes. |
| Back | Click **Back** to return to the previous screen. |

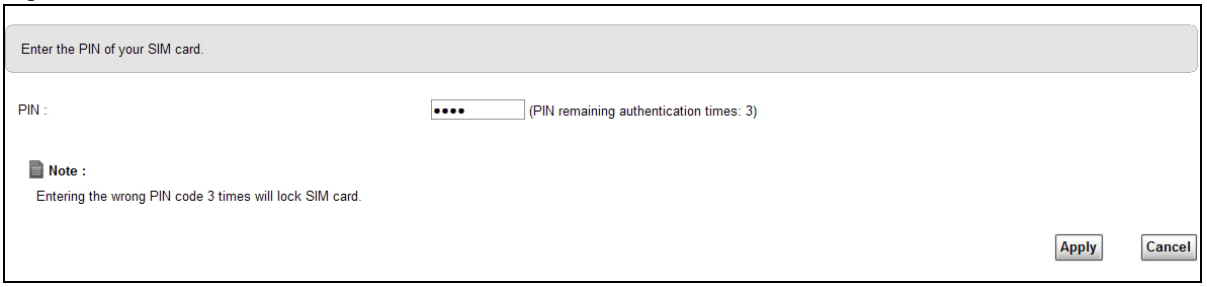
# 4.3 The SIM Screen

Use the **SIM** screen to enter the PIN of your SIM card.

**If the wrong PIN code is entered 3 times, it will cause the SIM card to be locked.**

Click **Network Setting > Broadband > SIM**. The following screen opens.

**Figure 16** SIM




The following table describes the fields in this screen.

**Table 6** SIM

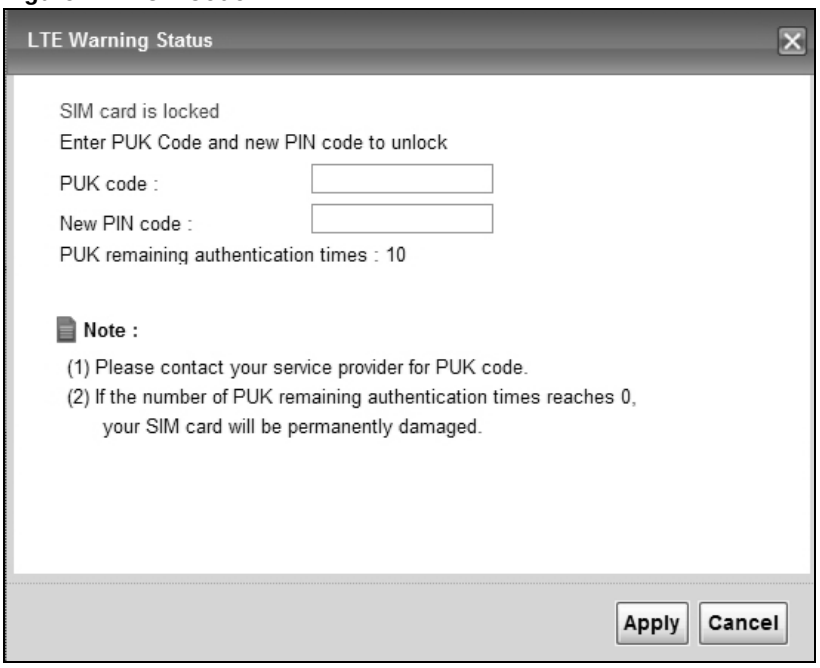
| LABEL | DESCRIPTION |
|---|---|
| PIN | Enter the PIN of your SIM card. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to return to the previous screen without saving. |

## 4.3.1 PUK Code Screen

If the SIM card is locked, use this screen to enter the PUK code.

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

**Figure 17** PUK Code




The following table describes the fields in this screen.

**Table 7** PUK Code

| LABEL | DESCRIPTION |
|---|---|
| PUK code | Enter the PUK (Pin Unlock Key) code to unlock the SIM card. |
| New PIN code | Enter the new PIN code for the SIM card. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to return to the previous screen without saving. |

# 4.4 Technical Reference

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

## Encapsulation

Be sure to use the encapsulation method required by your ISP. The LTE Device supports the following methods:

## IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP address and default gateway.

## DNS Server Address Assignment

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

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

1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.

2 If your ISP dynamically assigns the DNS server IP addresses (along with the LTE Device's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

## LTE Frequency Band Table

See the following table for the frequency bands used in LTE wireless technologies.

**Table 8** LTE Wireless Technologies

| BAND | UPLINK (UL) OPERATING BAND<br>BASE STATION RECEIVE<br>CPE TRANSMIT | DOWNLINK (DL) OPERATING BAND<br>BASE STATION TRANSMIT<br>CPE RECEIVE | DUPLEX MODE |
|---|---|---|---|
| | UL (LOW - HIGH) | DL (LOW - HIGH) | |
| 1 | 1920 MHz – 1980 MHz | 2110 MHz – 2170 MHz | FDD |
| 2 | 1850 MHz – 1910 MHz | 1930 MHz – 1990 MHz | FDD |
| 3 | 1710 MHz – 1785 MHz | 1805 MHz – 1880 MHz | FDD |
| 4 | 1710 MHz – 1755 MHz | 2110 MHz – 2155 MHz | FDD |
| 5 | 824 MHz – 849 MHz | 869 MHz – 894MHz | FDD |
| 6 | 830 MHz – 840 MHz | 875 MHz – 885 MHz | FDD |
| 7 | 2500 MHz – 2570 MHz | 2620 MHz – 2690 MHz | FDD |
| 8 | 880 MHz – 915 MHz | 925 MHz – 960 MHz | FDD |
| 9 | 1749.9 MHz – 1784.9 MHz | 1844.9 MHz – 1879.9 MHz | FDD |
| 10 | 1710 MHz – 1770 MHz | 2110 MHz – 2170 MHz | FDD |
| 11 | 1427.9 MHz – 1447.9 MHz | 1475.9 MHz – 1495.9 MHz | FDD |
| 12 | 699 MHz – 716 MHz | 729 MHz – 746 MHz | FDD |
| 13 | 777 MHz – 787 MHz | 746 MHz – 756 MHz | FDD |
| 14 | 788 MHz – 798 MHz | 758 MHz – 768 MHz | FDD |
| 15 | Reserved | Reserved | FDD |
| 16 | Reserved | Reserved | FDD |
| 17 | 704 MHz – 716 MHz | 734 MHz – 746 MHz | FDD |
| 18 | 815 MHz – 830 MHz | 860 MHz – 875 MHz | FDD |
| 19 | 830 MHz – 845 MHz | 875 MHz – 890 MHz | FDD |
| 20 | 832 MHz – 862 MHz | 791 MHz – 821 MHz | FDD |
| 21 | 1447.9 MHz – 1462.9 MHz | 1495.9 MHz – 1510.9 MHz | FDD |
| ... | | | |
| 24 | 1626.5 MHz – 1660.5 MHz | 1525 MHz – 1559 MHz | FDD |

**Table 8** LTE Wireless Technologies (continued)

| BAND | UPLINK (UL) OPERATING BAND BASE STATION RECEIVE CPE TRANSMIT | DOWNLINK (DL) OPERATING BAND BASE STATION TRANSMIT CPE RECEIVE | DUPLEX MODE |
|---|---|---|---|
| | UL (LOW - HIGH) | DL (LOW - HIGH) | |
| ... | | | |
| 33 | 1900 MHz – 1920 MHz | 1900 MHz – 1920 MHz | TDD |
| 34 | 2010 MHz – 2025 MHz | 2010 MHz – 2025 MHz | TDD |
| 35 | 1850 MHz – 1910 MHz | 1850 MHz – 1910 MHz | TDD |
| 36 | 1930 MHz – 1990 MHz | 1930 MHz – 1990 MHz | TDD |
| 37 | 1910 MHz – 1930 MHz | 1910 MHz – 1930 MHz | TDD |
| 38 | 2570 MHz – 2620 MHz | 2570 MHz – 2620 MHz | TDD |
| 39 | 1880 MHz – 1920 MHz | 1880 MHz – 1920 MHz | TDD |
| 40 | 2300 MHz – 2400 MHz | 2300 MHz – 2400 MHz | TDD |
| 41 | 2496 MHz 2690 MHz | 2496 MHz 2690 MHz | TDD |
| 42 | 3400 MHz – 3600 MHz | 3400 MHz – 3600 MHz | TDD |
| 43 | 3600 MHz – 3800 MHz | 3600 MHz – 3800 MHz | TDD |
| Note 1: Band 6 is not applicable | | | |

# 5

# Wireless

## 5.1 Overview

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

### 5.1.1 What You Can Do in this Chapter

- Use the **General** screen to enable the Wireless LAN, enter the SSID and select the wireless security mode (Section 5.2 on page 43).
- Use the **More AP** screen to set up multiple wireless networks on your LTE Device (Section 5.3 on page 49).
- Use the **WPS** screen to enable or disable WPS, view or generate a security PIN (Personal Identification Number) (Section 5.4 on page 51).
- Use the **WMM** screen to enable Wi-Fi MultiMedia (WMM) to ensure quality of service in wireless networks for multimedia applications (Section 5.5 on page 52).
- Use the **Scheduling** screen to schedule a time period for the wireless LAN to operate each day (Section 5.6 on page 54).

You don't necessarily need to use all these screens to set up your wireless connection. For example, you may just want to set up a network name, a wireless radio channel and some security in the **General** screen.

### 5.1.2 Wireless Network Overview

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

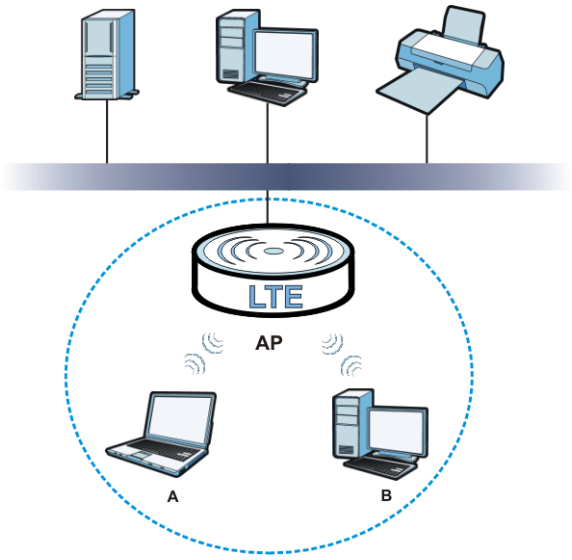
- A wireless client is a radio connected to a user's computer.
- An access point is a radio with a wired connection to a network, which can connect with numerous wireless clients and let them access the network.
- A bridge is a radio that relays communications between access points and wireless clients,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

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

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

The following figure provides an example of a wireless network.

**Figure 18** Example of a Wireless Network




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

Every wireless network must follow these basic guidelines.

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

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

  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every device in the same wireless network must use security compatible with the AP.
- Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

## Radio Channels

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

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

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

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

### 5.1.3 Before You Begin

Before you start using these screens, ask yourself the following questions. See Section 5.7 on page 54 if some of the terms used here do not make sense to you.

- What wireless standards do the other wireless devices support (IEEE 802.11g, for example)? What is the most appropriate standard to use?
- What security options do the other wireless devices support (WPA-PSK, for example)? What is the best one to use?
- Do the other wireless devices support WPS (Wi-Fi Protected Setup)? If so, you can set up a well-secured network very easily.

  Even if some of your devices support WPS and some do not, you can use WPS to set up your network and then add the non-WPS devices manually, although this is somewhat more complicated to do.
- What advanced options do you want to configure, if any? If you want to configure advanced options, ensure that you know precisely what you want to do. If you do not want to configure advanced options, leave them alone.

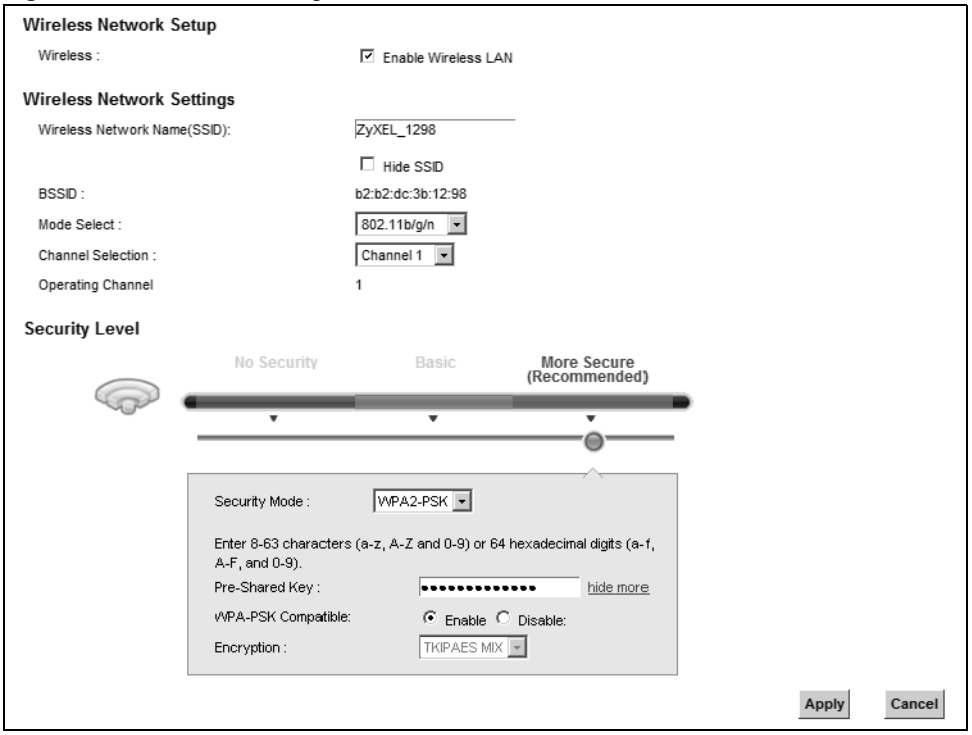
## 5.2 The Wireless General Screen

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

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

Click **Network Setting > Wireless** to open the **General** screen. Select the **Enable Wireless LAN** checkbox to show the Wireless configurations.

**Figure 19** Network Setting > Wireless > General




The following table describes the labels in this screen.

**Table 9** Network > Wireless LAN > General

| LABEL | DESCRIPTION |
|---|---|
| Wireless Network Setup | |
| Wireless | Select the **Enable Wireless LAN** check box to activate the wireless LAN. |
| Wireless Network Settings | |
| Wireless Network Name (SSID) | The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID.<br>Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN. |
| Hide SSID | Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. |
| BSSID | This shows the MAC address of the wireless interface on the LTE Device when wireless LAN is enabled. |
| Mode Select | This makes sure that only compliant WLAN devices can associate with the LTE Device.<br>Select **802.11b/g/n** to allow IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the LTE Device. The transmission rate of your LTE Device might be reduced.<br>Select **802.11b/g** to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the LTE Device. The transmission rate of your LTE Device might be reduced.<br>Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the LTE Device. Select **802.11n only in 2.4G band** to allow only IEEE 802.11n compliant WLAN devices with the same frequency range (2.4 GHz) to associate with the LTE Device. |

**Table 9** Network > Wireless LAN > General (continued)

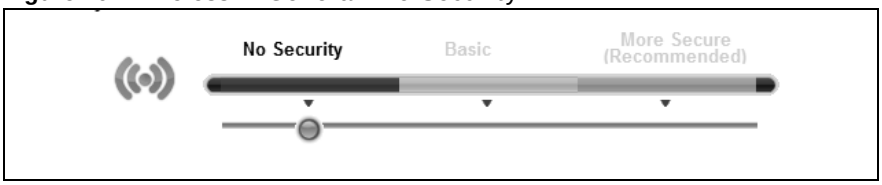
| LABEL | DESCRIPTION |
|---|---|
| Channel Selection | Set the channel depending on your particular region.<br>Select a channel or use **Auto** to have the LTE Device automatically determine a channel to use. If you are having problems with wireless interference, changing the channel may help. Try to use a channel that is as many channels away from any channels used by neighboring APs as possible. The channel number which the LTE Device is currently using then displays in the **Operating Channel** field. |
| Operating Channel | This is the channel currently being used by your AP. |
| Security Level | |
| Security Mode | Select **Basic** or **More Secure** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the LTE Device. When you select to use a security, additional options appears in this screen.<br>Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication.<br>See the following sections for more details about wireless security modes. |
| Apply | Click **Apply** to save your changes back to the LTE Device. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

## 5.2.1 No Security

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

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

**Figure 20** Wireless > General: No Security




The following table describes the labels in this screen.

**Table 10** Wireless > General: No Security

| LABEL | DESCRIPTION |
|---|---|
| Security Level | Choose **No Security** from the sliding bar. |

## 5.2.2 Basic (Static WEP/Shared WEP Encryption)

WEP encryption scrambles the data transmitted between the wireless stations and the access points (AP) to keep network communications private. Both the wireless stations and the access points must use the same WEP key.

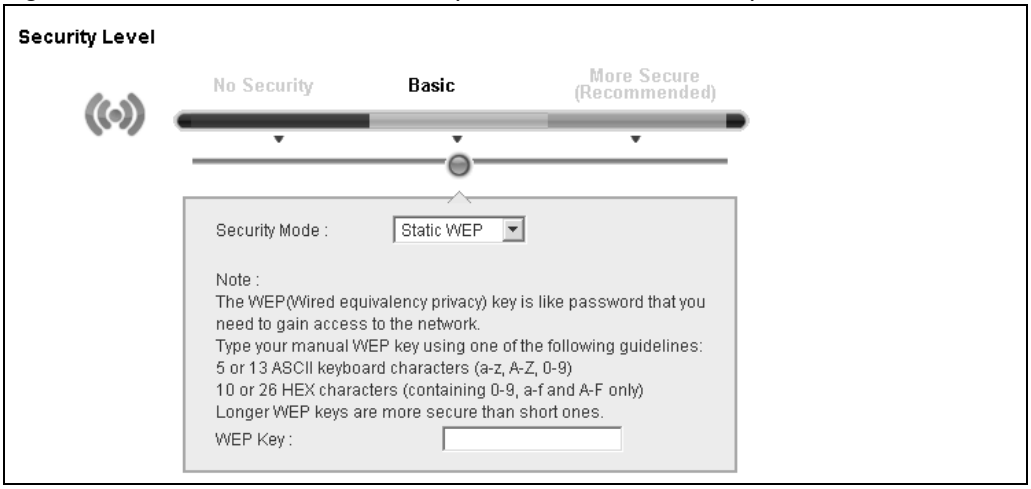
There are two types of WEP authentication namely, Open System (**Static WEP**) and Shared Key (**Shared WEP**).

Open system is implemented for ease-of-use and when security is not an issue. The wireless station and the AP or peer computer do not share a secret key. Thus the wireless stations can associate with any AP or peer computer and listen to any transmitted data that is not encrypted.

Shared key mode involves a shared secret key to authenticate the wireless station to the AP or peer computer. This requires you to enable the wireless LAN security and use same settings on both the wireless station and the AP or peer computer.

In order to configure and enable WEP encryption, click **Network Settings > Wireless** to display the **General** screen. Select **Basic** as the security level. Then select **Static WEP** or **Shared WEP** from the **Security Mode** list.

**Figure 21** Wireless > General: Basic (Static WEP/Shared WEP)




The following table describes the labels in this screen.

**Table 11** Wireless > General: Basic (Static WEP/Shared WEP)

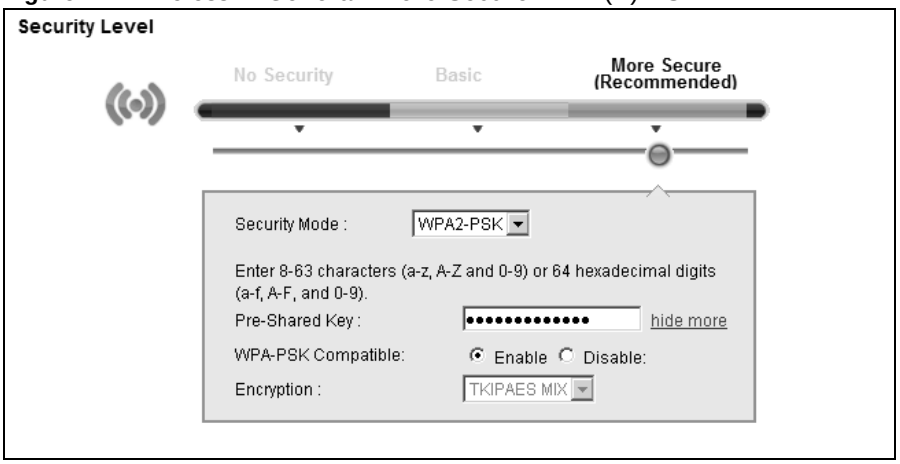
| LABEL | DESCRIPTION |
|---|---|
| Security Mode | Choose **Static WEP** or **Shared WEP** from the drop-down list box.<br>• Select **Static WEP** to have the LTE Device allow association with wireless clients that use Open System mode. Data transfer is encrypted as long as the wireless client has the correct WEP key for encryption. The LTE Device authenticates wireless clients using Shared Key mode that have the correct WEP key.<br>• Select **Shared WEP** to have the LTE Device authenticate only those wireless clients that use Shared Key mode and have the correct WEP key. |
| WEP Key | Enter a WEP key that will be used to encrypt data. Both the LTE Device and the wireless stations must use the same WEP key for data transmission. |

## 5.2.3 More Secure (WPA(2)-PSK)

The WPA-PSK security mode provides both improved data encryption and user authentication over WEP. Using a Pre-Shared Key (PSK), both the LTE Device and the connecting client share a common password in order to validate the connection. This type of encryption, while robust, is not as strong as WPA, WPA2 or even WPA2-PSK. The WPA2-PSK security mode is a newer, more robust version of the WPA encryption standard. It offers slightly better security, although the use of PSK makes it less robust than it could be.

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

**Figure 22** Wireless > General: More Secure: WPA(2)-PSK




The following table describes the labels in this screen.

**Table 12** Wireless > General: WPA(2)-PSK

| LABEL | DESCRIPTION |
|---|---|
| Security Level | Select **More Secure** to enable WPA(2)-PSK data encryption. |
| Security Mode | Select **WPA-PSK** or **WPA2-PSK** from the drop-down list box. |
| Pre-Shared Key | The encryption mechanisms used for **WPA / WPA2** and **WPA-PSK / WPA2-PSK** are the same. The only difference between the two is that **WPA-PSK / WPA2-PSK** uses a simple common password, instead of user-specific credentials.<br>Type a pre-shared key from 8 to 63 case-sensitive ASCII characters or 64 hexidecimal digits. |
| more.../hide more | Click **more...** to show more fields in this section. Click **hide more** to hide them. |
| WPA-PSK Compatible | This field appears when you choose **WPA-PSK2** as the **Security Mode**.<br>Check this field to allow wireless devices using **WPA-PSK** security mode to connect to your LTE Device. The LTE Device supports WPA-PSK and WPA2-PSK simultaneously. |
| Encryption | If the security mode is **WPA-PSK**, the encryption mode is set to **TKIP** to enable Temporal Key Integrity Protocol (TKIP) security on your wireless network.<br>If the security mode is **WPA-PSK2** and **WPA-PSK Compatible** is disabled, the encryption mode is set to **AES** to enable Advanced Encryption System (AES) security on your wireless network. AES provides superior security to TKIP.<br>If the security mode is **WPA-PSK2** and **WPA-PSK Compatible** is enabled, the encryption mode is set to **TKIPAES MIX** to allow both TKIP and AES types of security in your wireless network. |

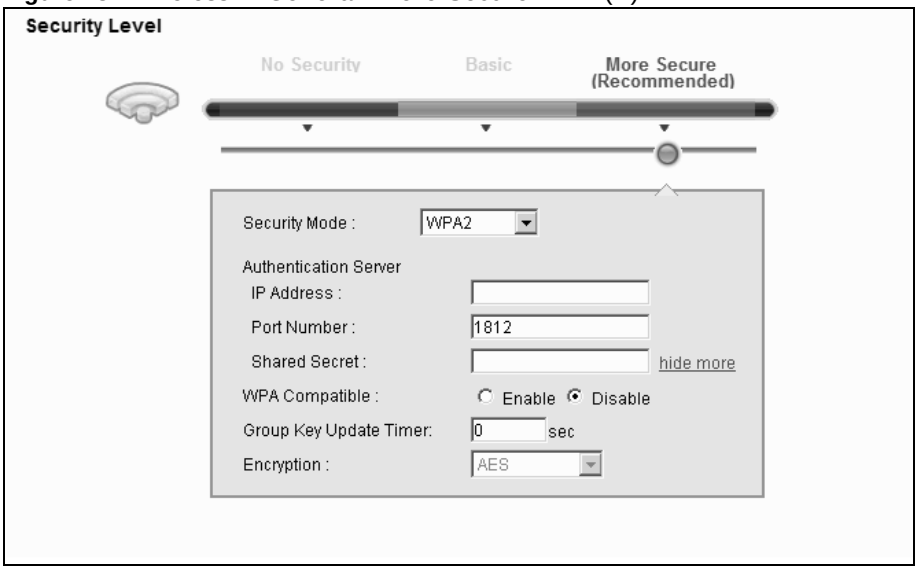
## 5.2.4 WPA(2) Authentication

The WPA2 security mode is currently the most robust form of encryption for wireless networks. It requires a RADIUS server to authenticate user credentials and is a full implementation the security protocol. Use this security option for maximum protection of your network. However, it is the least backwards compatible with older devices.

The WPA security mode is a security subset of WPA2. It requires the presence of a RADIUS server on your network in order to validate user credentials. This encryption standard is slightly older than WPA2 and therefore is more compatible with older devices.

Click **Network Settings** > **Wireless** to display the **General** screen. Select **More Secure** as the security level. Then select **WPA** or **WPA2** from the **Security Mode** list.

**Figure 23** Wireless > General: More Secure: WPA(2)




The following table describes the labels in this screen.

**Table 13** Wireless > General: More Secure: WPA(2)

| LABEL | DESCRIPTION |
|---|---|
| Security Level | Select **More Secure** to enable WPA(2)-PSK data encryption. |
| Security Mode | Choose **WPA** or **WPA2** from the drop-down list box. |
| 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. The default port number is **1812**.<br><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 128 alphanumeric characters) as the key to be shared between the external authentication server and the LTE Device.<br><br>The key must be the same on the external authentication server and your LTE Device. The key is not sent over the network. |
| more.../hide more | Click **more...** to show more fields in this section. Click **hide more** to hide them. |

**Table 13** Wireless > General: More Secure: WPA(2) (continued)

| LABEL | DESCRIPTION |
|---|---|
| WPA Compatible | This field is only available for WPA2. Select this if you want the LTE Device to support WPA and WPA2 simultaneously. |
| Group Key Update Timer | The **Group Key Update Timer** is the rate at which the RADIUS server sends a new group key out to all clients.<br>If the value is set to "0", the update timer function is disabled. |
| Encryption | If the security mode is **WPA**, the encryption mode is set to **TKIP** to enable Temporal Key Integrity Protocol (TKIP) security on your wireless network.<br>If the security mode is **WPA2**, the encryption mode is set to **AES** to enable Advanced Encryption System (AES) security on your wireless network. AES provides superior security to TKIP. |

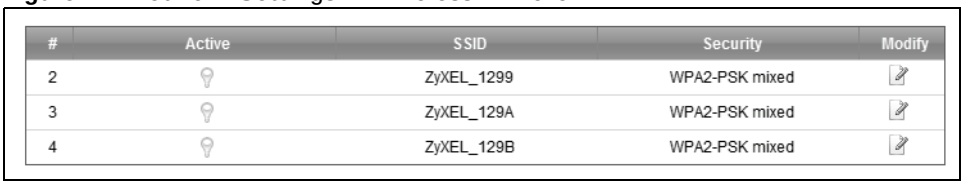
# 5.3 The More AP Screen

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

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

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

**Figure 24** Network Settings > Wireless > More AP




The following table describes the labels in this screen.

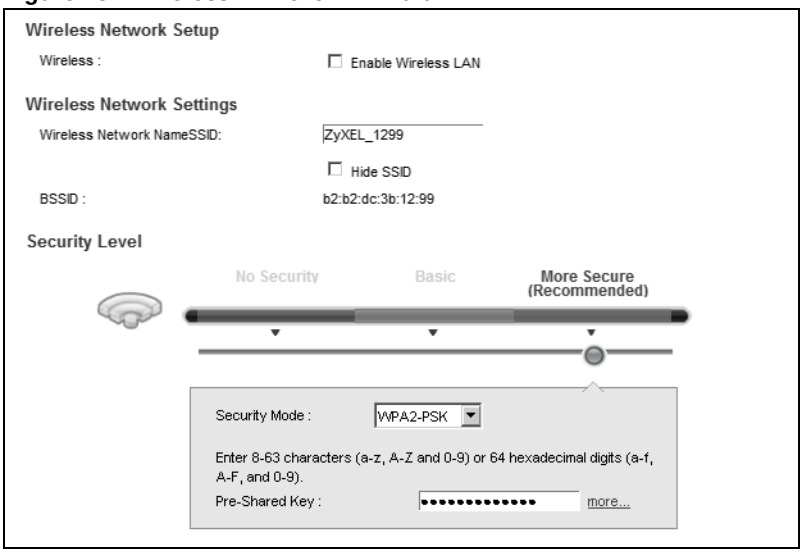
**Table 14** Network Settings > Wireless > More AP

| LABEL | DESCRIPTION |
|---|---|
| # | This is the index number of the entry. |
| Active | This field indicates whether this SSID is active. A yellow bulb signifies that this SSID is active. A gray bulb signifies that this SSID is not active. |
| SSID | An SSID profile is the set of parameters relating to one of the LTE Device's BSSs. The SSID (Service Set IDentifier) identifies the Service Set with which a wireless device is associated.<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. |
| Modify | Click the **Edit** icon to configure the SSID profile. |

## 5.3.1 Edit More AP

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

**Figure 25** Wireless > More AP: Edit




The following table describes the fields in this screen.

**Table 15** Wireless > More AP: Edit

| LABEL | DESCRIPTION |
|---|---|
| Wireless Network Setup | |
| Wireless | Select the **Enable Wireless LAN** check box to activate the wireless LAN. |
| Wireless Network Settings | |
| Wireless Network Name (SSID) | The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID.<br>Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN. |
| Hide SSID | Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. |
| BSSID | This shows the MAC address of the wireless interface on the LTE Device when wireless LAN is enabled. |
| Security Level | |
| Security Mode | Select **Basic (WEP)** or **More Secure (WPA(2)-PSK, WPA(2))** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the LTE Device. After you select to use a security, additional options appears in this screen.<br>Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication.<br>See Section 5.2.1 on page 45 for more details about this field. |
| Apply | Click **Apply** to save your changes. |
| Back | Click **Back** to exit this screen without saving. |

# 5.4 The WPS Screen

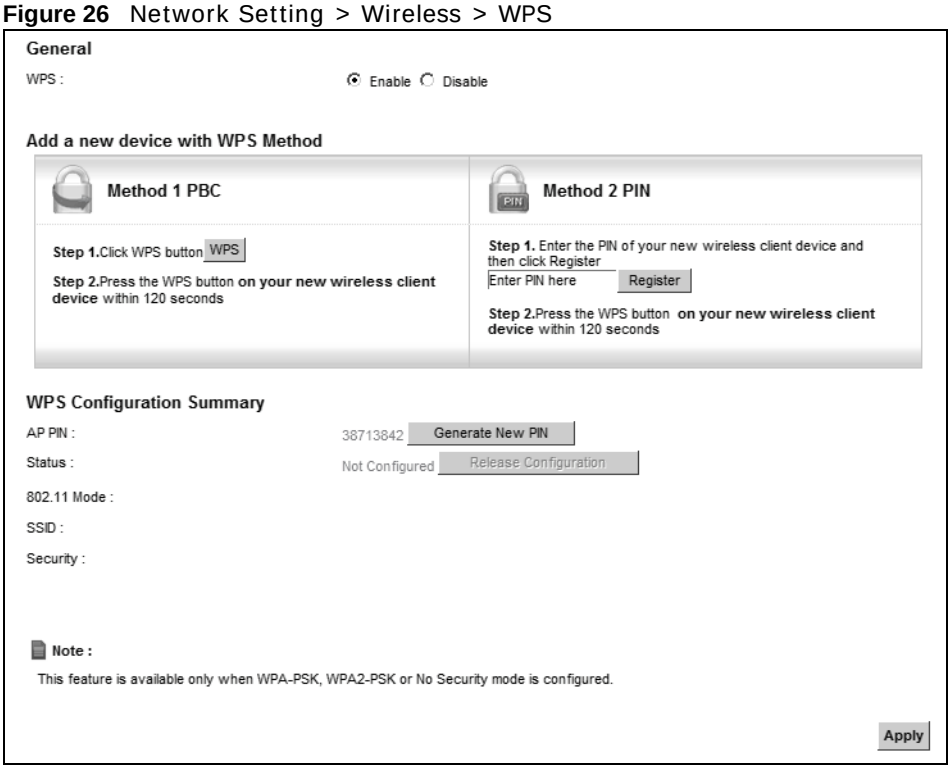
Use this screen to configure WiFi Protected Setup (WPS) on your LTE Device.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Set up each WPS connection between two devices. Both devices must support WPS. See Section 5.7.6.3 on page 61 for more information about WPS.

Note: The LTE Device applies the security settings of the **SSID1** profile (see Section 5.2 on page 43). If you want to use the WPS feature, make sure you have set the security mode of **SSID1** to **WPA-PSK**, **WPA2-PSK** or **No Security**.

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

**Figure 26** Network Setting > Wireless > WPS




The following table describes the labels in this screen.

**Table 16** Network Setting > Wireless > WPS

| LABEL | DESCRIPTION |
|---|---|
| Enable WPS | Select **Enable** to activate WPS on the LTE Device. |
| Add a new device with WPS Method | |
| Method 1 PBC | Use this section to set up a WPS wireless network using Push Button Configuration (PBC). |
| WPS | Click this button to add another WPS-enabled wireless device (within wireless range of the LTE Device) to your wireless network. This button may either be a physical button on the outside of device, or a menu button similar to the **WPS** button on this screen.<br><br>Note: You must press the other wireless device's WPS button within two minutes of pressing this button. |

**Table 16** Network Setting > Wireless > WPS (continued)

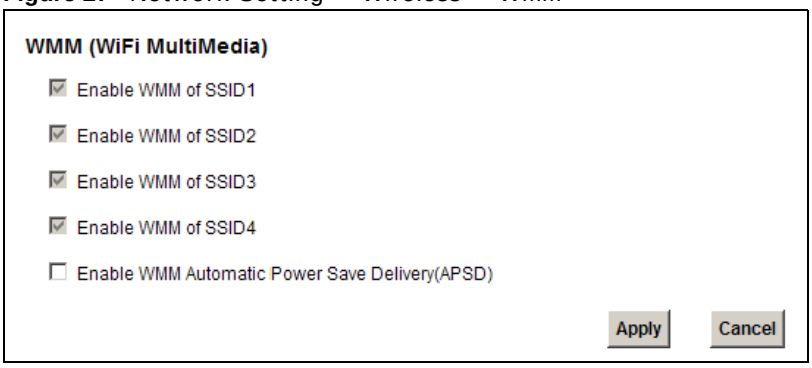
| LABEL | DESCRIPTION |
|---|---|
| Method 2 PIN | Use this section to set up a WPS wireless network by entering the PIN (Personal Identification Number) of the client into the LTE Device. |
| Register | Enter the PIN of the device that you are setting up a WPS connection with and click **Register** to authenticate and add the wireless device to your wireless network.<br>You can find the PIN either on the outside of the device, or by checking the device's settings.<br>Note: You must also activate WPS on that device within two minutes to have it present its PIN to the LTE Device. |
| WPS Configuration Summary | |
| AP PIN | The PIN of the LTE Device is shown here. Enter this PIN in the configuration utility of the device you want to connect to using WPS.<br>The PIN is not necessary when you use WPS push-button method.<br>Click the **Generate New PIN** button to have the LTE Device create a new PIN. |
| Status | This displays **Configured** when the LTE Device has connected to a wireless network using WPS or **Enable WPS** 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 **Not Configured** when there is no wireless or wireless security changes on the LTE Device or you click **Release Configuration** to remove the configured wireless and wireless security settings. |
| Release Configuration | This button is available when the WPS status is **Configured.**<br>Click this button to remove all configured wireless and wireless security settings for WPS connections on the LTE Device. |
| 802.11 Mode | This is the 802.11 mode used. Only compliant WLAN devices can associate with the LTE Device. |
| SSID | This is the name of the wireless network. |
| Security | This is the type of wireless security employed by the network. |
| Apply | Click **Apply** to save your changes. |

# 5.5 The WMM Screen

Use this screen to enable or disable Wi-Fi MultiMedia (WMM) wireless networks for multimedia applications.

Click **Network Setting > Wireless > WMM**. The following screen displays.

**Figure 27** Network Setting > Wireless > WMM




The following table describes the labels in this screen.

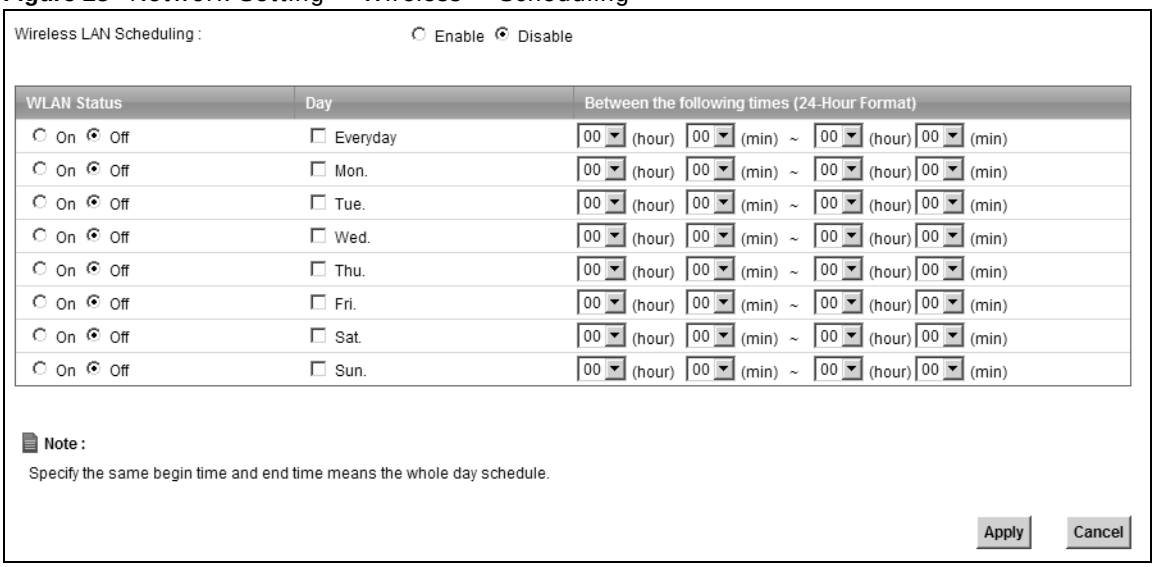
**Table 17** Network Setting > Wireless > WMM

| LABEL | DESCRIPTION |
|---|---|
| Enable WMM of SSID1~4 | This enables the LTE Device to 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. |
| Enable WMM Automatic Power Save Deliver (APSD) | Click this to increase battery life for battery-powered wireless clients. APSD uses a longer beacon interval when transmitting traffic that does not require a short packet exchange interval. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

# 5.6 Scheduling Screen

Click **Network Setting > Wireless > Scheduling** to open the **Wireless LAN Scheduling** screen. Use this screen to configure when the LTE Device enables or disables the wireless LAN.

**Figure 28** Network Setting > Wireless > Scheduling




The following table describes the labels in this screen.

**Table 18** Network Setting > Wireless > Scheduling

| LABEL | DESCRIPTION |
|---|---|
| Wireless LAN Scheduling | Select **Enable** to activate wireless LAN scheduling on your LTE Device. |
| WLAN status | Select **On** or **Off** to enable or disable the wireless LAN. |
| Day | Select the day(s) you want to turn the wireless LAN on or off. |
| Between the following times | Specify the time period during which to apply the schedule.<br>For example, you want the wireless network to be only available during work hours. Check Mon ~ Fri in the day column, and specify 8:00 ~ 18:00 in the time table. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

# 5.7 Technical Reference

This section discusses wireless LANs in depth. For more information, see the appendix.

## 5.7.1 Additional Wireless Terms

The following table describes some wireless network terms and acronyms used in the LTE Device's web configurator.

**Table 19** Additional Wireless Terms

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

## 5.7.2 Wireless Security Overview

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

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

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

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

A good way to come up with effective security keys, passwords and so on is to use obscure information that you personally will easily remember, and to enter it in a way that appears random

and does not include real words. For example, if your mother owns a 1970 Dodge Challenger and her favorite movie is Vanishing Point (which you know was made in 1971) you could use "70dodchal71vanpoi" as your security key.

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

#### 5.7.2.1 SSID

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

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

#### 5.7.2.2 MAC Address Filter

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

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

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

#### 5.7.2.3 User Authentication

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

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

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

1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

### 5.7.2.4 Encryption

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

The types of encryption you can choose depend on the type of authentication. (See Section 5.7.2.3 on page 56 for information about this.)

**Table 20** Types of Encryption for Each Type of Authentication

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

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

Usually, you should set up the strongest encryption that every device in the wireless network supports. For example, suppose you have a wireless network with the LTE Device and you do not have a RADIUS server. Therefore, there is no authentication. Suppose the wireless network has two devices. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.

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

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

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

## 5.7.3 Signal Problems

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

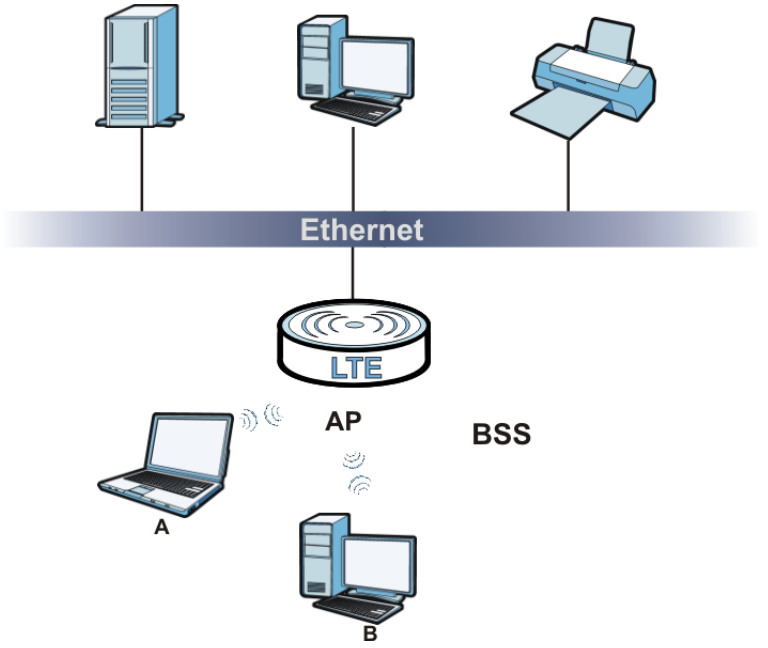
Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters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

## 5.7.4 BSS

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

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

**Figure 29** Basic Service set




## 5.7.5 MBSSID

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

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

### 5.7.5.1 Notes on Multiple BSSs

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

## 5.7.6 WiFi Protected Setup (WPS)

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

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

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

### 5.7.6.1 Push Button Configuration

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

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

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

1. Ensure that the two devices you want to set up are within wireless range of one another.
2. Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the LTE Device, see Section 5.4 on page 51).
3. Press the button on one of the devices (it doesn't matter which). For the LTE Device you must press the WPS button for more than three seconds.
4. Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through an secure connection to the enrollee.

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

### 5.7.6.2 PIN Configuration

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

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

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

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

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

1 Ensure WPS is enabled on both devices.

2 Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this.

3 Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide for how to find the WPS PIN - for the LTE Device, see Section 5.4 on page 51).

4 Enter the client's PIN in the AP's configuration interface.

5 If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client - it does not matter which.

6 Start WPS on both devices within two minutes.

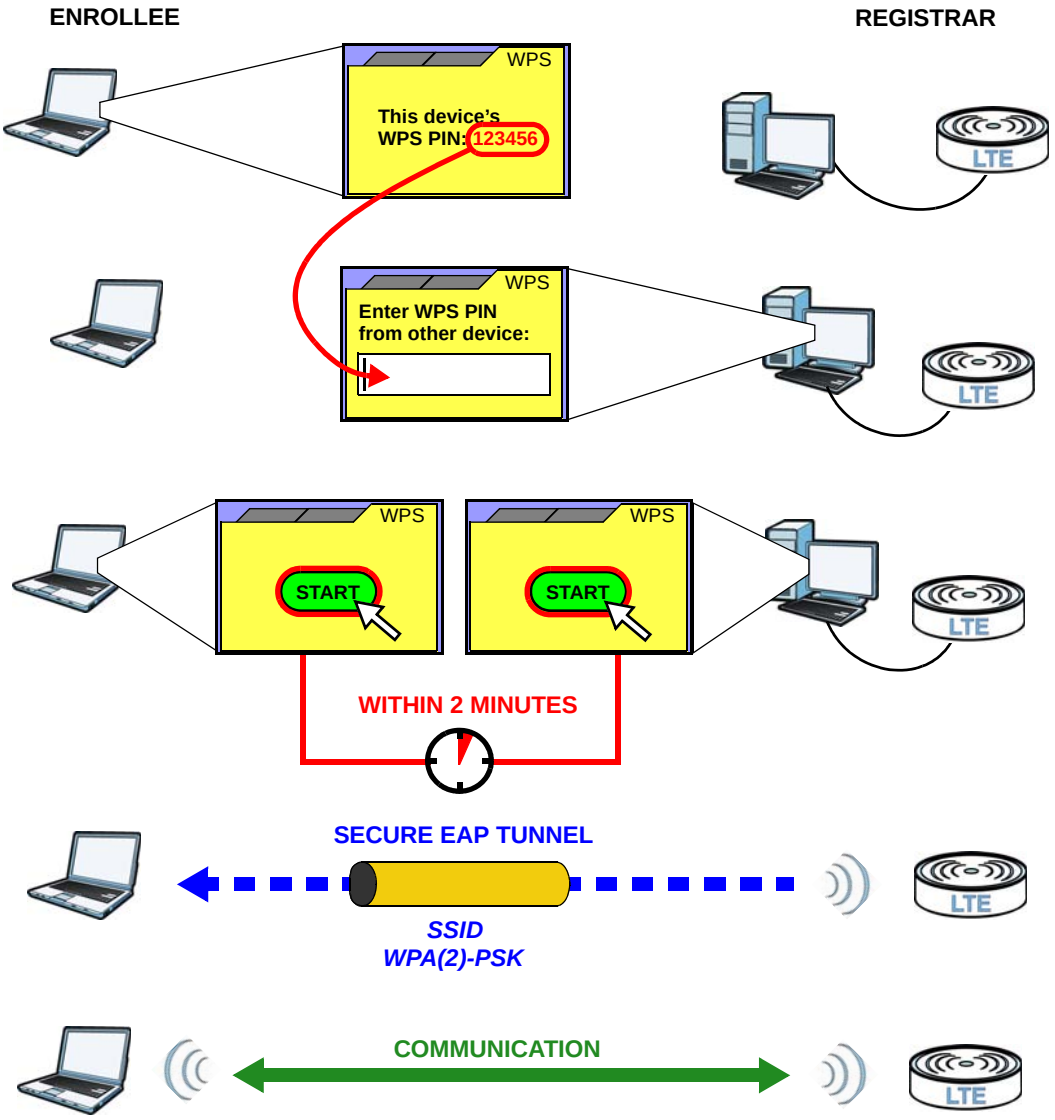
7 Use the configuration utility to activate WPS, not the push-button on the device itself.

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

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

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

**Figure 30** Example WPS Process: PIN Method

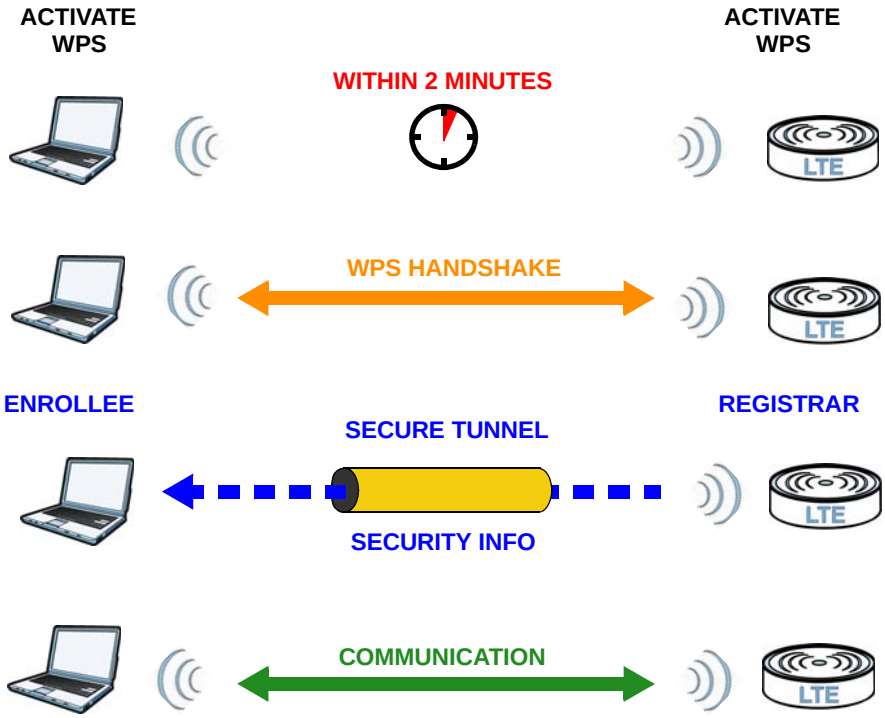



## 5.7.6.3 How WPS Works

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

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

**Figure 31** How WPS works




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

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

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

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

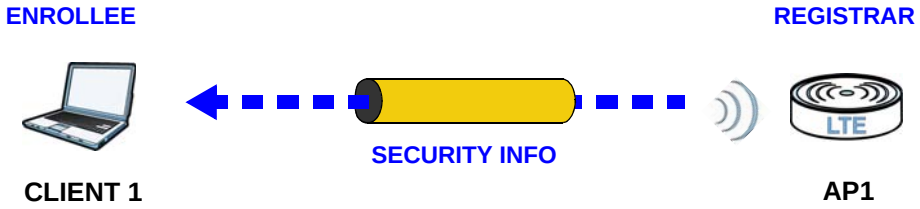
### 5.7.6.4 Example WPS Network Setup

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

The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1**

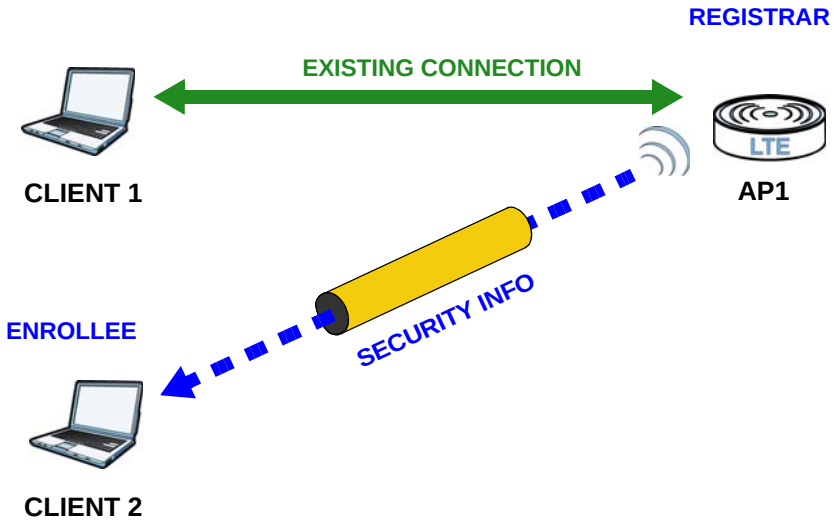
is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information.

**Figure 32** WPS: Example Network Step 1



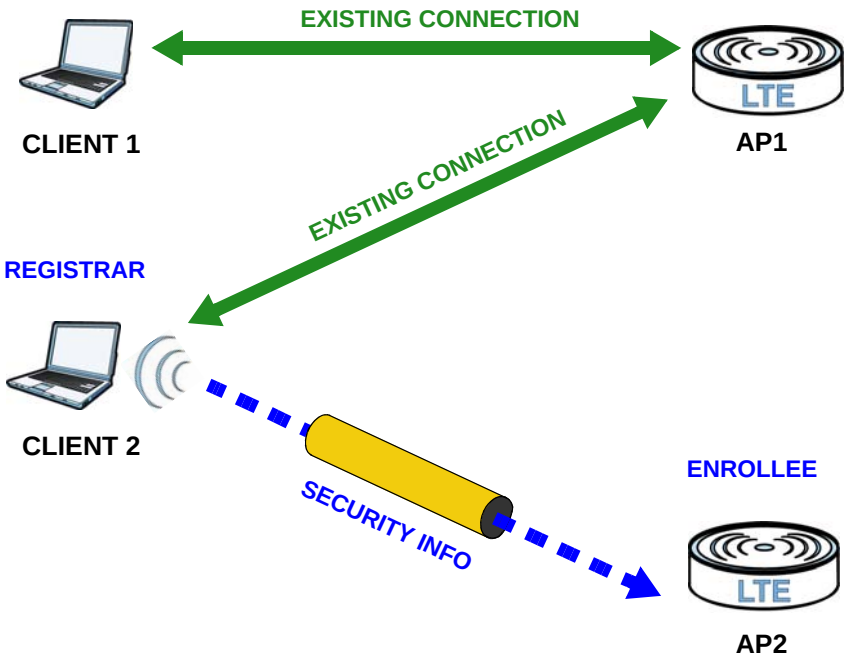

In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the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

**Figure 33** WPS: Example Network Step 2



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

**Figure 34** WPS: Example Network Step 3




### 5.7.6.5 Limitations of WPS

WPS has some limitations of which you should be aware.

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

  For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way.
- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

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

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

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

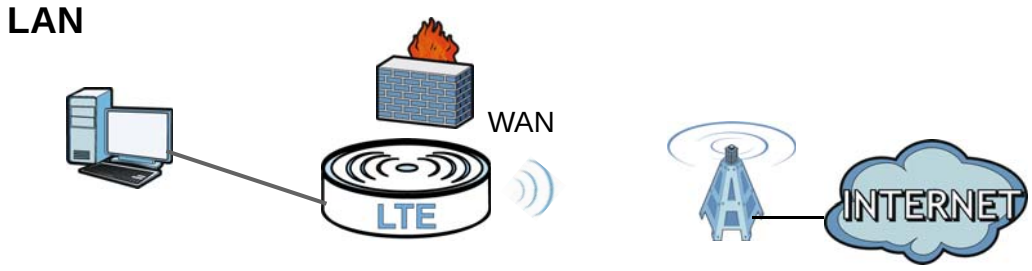
# 6

# Home Networking

## 6.1 Overview

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

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




### 6.1.1 What You Can Do in this Chapter

- Use the **LAN Setup** screen to set the LAN IP address, DHCP, subnet mask, and DNS settings (Section 6.2 on page 69).
- Use the **Static DHCP** screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses (Section 6.3 on page 70).
- Use the **UPnP** screen to enable UPnP (Section 6.4 on page 71).

### 6.1.2 What You Need To Know

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

#### 6.1.2.1 About LAN

##### IP Address

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

### Subnet Mask

The subnet mask specifies the network number portion of an IP address. Your LTE Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the LTE Device unless you are instructed to do otherwise.

### DHCP

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

### DNS

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

## 6.1.2.2 About UPnP

### How do I know if I'm using UPnP?

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

### Cautions with UPnP

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

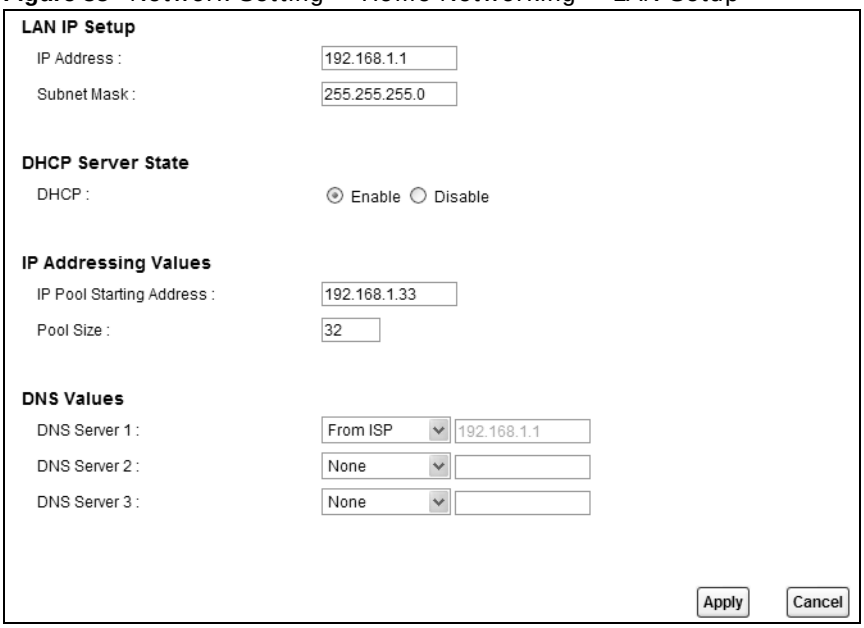
When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the LTE Device allows multicast messages on the LAN only.

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

# 6.2 The LAN Setup Screen

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

**Figure 35** Network Setting > Home Networking > LAN Setup




The following table describes the fields in this screen.

**Table 21** Network Setting > Home Networking > LAN Setup

| LABEL | DESCRIPTION |
|---|---|
| LAN IP Setup | |
| IP Address | Enter the LAN IP address you want to assign to your LTE Device in dotted decimal notation, for example, 192.168.1.1 (factory default). |
| IP Subnet Mask | Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your LTE Device automatically computes the subnet mask based on the IP address you enter, so do not change this field unless you are instructed to do so. |
| DHCP Server State | |
| DHCP | Select **Enable** to have your LTE Device assign IP addresses, an IP default gateway and DNS servers to LAN computers and other devices that are DHCP clients.<br>If you select **Disable**, you need to manually configure the IP addresses of the computers and other devices on your LAN.<br>When DHCP is used, the following fields need to be set. |
| IP Addressing Values | |
| IP Pool Starting Address | This field specifies the first of the contiguous addresses in the IP address pool. |
| Pool Size | This field specifies the size, or count of the IP address pool. |
| DNS Values | |

**Table 21** Network Setting > Home Networking > LAN Setup (continued)

| LABEL | DESCRIPTION |
|---|---|
| DNS Server 1-3 | Select **From ISP** if your ISP dynamically assigns DNS server information (and the LTE Device's WAN IP address).<br><br>Select **DNS-Proxy** to have the LTE Device send its own address to the LAN clients for them to use as the DNS server.<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. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**.<br><br>Select **None** if you do not want to configure DNS servers. You must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

# 6.3 The Static DHCP Screen

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

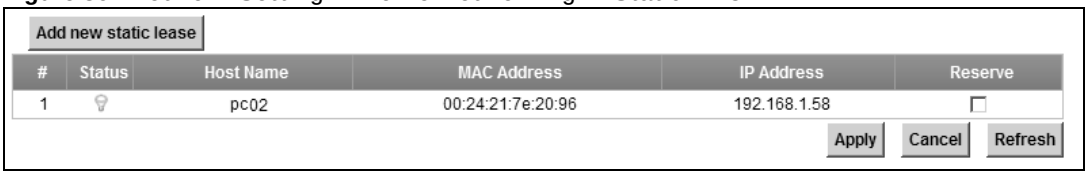
Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

## 6.3.1 Before You Begin

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

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

**Figure 36** Network Setting > Home Networking > Static DHCP




The following table describes the labels in this screen.

**Table 22** Network Setting > Home Networking > Static DHCP

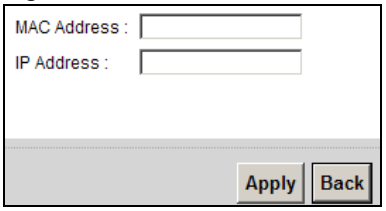
| LABEL | DESCRIPTION |
|---|---|
| Add new static lease | Click this to add a new static DHCP entry. |
| # | This is the index number of the entry. |

**Table 22** Network Setting > Home Networking > Static DHCP (continued)

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

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

**Figure 37** Static DHCP: Add




The following table describes the labels in this screen.

**Table 23** Static DHCP: Add

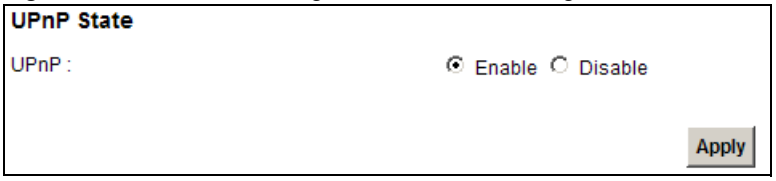
| LABEL | DESCRIPTION |
|---|---|
| MAC Address | Enter the MAC address of a computer on your LAN. |
| IP Address | Enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify. |
| Apply | Click **Apply** to save your changes. |
| Back | Click **Back** to exit this screen without saving. |

# 6.4 The UPnP Screen

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

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

**Figure 38** Network Setting > Home Networking > UPnP




The following table describes the labels in this screen.

**Table 24** Network Settings > Home Networking > UPnP

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

# 7

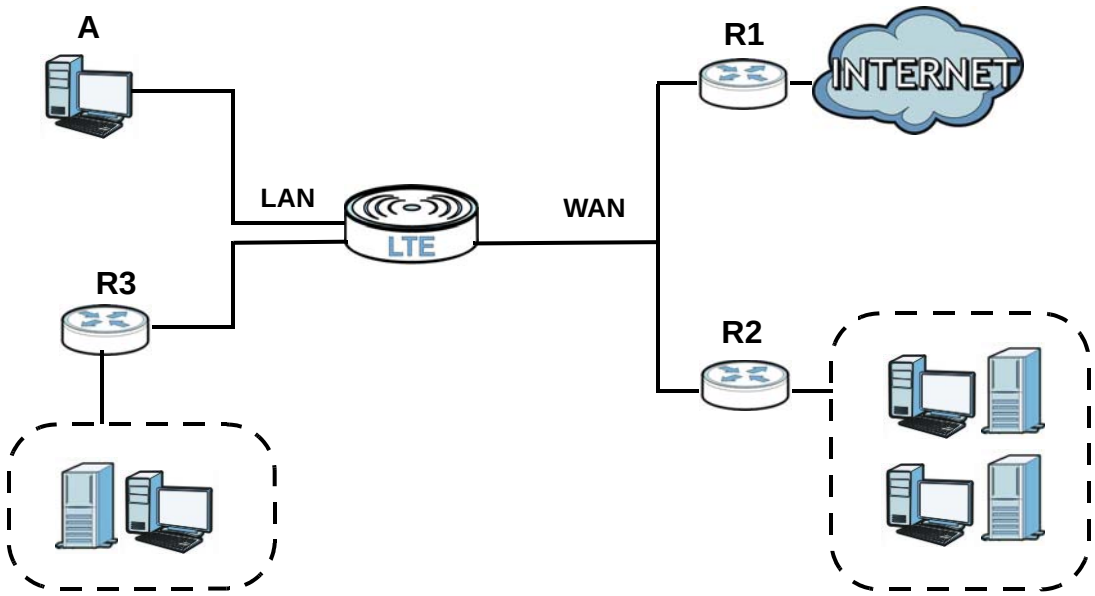
# Routing

## 7.1 Overview

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

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

**Figure 39** Example of Static Routing Topology



# 7.2 Configuring Static Route

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

**Figure 40** Network Setting > Static Route


The following table describes the labels in this screen.

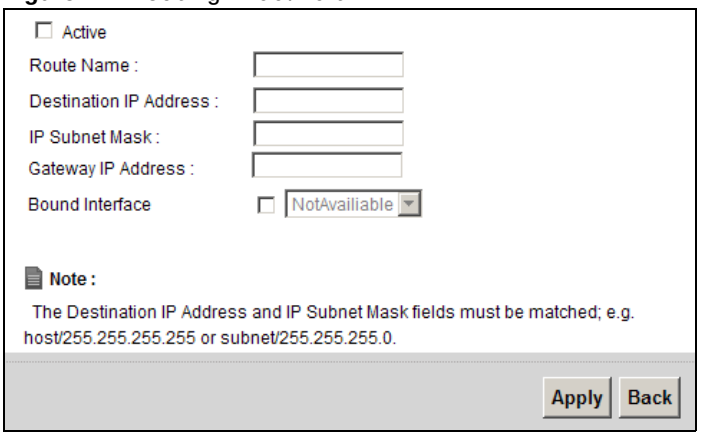
**Table 25** Network Setting > Static Route

| LABEL | DESCRIPTION |
|---|---|
| Add New Static Route | Click this to set up a new static route on the LTE Device. |
| # | This is the number of an individual static route. |
| Active | This indicates whether the rule is active or not.<br>A yellow bulb signifies that this static route is active. A gray bulb signifies that this static route is not active. |
| Status | This shows whether the static route is currently in use or not. A yellow bulb signifies that this static route is in use. A gray bulb signifies that this static route is not in use. |
| Name | This is the name that describes or identifies this route. |
| Destination IP | This parameter specifies the IP network address of the final destination. Routing is always based on network number. |
| 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. |
| Subnet Mask | This parameter specifies the IP network subnet mask of the final destination. |
| Interface | This indicates which interface handles the traffic forwarded by this route. |
| Modify | Click the **Edit** icon to go to the screen where you can set up a static route on the LTE Device.<br>Click the **Delete** icon to remove a static route from the LTE Device. |

## 7.2.1 Add/Edit Static Route

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

**Figure 41** Routing: Add/Edit




The following table describes the labels in this screen.

**Table 26** Routing: Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Active | Click this to activate this static route. |
| Route Name | Enter the name of the IP static route. Leave this field blank to delete this static route. |
| Destination IP Address | This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID. |
| IP Subnet Mask | Enter the IP subnet mask here. |
| Gateway IP Address | You can decide if you want to forward packets to a gateway IP address or a bound interface.<br>If you want to configure **Gateway IP Address**, enter the IP address of the next-hop gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations. |
| Bound Interface | You can decide if you want to forward packets to a gateway IP address or a bound interface.<br>If you want to configure **Bound Interface**, select the check box and choose an interface through which the traffic is sent. |
| Apply | Click **Apply** to save your changes. |
| Back | Click **Back** to exit this screen without saving. |

# 8

# Quality of Service (QoS)

## 8.1 Overview

This chapter discusses the LTE Device's **QoS** screens. Use these screens to set up your LTE Device to use QoS for traffic management.

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. QoS allows the LTE Device to group and prioritize application traffic and fine-tune network performance.

Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

The LTE Device assigns each packet a priority and then queues the packet accordingly. Packets assigned a high priority are processed more quickly than those with low priority if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video.

### 8.1.1 What You Can Do in this Chapter

- Use the **General** screen to enable QoS, set the bandwidth, and allow the LTE Device to automatically assign priority to upstream traffic according to the IP precedence or packet length (Section 8.2 on page 78).
- Use the **Queue Setup** screen to configure QoS queue assignment (Section 8.3 on page 79).
- Use the **Class Setup** screen to set up classifiers to sort traffic into different flows and assign priority and define actions to be performed for a classified traffic flow (Section 8.4 on page 80).
- Use the **Monitor** screen to view the LTE Device's QoS-related packet statistics (Section 8.5 on page 84).

### 8.1.2 What You Need to Know

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

#### QoS versus Cos

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. CoS (class of service) is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

CoS technology includes DiffServ (Differentiated Services or DS). DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit ToS (Type of Service) field in the IP header.

### Tagging and Marking

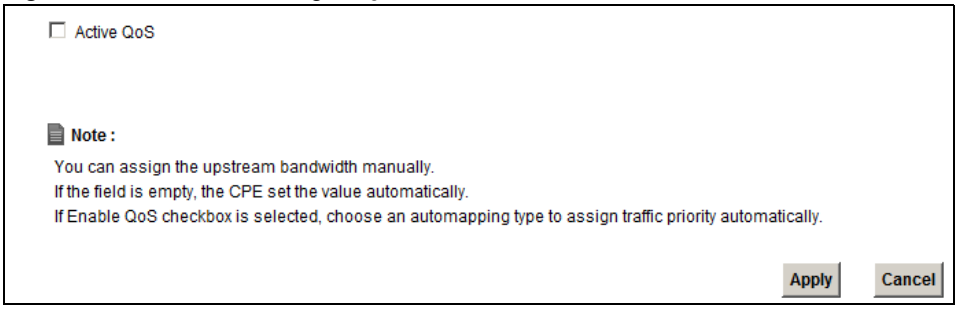
In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or service based on the tag or marker.

## 8.2 The QoS General Screen

Use this screen to enable or disable QoS, set the bandwidth, and select to have the LTE Device automatically assign priority to upstream traffic according to the IP precedence or packet length.

Click **Network Setting > QoS** to open the **General** screen.

**Figure 42** Network Setting > QoS > General




The following table describes the labels in this screen.

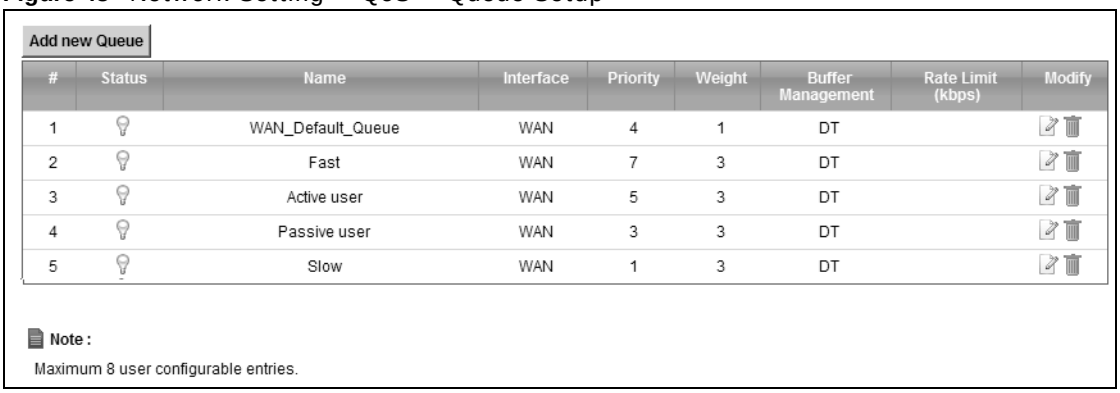
**Table 27** Network Setting > QoS > General

| LABEL | DESCRIPTION |
|---|---|
| Active QoS | Select the check box to turn on QoS to improve your network performance.<br><br>You can give priority to traffic that the LTE Device forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

# 8.3 The Queue Setup Screen

Use this screen to configure QoS queue assignment. Click **Network Setting > QoS > Queue Setup** to open the screen as shown next.

**Figure 43** Network Setting > QoS > Queue Setup




The following table describes the labels in this screen.

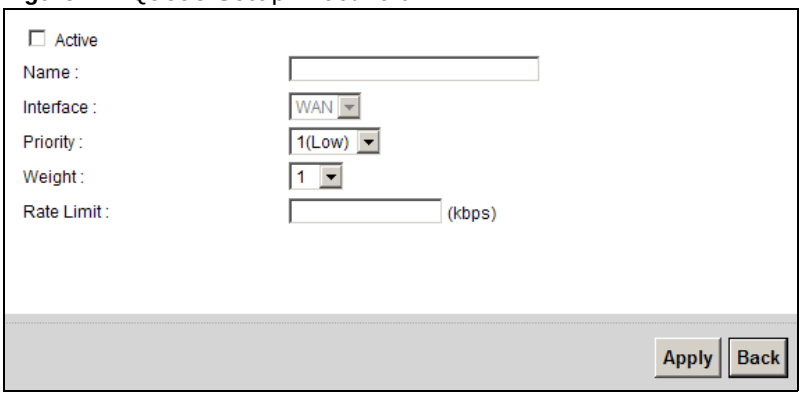
**Table 28** Network Setting > QoS > Queue Setup

| LABEL | DESCRIPTION |
|---|---|
| Add new Queue | Click this to create a new entry. |
| # | This is the index number of this entry. |
| Status | This indicates whether the queue is active or not.<br>A yellow bulb signifies that this queue is active. A gray bulb signifies that this queue is not active. |
| Name | This shows the descriptive name of this queue. |
| Interface | This shows the name of the LTE Device's interface through which traffic in this queue passes. |
| Priority | This shows the priority of this queue. |
| Weight | This shows the weight of this queue. |
| Buffer Management | This shows the queue management algorithm used by the LTE Device. |
| Rate Limit (kbps) | This shows the maximum transmission rate allowed for traffic on this queue. |
| Modify | Click the **Edit** icon to edit the queue.<br>Click the **Delete** icon to delete an existing queue. Note that subsequent rules move up by one when you take this action. |

### 8.3.1 Add/Edit a QoS Queue

Use this screen to configure a queue. Click **Add new Queue** in the **Queue Setup** screen or the **Edit** icon next to an existing queue.

**Figure 44** Queue Setup: Add/Edit




The following table describes the labels in this screen.

**Table 29** Queue Setup: Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Active | Select to enable or disable this queue. |
| Name | Enter the descriptive name of this queue. |
| Interface | This shows the interface of this queue. |
| Priority | Select the priority level (from 1 to 7) of this queue.<br>The larger the number, the higher the priority level. Traffic assigned to higher priority queues gets through faster while traffic in lower priority queues is dropped if the network is congested. |
| Weight | Select the weight (from 1 to 15) of this queue.<br>If two queues have the same priority level, the LTE Device divides the bandwidth across the queues according to their weights. Queues with larger weights get more bandwidth than queues with smaller weights. |
| Rate Limit | Specify the maximum transmission rate (in Kbps) allowed for traffic on this queue. |
| Apply | Click **Apply** to save your changes. |
| Back | Click **Back** to return to the previous screen without saving. |

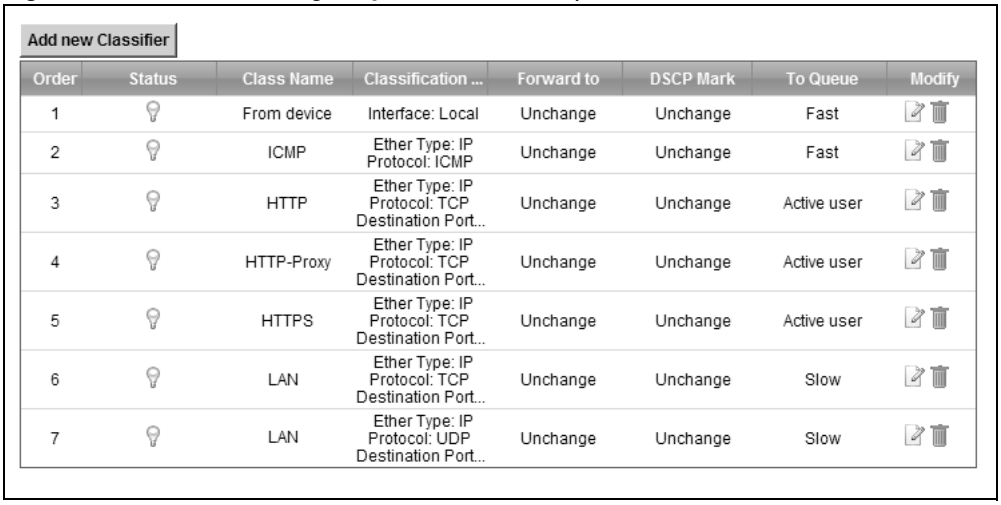
## 8.4 The Class Setup Screen

Use this screen to add, edit or delete QoS classifiers. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming interface. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

You can give different priorities to traffic that the LTE Device forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.

Click **Network Setting > QoS > Class Setup** to open the following screen.

**Figure 45** Network Setting > QoS > Class Setup




The following table describes the labels in this screen.

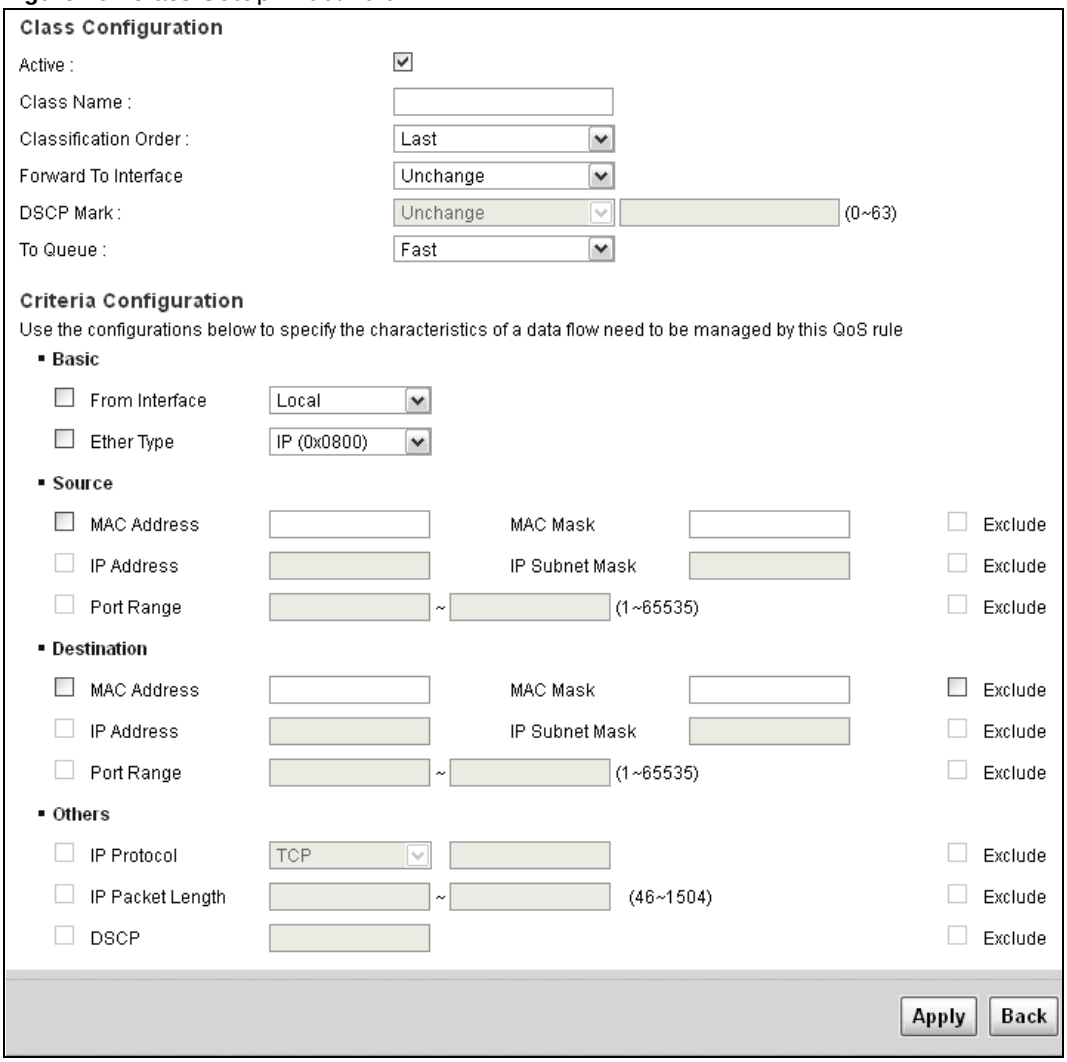
**Table 30** Network Setting > QoS > Class Setup

| LABEL | DESCRIPTION |
|---|---|
| Add new Classifier | Click this to create a new classifier. |
| Order | This field displays the order number of the classifier. |
| Status | This indicates whether the classifier is active or not.<br>A yellow bulb signifies that this classifier is active. A gray bulb signifies that this classifier is not active. |
| Class Name | This is the name of the classifier. |
| Classification Criteria | This shows criteria specified in this classifier, for example the interface from which traffic of this class should come and the source MAC address of traffic that matches this classifier. |
| Forward to | This is the interface through which traffic that matches this classifier is forwarded out. |
| DSCP Mark | This is the DSCP number added to traffic of this classifier. |
| To Queue | This is the name of the queue in which traffic of this classifier is put. |
| Modify | Click the **Edit** icon to edit the classifier.<br>Click the **Delete** icon to delete an existing classifier. Note that subsequent rules move up by one when you take this action. |

## 8.4.1 Add/Edit QoS Class

Click **Add new Classifier** in the **Class Setup** screen or the **Edit** icon next to an existing classifier to configure it.

**Figure 46** Class Setup: Add/Edit




The following table describes the labels in this screen.

**Table 31** Class Setup: Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Class Configuration | |
| Active | Select to enable this classifier. |
| Class Name | Enter a descriptive name of up to 32 printable English keyboard characters, including spaces. |
| Classification Order | Select an existing number for where you want to put this classifier to move the classifier to the number you selected after clicking **Apply**.<br><br>Select **Last** to put this rule in the back of the classifier list. |

**Table 31** Class Setup: Add/Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Forward to Interface | Select a WAN interface through which traffic of this class will be forwarded out. If you select **Unchange**, the LTE Device forward traffic of this class according to the default routing table. |
| DSCP Mark | This field is available only when you select the **Ether Type** check box in **Criteria Configuration-Basic** section.<br>If you select **Mark**, enter a DSCP value with which the LTE Device replaces the DSCP field in the packets.<br>If you select **Unchange**, the LTE Device keep the DSCP field in the packets. |
| To Queue | Select a queue that applies to this class.<br>You should have configured a queue in the **Queue Setup** screen already. |
| Criteria Configuration<br>Use the following fields to configure the criteria for traffic classification. | |
| Basic | |
| From Interface | Select whether the traffic class comes from the **LTE**, **Local**, or **Lan** interface. |
| Ether Type | Select a predefined application to configure a class for the matched traffic.<br>If you select **IP**, you also need to configure source or destination MAC address, IP address, DHCP options, DSCP value or the protocol type. |
| Source | |
| MAC Address | Select the check box and enter the source MAC address of the packet. |
| MAC Mask | Type the mask for the specified MAC address to determine which bits a packet's MAC address should match.<br>Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria. |
| IP Address | Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address. |
| IP Subnet Mask | Enter the source subnet mask. |
| Port Range | If you select **TCP** or **UDP** in the **IP Protocol** field, select the check box and enter the port number(s) of the source. |
| Exclude | Select this option to exclude the packets that match the specified criteria from this classifier. |
| Destination | |
| MAC Address | Select the check box and enter the destination MAC address of the packet. |
| MAC Mask | Type the mask for the specified MAC address to determine which bits a packet's MAC address should match.<br>Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria. |
| IP Address | Select the check box and enter the destination IP address in dotted decimal notation. A blank source IP address means any source IP address. |
| IP Subnet Mask | Enter the destination subnet mask. |

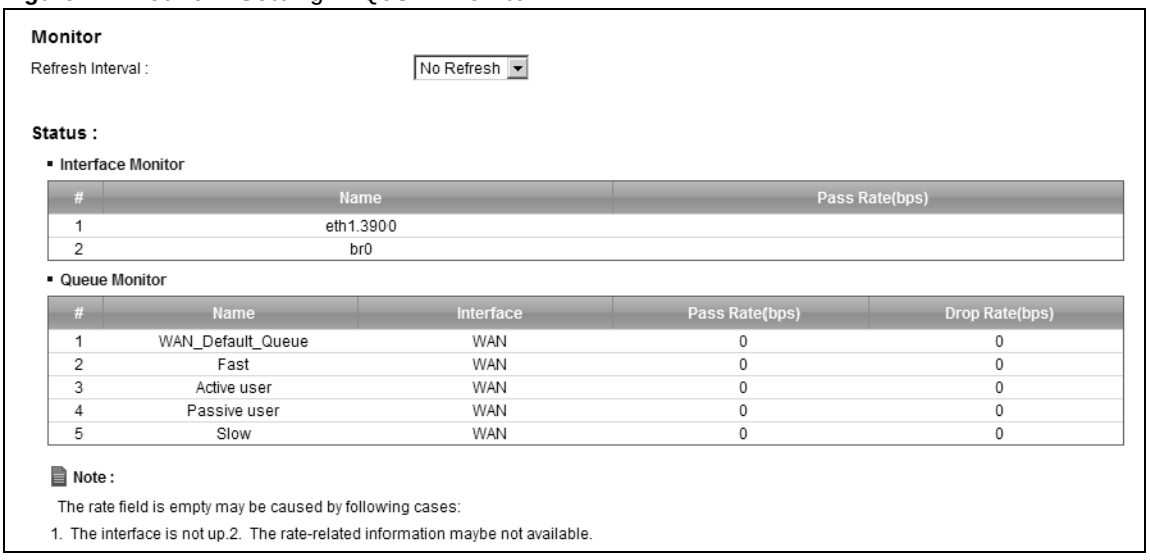
**Table 31** Class Setup: Add/Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Port Range | If you select **TCP** or **UDP** in the **IP Protocol** field, select the check box and enter the port number(s) of the source. |
| Exclude | Select this option to exclude the packets that match the specified criteria from this classifier. |
| Others | |
| IP Protocol | This field is available only when you select **IP** in the **Ether Type** field.<br>Select this option and select the protocol (service type) from **TCP** or **UDP**. If you select **User defined**, enter the protocol (service type) number. |
| IP Packet Length | This field is available only when you select **IP** in the **Ether Type** field.<br>Select this option and enter the minimum and maximum packet length (from 46 to 1504) in the fields provided. |
| DSCP | This field is available only when you select **IP** in the **Ether Type** field.<br>Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided. |
| Exclude | Select this option to exclude the packets that match the specified criteria from this classifier. |
| Apply | Click **Apply** to save your changes. |
| Back | Click **Back** to return to the previous screen without saving. |

# 8.5 The QoS Monitor Screen

To view the LTE Device's QoS packet statistics, click **Network Setting > QoS > Monitor**. The screen appears as shown.

**Figure 47** Network Setting > QoS > Monitor



The following table describes the labels in this screen.

**Table 32** Network Setting > QoS > Monitor

| LABEL | DESCRIPTION |
|---|---|
| Monitor | |
| Refresh Interval | Select how often you want the LTE Device to update this screen. Select **No Refresh** to stop refreshing statistics. |
| Status | |
| # | This is the index number of the entry. |
| Name | This shows the name of the WAN interface on the LTE Device. |
| Pass Rate (bps) | This shows how much traffic (bps) forwarded to this interface are transmitted successfully. |
| Queue Monitor | |
| # | This is the index number of the entry. |
| Name | This shows the name of the queue. |
| Pass Rate (bps) | This shows how much traffic (bps) assigned to this queue are transmitted successfully. |
| Drop Rate (bps) | This shows how much traffic (bps) assigned to this queue are dropped. |

# 8.6 QoS Technical Reference

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

## 8.6.1 DiffServ

QoS is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

DiffServ (Differentiated Services) 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 (DSCPs) 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.

### 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.

| DSCP (6 bits) | Unused (2 bits) |
|---|---|

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 kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

# 9

# Network Address Translation (NAT)

## 9.1 Overview

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

### 9.1.1 What You Can Do in this Chapter

- Use the **Port Forwarding** screen to configure forward incoming service requests to the server(s) on your local network (Section 9.2 on page 88).
- Use the **DMZ** screen to view and configure the IP address of your network DMZ. (Section 9.3 on page 91).
- Use the **Sessions** screen to limit the number of concurrent NAT sessions each client can use (Section 9.4 on page 91).

### 9.1.2 What You Need To Know

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

#### Inside/Outside and Global/Local

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

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

#### NAT

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

### Port Forwarding

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

### Finding Out More

See Section 9.5 on page 92 for advanced technical information on NAT.

## 9.2 The Port Forwarding Screen

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

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

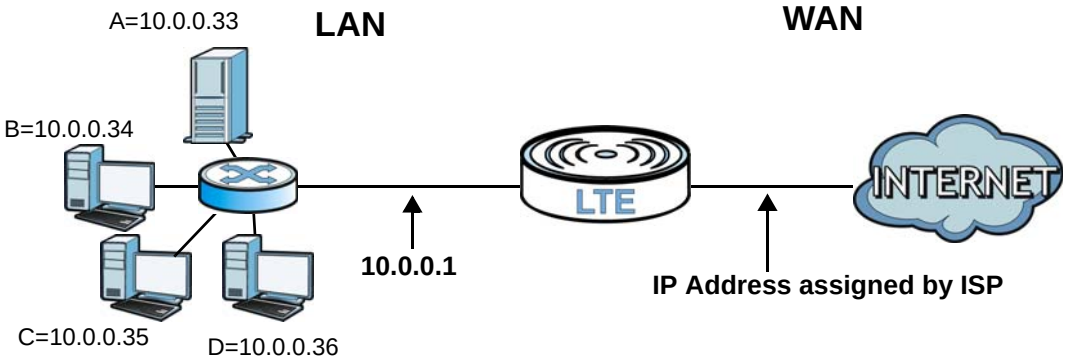
The most often used port numbers and services are shown in Appendix D on page 207. Please refer to RFC 1700 for further information about port numbers.

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

### Configuring Servers Behind Port Forwarding (Example)

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

**Figure 48** Multiple Servers Behind NAT Example

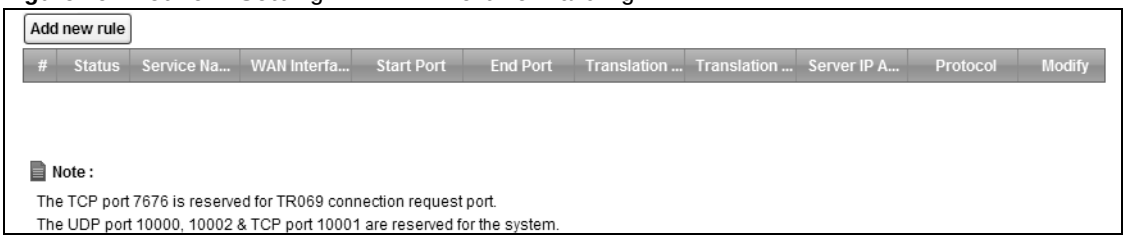


## 9.2.1 The Port Forwarding Screen

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

See Appendix D on page 207 for port numbers commonly used for particular services.

**Figure 49** Network Setting > NAT > Port Forwarding




The following table describes the fields in this screen.

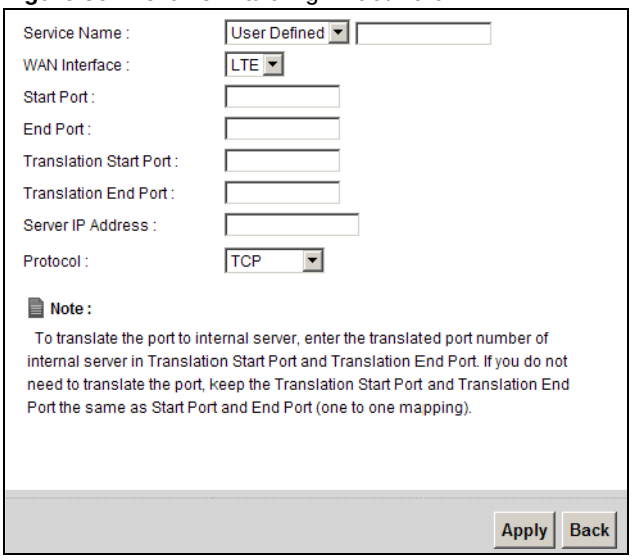
**Table 33** Network Setting > NAT > Port Forwarding

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

## 9.2.2 The Port Forwarding Edit Screen

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

**Figure 50** Port Forwarding: Add/Edit




The following table describes the labels in this screen.

**Table 34** Port Forwarding: Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Service Name | Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on). |
| WAN Interface | This is the WAN interface through which the service is forwarded. |
| Start Port | Enter the original destination port for the packets.<br>To forward only one port, enter the port number again in the **External End Port** field.<br>To forward a series of ports, enter the start port number here and the end port number in the **External End Port** field. |
| End Port | Enter the last port of the original destination port range.<br>To forward only one port, enter the port number in the **External Start Port** field above and then enter it again in this field.<br>To forward a series of ports, enter the last port number in a series that begins with the port number in the **External Start Port** field above. |
| Translation Start Port | This shows the port number to which you want the LTE Device to translate the incoming port. For a range of ports, enter the first number of the range to which you want the incoming ports translated. |
| Translation End Port | This shows the last port of the translated port range. |
| Server IP Address | Enter the inside IP address of the virtual server here. |
| Protocol | Select the protocol supported by this virtual server. Choices are **TCP**, **UDP**, or **TCP/UDP**. |
| Apply | Click **Apply** to save your changes. |
| Back | Click **Back** to return to the previous screen without saving. |

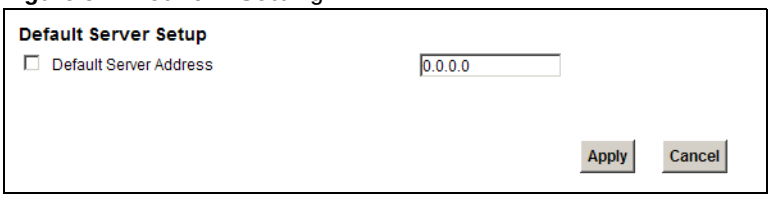
# 9.3 The DMZ Screen

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

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

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

**Figure 51** Network Setting > NAT > DMZ




The following table describes the fields in this screen.

**Table 35** Network Setting > NAT > DMZ

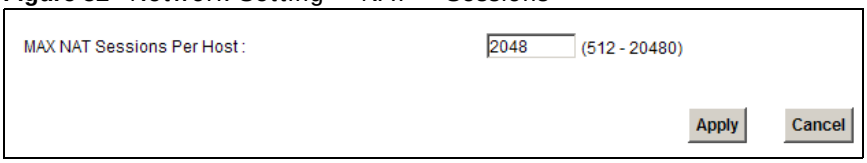
| LABEL | DESCRIPTION |
|---|---|
| Default Server Address | Enter the IP address of your network DMZ host, if you have one. **0.0.0.0** means this feature is disabled. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

# 9.4 The Sessions Screen

Use the **Sessions** screen to limit the number of concurrent NAT sessions each client can use.

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

**Figure 52** Network Setting > NAT > Sessions



The following table describes the fields in this screen.

**Table 36** Network Setting > NAT > Sessions

| LABEL | DESCRIPTION |
|---|---|
| MAX NAT Session | Use this field to set a common limit to the number of concurrent NAT sessions each client computer can have.<br>If only a few clients use peer to peer applications, you can raise this number to improve their performance. With heavy peer to peer application use, lower this number to ensure no single client uses too many of the available NAT sessions. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

# 9.5 Technical Reference

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

## 9.5.1 NAT Definitions

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

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

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

**Table 37** NAT Definitions

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

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

## 9.5.2 What NAT Does

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

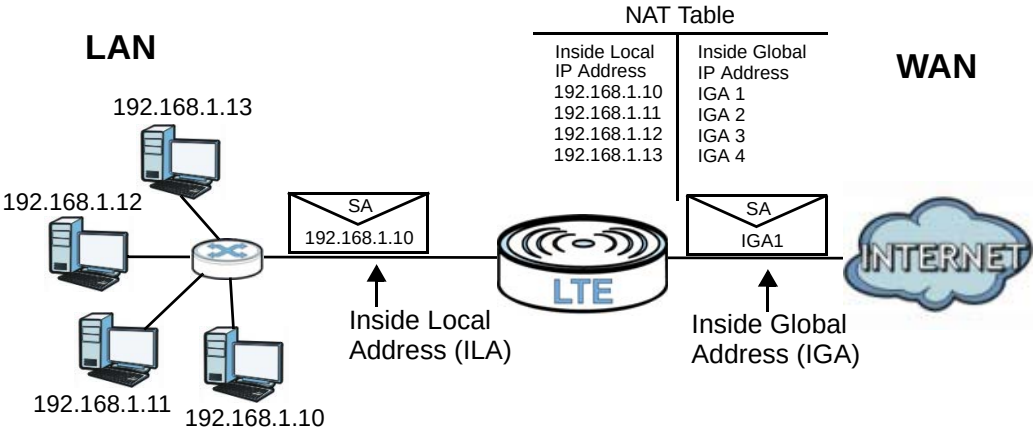
global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

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

## 9.5.3 How NAT Works

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

**Figure 53** How NAT Works



# 10

# Dynamic DNS

## 10.1 Overview

This chapter discusses how to configure your LTE Device to use Dynamic DNS.

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

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

### 10.1.1 What You Need To Know

#### DYNDNS Wildcard

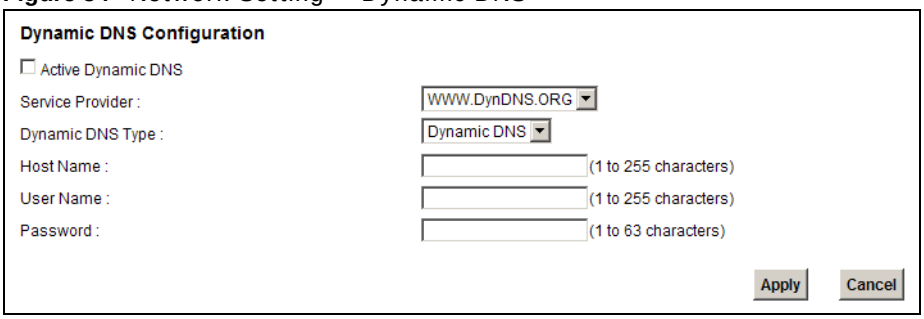
Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

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

# 10.2 The Dynamic DNS Screen

Use the **Dynamic DNS** screen to enable DDNS and configure the DDNS settings on the LTE Device. To change your LTE Device's DDNS, click **Network Setting > Dynamic DNS**. The screen appears as shown.

**Figure 54** Network Setting > Dynamic DNS




The following table describes the fields in this screen.

**Table 38** Network Setting > DNS

| LABEL | DESCRIPTION |
|---|---|
| Dynamic DNS Configuration | |
| Active Dynamic DNS | Select this check box to use dynamic DNS. |
| Service Provider | Select the name of your Dynamic DNS service provider. |
| Dynamic DNS Type | Select the type of service that you are registered for from your Dynamic DNS service provider. |
| Host Name | Type the domain name assigned to your LTE Device by your Dynamic DNS provider.<br>You can specify up to two host names in the field separated by a comma (","). |
| User Name | Type your user name. |
| Password | Type the password assigned to you. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

# 11

# Firewall

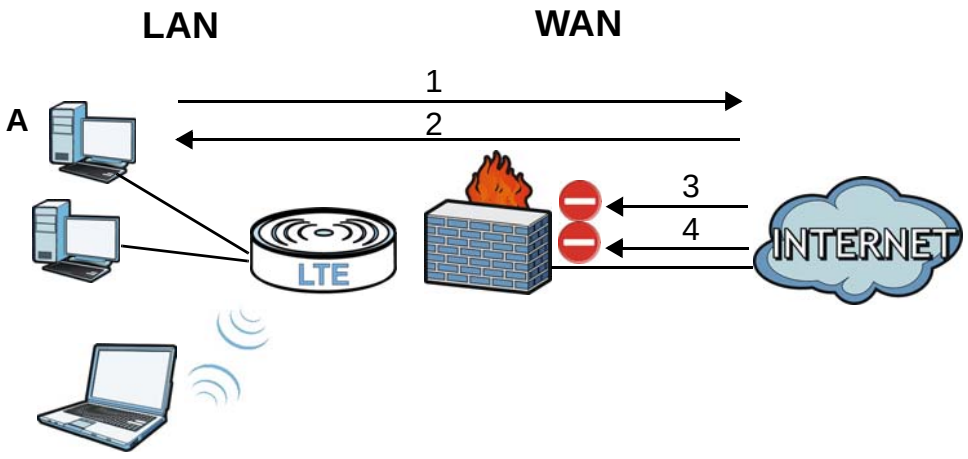
## 11.1 Overview

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

- Allows traffic that originates from your LAN computers to go to all other networks.
- Blocks traffic that originates on 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 55** Default Firewall Action




### 11.1.1 What You Can Do in this Chapter

- Use the **General** screen to enable or disable the LTE Device's firewall (Section 11.2 on page 99).
- Use the **Services** screen to view the configured firewall rules and add, edit or remove a firewall rule (Section 11.3 on page 100).
- Use the **Access Control** screen to view and configure incoming/outgoing filtering rules (Section 11.4 on page 101).
- Use the **DoS** screen to enable or disable Denial of Service (DoS) protection (Section 11.4 on page 101).

## 11.1.2 What You Need to Know

### DoS

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

### Firewall

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

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

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

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

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

### ICMP

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

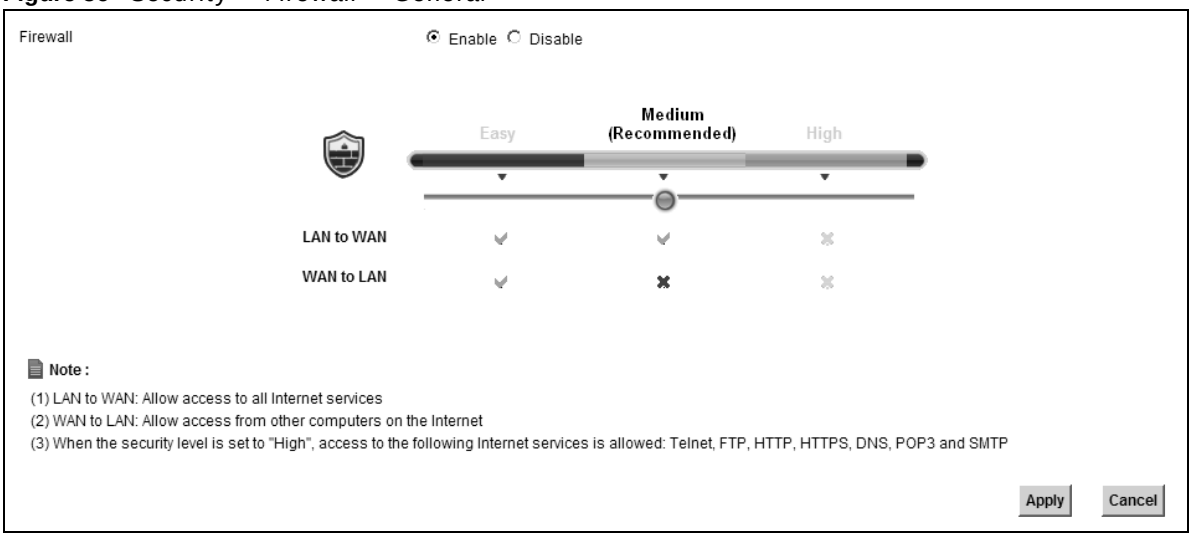
### Finding Out More

See Section 11.6 on page 104 for advanced technical information on firewall.

# 11.2 The General Screen

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

**Figure 56** Security > Firewall > General




The following table describes the labels in this screen.

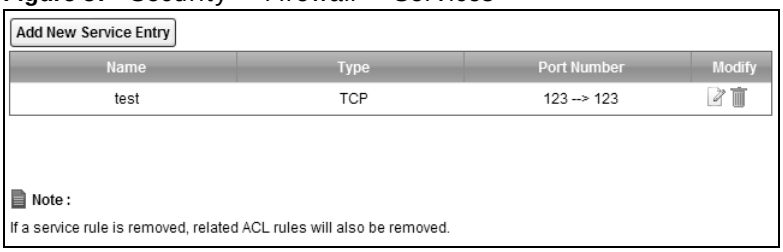
**Table 39** Security > Firewall > General

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

# 11.3 The Services Screen

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

**Figure 57** Security > Firewall > Services




Each field is described in the following table.

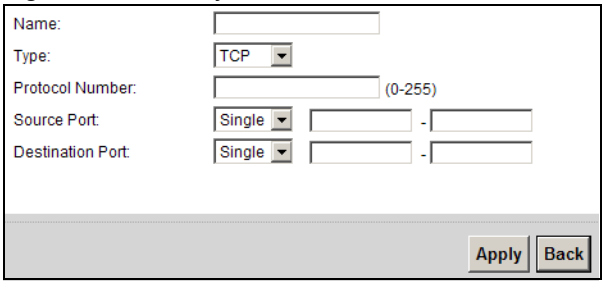
**Table 40** Security > Firewall > Services

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

## 11.3.1 The Add New Services Entry Screen

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

**Figure 58** Security > Firewall > Services > Add New Service Entry



Each field is described in the following table.

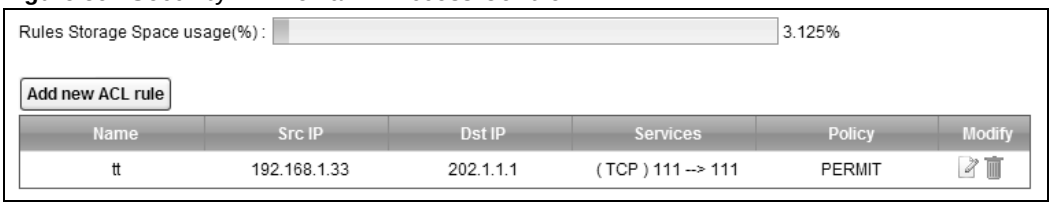
**Table 41** Security > Firewall > Services > Add New Service Entry

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

# 11.4 The Access Control Screen

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

**Figure 59** Security > Firewall > Access Control




Each field is described in the following table.

**Table 42** Security > Firewall > Access Control

| LABEL | DESCRIPTION |
|---|---|
| Rules Storage Space usage(%) | This bar shows the percentage of the LTE Device's space has been used. If the usage is almost full, you may need to remove an existing filter rule before you create a new one. |
| Add new ACL rule | Click this to go to add a filter rule for incoming or outgoing IP traffic. |
| Name | This displays the name of the rule. |
| Src IP | This displays the source IP addresses to which this rule applies. Please note that a blank source address is equivalent to **Any**. |
| Dst IP | This displays the destination IP addresses to which this rule applies. Please note that a blank destination address is equivalent to **Any**. |
| Services | This displays the protocol type and a port range that define the service to which this rule applies. |

**Table 42** Security > Firewall > Access Control (continued)

| LABEL | DESCRIPTION |
|---|---|
| Policy | This field displays whether the rule silently discards packets (**DROP**), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender (**REJECT**) or allows the passage of packets (**PERMIT**). |
| Modify | Click the **Edit** icon to edit the rule.<br>Click the **Delete** icon to delete an existing rule. Note that subsequent rules move up by one when you take this action. |

## 11.4.1 The Add New ACL Rule/Edit Screen

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

**Figure 60** Security > Firewall > Access Control > Add New ACL Rule/Edit


Each field is described in the following table.

**Table 43** Security > Firewall > Access Control > Add New ACL Rule/Edit

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

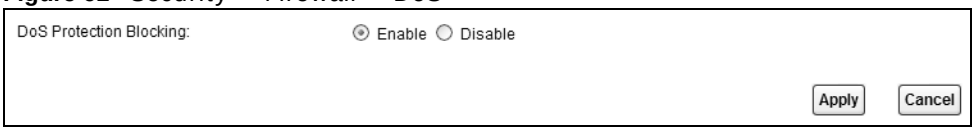
**Table 43** Security > Firewall > Access Control > Add New ACL Rule/Edit (continued)

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

# 11.5 The DoS Screen

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

**Figure 61** Security > Firewall > DoS



Each field is described in the following table.

**Table 44** Security > Firewall > DoS

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

# 11.6 Firewall Technical Reference

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

## 11.6.1 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.
3. Limit who can access your LTE Device.
4. Don't enable any local service (such as Telnet or FTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
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. Keep the firewall in a secured (locked) room.

## 11.6.2 Security Considerations

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

Consider these security ramifications before creating a rule:

1. Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
2. Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?

**3** Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.

**4** Does this rule conflict with any existing rules?

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

# 12

# MAC Filter

## 12.1 Overview

This chapter discusses MAC address filtering.

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

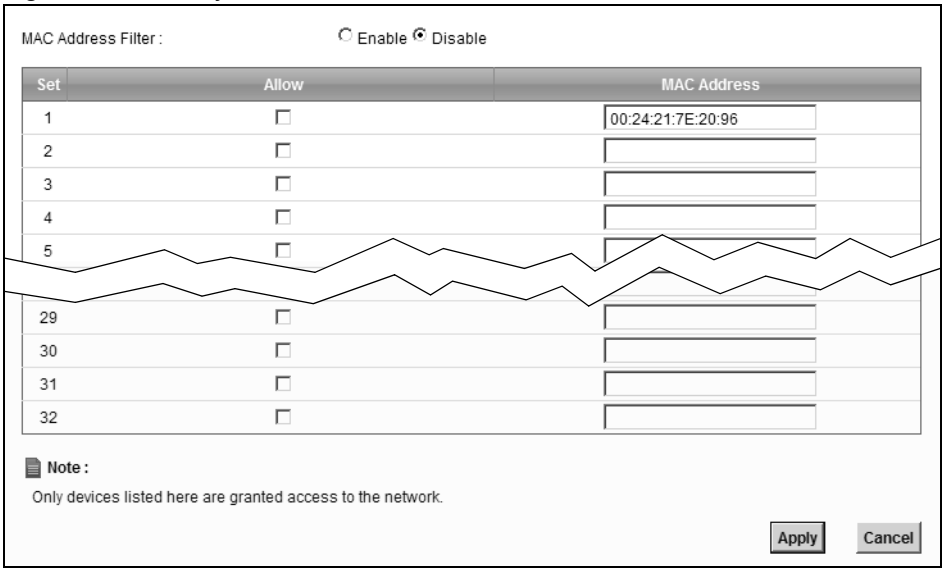
### 12.1.1 What You Need to Know

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

## 12.2 The MAC Filter Screen

Use the **MAC Filter** screen to allow wireless and LAN clients access to the LTE Device. To change your LTE Device's MAC filter settings, click **Security** > **MAC Filter**. The screen appears as shown.

**Figure 62** Security > MAC Filter



The following table describes the labels in this menu.

**Table 45** Security > MAC Filter

| LABEL | DESCRIPTION |
|---|---|
| MAC Address Filter | Select **Enable** to activate MAC address filtering. |
| Set | This is the index number of the MAC address. |
| Allow | Select **Allow** to permit access to the LTE Device. MAC addresses not listed will be denied access to the LTE Device.<br>If you clear this, the **MAC Address** field for this set clears. |
| MAC Address | Enter the MAC addresses of the wireless station and LAN devices that are allowed access to the LTE Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

# 13

# Parental Control

## 13.1 Overview

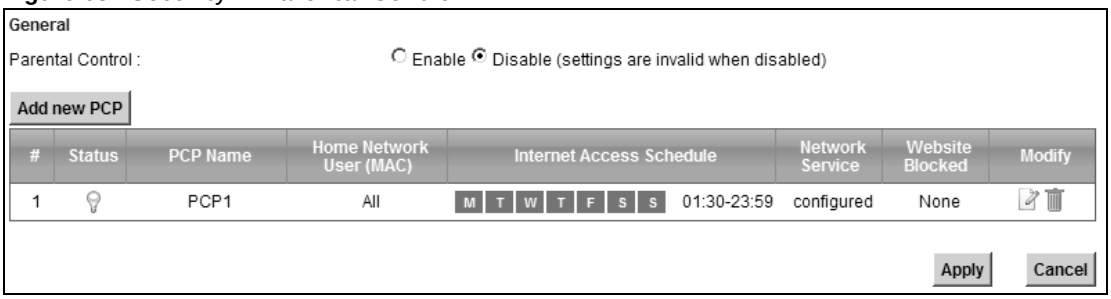
Parental control allows you to block web sites with the specific URL. You can also define time periods and days during which the LTE Device performs parental control on a specific user.

## 13.2 The Parental Control Screen

Use this screen to enable parental control, view the parental control rules and schedules.

Click **Security > Parental Control** to open the following screen.

**Figure 63** Security > Parental Control




The following table describes the fields in this screen.

**Table 46** Parental Control > Parental Control

| LABEL | DESCRIPTION |
|---|---|
| Parental Control | Select **Enable** to activate parental control. |
| Add new PCP | Click this if you want to configure a new parental control rule. |
| # | This shows the index number of the rule. |
| Status | This indicates whether the rule is active or not.<br>A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active. |
| PCP Name | This shows the name of the rule. |
| Home Network User (MAC) | This shows the MAC address of the LAN user's computer to which this rule applies. |
| Internet Access Schedule | This shows the day(s) and time on which parental control is enabled. |
| Network Service | This shows whether the network service is configured. If not, **None** will be shown. |

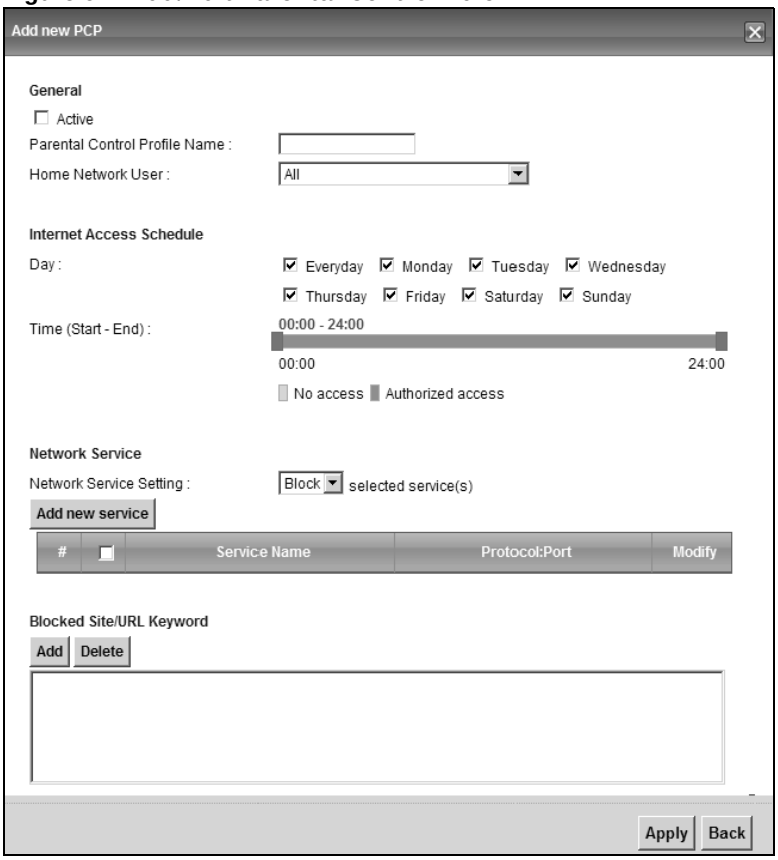
**Table 46** Parental Control > Parental Control (continued)

| LABEL | DESCRIPTION |
|---|---|
| Website Block | This shows whether the website block is configured. If not, **None** will be shown. |
| Modify | Click the **Edit** icon to go to the screen where you can edit the rule.<br>Click the **Delete** icon to delete an existing rule. |
| Add | Click **Add** to create a new schedule. |
| Apply | Click **Apply** to save your changes back to the LTE Device. |

## 13.2.1 Add/Edit a Parental Control Rule

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

**Figure 64** Add/Edit Parental Control Rule




The following table describes the fields in this screen.

**Table 47** Add/Edit Parental Control Rule

| LABEL | DESCRIPTION |
|---|---|
| General | |
| Active | Select the checkbox to activate this parental control rule. |
| Parental Control Profile Name | Enter a descriptive name for the rule. |

**Table 47** Add/Edit Parental Control Rule (continued)

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

# 14.1 Overview

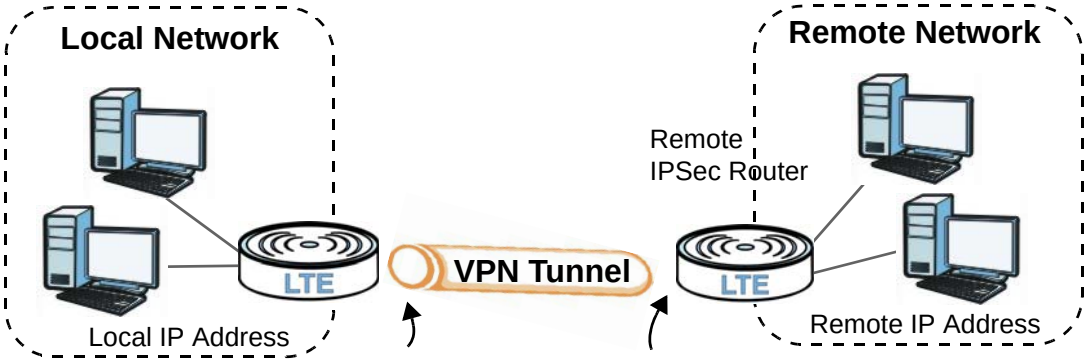
This chapter shows you how to configure the LTE Device's VPN settings.

# 14.2 IPSec VPN

## 14.2.1 The General Screen

The following figure helps explain the main fields in the web configurator.

**Figure 65** IPSec Fields Summary




Click **Security > VPN** to open this screen as shown next.

**Figure 66** IPSec VPN

This screen contains the following fields:

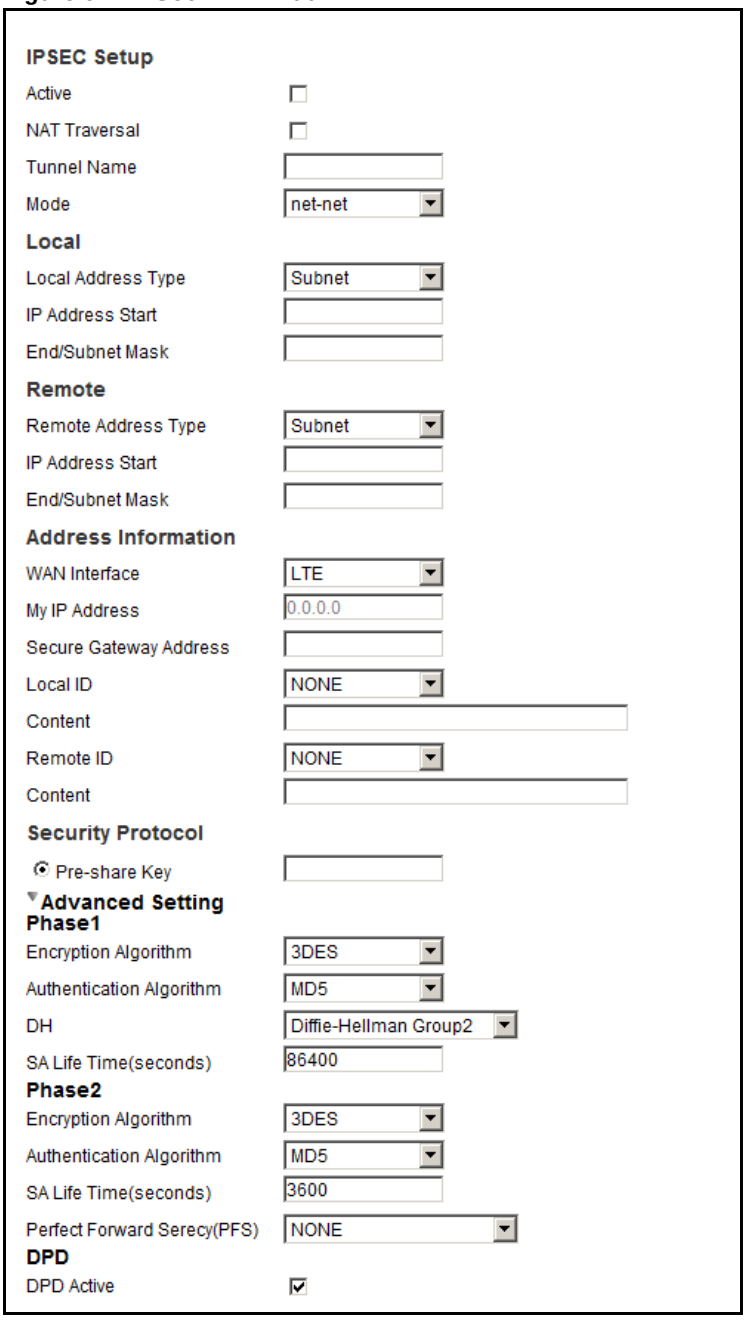
**Table 48** IPSec VPN

| LABEL | DESCRIPTION |
|---|---|
| Add New Tunnel | Click this button to add an item to the list. |
| # | This is the VPN policy index number. |
| Active | This displays if the VPN policy is enabled. |
| Tunnel Name | Enter the name of the VPN connection. |
| Local Address | This displays the IP address of the LTE Device. |
| Remote Address | This displays the IP address of the remote IPSec router. |
| IPSec Algorithm | This displays the encryption algorithm being used for the VPN connection. |

## 14.2.2 IPSec VPN: Add

Use these settings. Click **Security > VPN > Add New Tunnel** to open this screen as shown next.

**Figure 67** IPSec VPN: Add




This screen contains the following fields:

**Table 49** IPSec VPN: Add

| LABEL | DESCRIPTION |
|---|---|
| IPSEC Setup | |
| Active | Select **Active** to activate this VPN policy. |

**Table 49** IPSec VPN: Add

| LABEL | DESCRIPTION |
|---|---|
| NAT Traversal | Select this if any of these conditions are satisfied.<br>• This IKE SA might be used to negotiate IPSec SAs that use ESP as the active protocol.<br>• There are one or more NAT routers between the LTE Device and remote IPSec router, and these routers do not support IPSec pass-thru or a similar feature.<br>The remote IPSec router must also enable NAT traversal, and the NAT routers have to forward packets with UDP port 500 and UDP 4500 headers unchanged. |
| Tunnel Name | Enter the name of the VPN connection. |
| Mode | Select the encapsulation mode. When **net-net** is selected, the connection will operate in tunnel mode. |
| Local | |
| Local Address Type | Select **Single** or **Subnet** to specify if the VPN connection begins at an IP address or subnet. |
| IP Address Start | If **Single** is selected, enter a (static) IP address on the LAN behind your LTE Device.<br>If **Subnet** is selected, specify IP addresses on a network by their subnet mask by entering a (static) IP address on the LAN behind your LTE Device. Then enter the subnet mask to identify the network address. |
| End/Subnet Mask | If **Subnet** is selected, enter the subnet mask to identify the network address. |
| Remote | |
| Remote Address Type | Select **Single** or **Subnet** to specify if the VPN connection terminates at an IP address or subnet. |
| IP Address Start | If **Single** is selected, enter a (static) IP address on the LAN behind the remote IPSec's router.<br>If **Subnet** is selected, specify IP addresses on a network by their subnet mask by entering a (static) IP address on the LAN behind the remote IPSec's router. Then enter the subnet mask to identify the network address. |
| End/Subnet Mask | If **Subnet** is selected, enter the subnet mask to identify the network address. |
| Address Information | |
| WAN Interface | Select the interface for the VPN gateway. |
| My IP Address | Enter the IP address of the LTE Device in the IKE SA. |
| Secure Gateway Address | Enter the IP address of the remote IPSec router in the IKE SA. |
| Local ID | Select **IP** to identify the LTE Device by its IP address.<br>Select **DNS** to identify this LTE Device by a domain name.<br>Select **E-mail** to identify this LTE Device by an e-mail address. |

**Table 49** IPSec VPN: Add

| LABEL | DESCRIPTION |
|---|---|
| Content | When you select **IP** in the **Local ID** field, type the IP address of your computer in the **Content** field. If you configure the **Content** field to 0.0.0.0 or leave it blank, the LTE Device automatically uses the **Pre-Share Key** (refer to the **Pre-Share Key** field description).<br><br>It is recommended that you type an IP address other than 0.0.0.0 in the **Content** field or use the **DNS** or **E-mail** ID type in the following situations.<br><br>• When there is a NAT router between the two IPSec routers.<br>• When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses.<br><br>When you select **DNS** or **E-mail** in the **Local ID** field, type a domain name or e-mail address by which to identify this LTE Device in the **Content** field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string. |
| Remote ID | Select **IP** to identify the remote IPSec router by its IP address.<br><br>Select **DNS** to identify the remote IPSec router by a domain name.<br><br>Select **E-mail** to identify the remote IPSec router by an e-mail address. |
| Content | The configuration of the remote content depends on the remote ID type.<br><br>For **IP**, type the IP address of the computer with which you will make the VPN connection. If you configure this field to 0.0.0.0 or leave it blank, the LTE Device will use the address in the **Secure Gateway Address** field (refer to the **Secure Gateway Address** field description).<br><br>For **DNS** or **E-mail**, type a domain name or e-mail address by which to identify the remote IPSec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.<br><br>It is recommended that you type an IP address other than 0.0.0.0 or use the **DNS** or **E-mail** ID type in the following situations:<br><br>• When there is a NAT router between the two IPSec routers.<br>• When you want the LTE Device to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses. |
| Security Protocol | |
| Pre-Shared Key | Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation.<br><br>Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x" (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", “0x” denotes that the key is hexadecimal and “0123456789ABCDEF” is the key itself. |
| Advanced Setting - Phase 1 | |

**Table 49** IPSec VPN: Add

| LABEL | DESCRIPTION |
|---|---|
| Encryption Algorithm | Select which key size and encryption algorithm to use in the IKE SA. Choices are:<br>**DES** - a 56-bit key with the DES encryption algorithm<br>**3DES** - a 168-bit key with the DES encryption algorithm<br>**AES128** - a 128-bit key with the AES encryption algorithm<br>**AES192** - a 192-bit key with the AES encryption algorithm<br>**AES256** - a 256-bit key with the AES encryption algorithm<br>The LTE Device and the remote IPSec router must use the same key size and encryption algorithm. Longer keys require more processing power, resulting in increased latency and decreased throughput. |
| Authentication Algorithm | Select which hash algorithm to use to authenticate packet data. Choices are **MD5**, **SHA1**, **SHA2-256** and **SHA2-512**. **SHA** is generally considered stronger than **MD5**, but it is also slower. |
| DH | Select which Diffie-Hellman key group you want to use for encryption keys. Choices are:<br>**Diffie-Hellman Group2** - use a 1024-bit random number<br>**Diffie-Hellman Group5** - use a 1536-bit random number<br>**Diffie-Hellman Group14** - use a 2048-bit random number<br>The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group. |
| SA Life Time | Define the length of time before an IPSec SA automatically renegotiates in this field.<br>A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected. |
| Phase 2 | |
| Encryption Algorithm | Select which key size and encryption algorithm to use in the IKE SA. Choices are:<br>**DES** - a 56-bit key with the DES encryption algorithm<br>**3DES** - a 168-bit key with the DES encryption algorithm<br>**AES128** - a 128-bit key with the AES encryption algorithm<br>**AES192** - a 192-bit key with the AES encryption algorithm<br>**AES256** - a 256-bit key with the AES encryption algorithm<br>The LTE Device and the remote IPSec router must use the same key size and encryption algorithm. Longer keys require more processing power, resulting in increased latency and decreased throughput. |
| Authentication Algorithm | Select which hash algorithm to use to authenticate packet data. Choices are **MD5**, **SHA1**, **SHA2-256** and **SHA2-512**. **SHA** is generally considered stronger than **MD5**, but it is also slower. |

**Table 49** IPSec VPN: Add

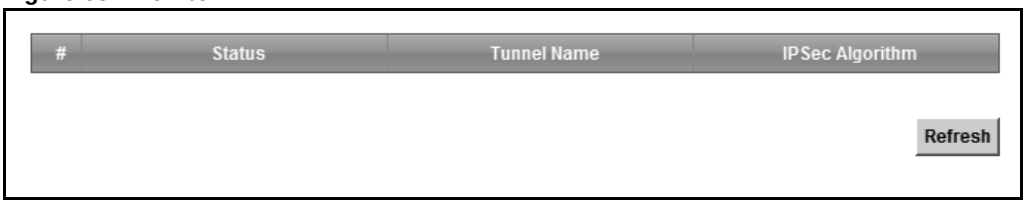
| LABEL | DESCRIPTION |
|---|---|
| SA Life Time | Define the length of time before an IPSec SA automatically renegotiates in this field.<br><br>A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected. |
| Perfect Forward Secrecy (PFS) | Select whether or not you want to enable Perfect Forward Secrecy (PFS)<br><br>PFS changes the root key that is used to generate encryption keys for each IPSec SA. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group. Choices are:<br><br>**Diffie-Hellman Group2** - use a 1024-bit random number<br><br>**Diffie-Hellman Group5** - use a 1536-bit random number<br><br>**Diffie-Hellman Group14** - use a 2048-bit random number |
| DPD Active | Select the Dead Peer Detection (DPD) Active check box if you want the LTE Device to make sure the remote IPSec router is there before it transmits data through the IKE SA. The remote IPSec router must support DPD. If the remote IPSec router does not respond, the LTE Device shuts down the IKE SA.<br><br>If the remote IPSec router does not support DPD, see if you can use the VPN connection connectivity check. |

## 14.2.3 The Monitor Screen

The following figure helps explain the main fields in the web configurator.

Click **Security > VPN > Monitor** to open this screen as shown next.

**Figure 68** Monitor




This screen contains the following fields:

**Table 50** Monitor

| LABEL | DESCRIPTION |
|---|---|
| # | This is the VPN policy index number. |
| Status | This displays if the VPN policy is connected. |
| Tunnel Name | Enter the name of the VPN connection. |
| IPSec Algorithm | This displays the encryption algorithm being used for the VPN connection. |
| Refresh | Click this button to refresh the information on the screen. |

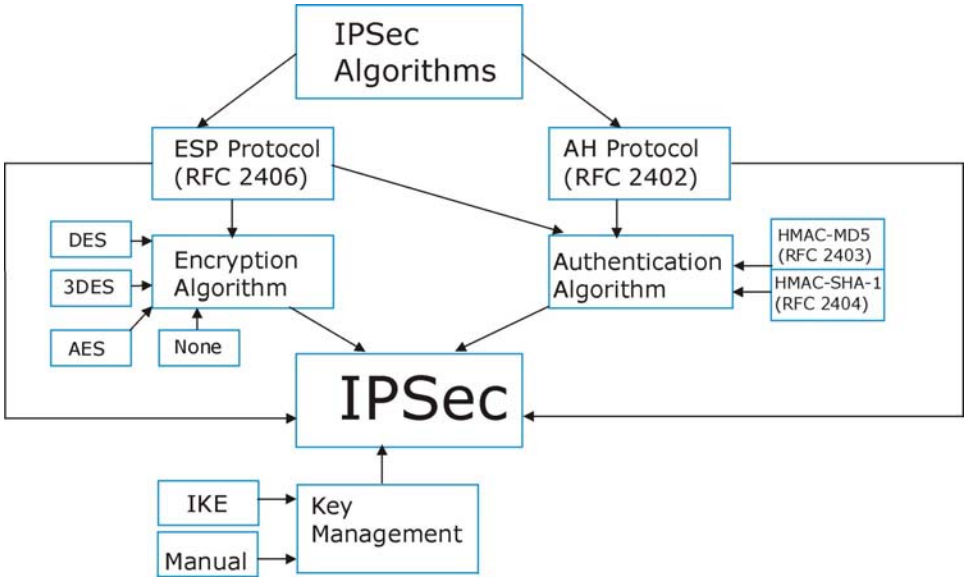
# 14.3 Technical Reference

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

## 14.3.1 IPSec Architecture

The overall IPSec architecture is shown as follows.

**Figure 69** IPSec Architecture




### IPSec Algorithms

The **ESP** (Encapsulating Security Payload) Protocol (RFC 2406) and **AH** (Authentication Header) protocol (RFC 2402) describe the packet formats and the default standards for packet structure (including implementation algorithms).

The Encryption Algorithm describes the use of encryption techniques such as DES (Data Encryption Standard) and Triple DES algorithms.

The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404, provide an authentication mechanism for the **AH** and **ESP** protocols.

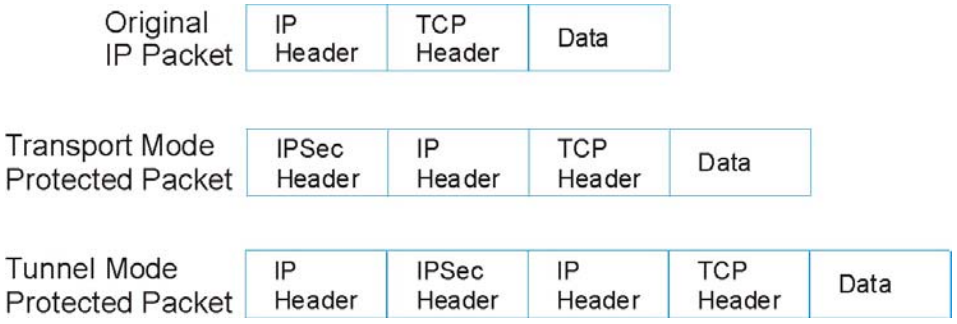
### Key Management

Key management allows you to determine whether to use IKE (ISAKMP) or manual key configuration in order to set up a VPN.

## 14.3.2 Encapsulation

The two modes of operation for IPSec VPNs are **Transport** mode and **Tunnel** mode. At the time of writing, the LTE Device supports **Tunnel** mode only.

**Figure 70** Transport and Tunnel Mode IPSec Encapsulation




### Transport Mode

**Transport** mode is used to protect upper layer protocols and only affects the data in the IP packet. In **Transport** mode, the IP packet contains the security protocol (**AH** or **ESP**) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP).

With **ESP,** protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data.

With the use of **AH** as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process.

### Tunnel Mode

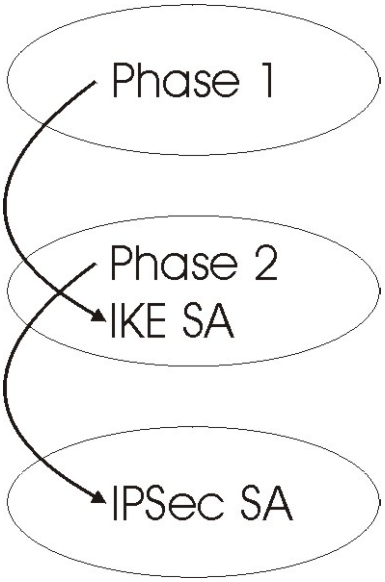
**Tunnel** mode encapsulates the entire IP packet to transmit it securely. A **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel** mode is required for gateway to gateway and host to gateway communications. **Tunnel** mode communications have two sets of IP headers:

- **Outside header**: The outside IP header contains the destination IP address of the VPN gateway.
- **Inside header**: The inside IP header contains the destination IP address of the final system behind the VPN gateway. The security protocol appears after the outer IP header and before the inside IP header.

### 14.3.3 IKE Phases

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.

**Figure 71** Two Phases to Set Up the IPSec SA




In phase 1 you must:

- Choose a negotiation mode.
- Authenticate the connection by entering a pre-shared key.
- Choose an encryption algorithm.
- Choose an authentication algorithm.
- Choose a Diffie-Hellman public-key cryptography key group.
- Set the IKE SA lifetime. This field allows you to determine how long an IKE SA should stay up before it times out. An IKE SA times out when the IKE SA lifetime period expires. If an IKE SA times out when an IPSec SA is already established, the IPSec SA stays connected.

In phase 2 you must:

- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose a Diffie-Hellman public-key cryptography key group.
- Set the IPSec SA lifetime. This field allows you to determine how long the IPSec SA should stay up before it times out. The LTE Device automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. If an IPSec SA times out, then the IPSec router must renegotiate the SA the next time someone attempts to send traffic.

### 14.3.4 Negotiation Mode

The phase 1 **Negotiation Mode** you select determines how the Security Association (SA) will be established for each connection through IKE negotiations.

- **Main Mode** ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). It uses 6 messages in three round trips: SA negotiation, Diffie-Hellman exchange and an exchange of nonces (a nonce is a random number). This mode features identity protection (your identity is not revealed in the negotiation).
- **Aggressive Mode** is quicker than **Main Mode** because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that faster speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situations where the address of the initiator is not know by the responder and both parties want to use pre-shared key authentication.

## 14.3.5 IPSec and NAT

Read this section if you are running IPSec on a host computer behind the LTE Device.

NAT is incompatible with the **AH** protocol in both **Transport** and **Tunnel** mode. An IPSec VPN using the **AH** protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet. When using **AH** protocol, packet contents (the data payload) are not encrypted.

A NAT device in between the IPSec endpoints will rewrite either the source or destination address with one of its own choosing. The VPN device at the receiving end will verify the integrity of the incoming packet by computing its own hash value, and complain that the hash value appended to the received packet doesn't match. The VPN device at the receiving end doesn't know about the NAT in the middle, so it assumes that the data has been maliciously altered.

IPSec using **ESP** in **Tunnel** mode encapsulates the entire original packet (including headers) in a new IP packet. The new IP packet's source address is the outbound address of the sending VPN gateway, and its destination address is the inbound address of the VPN device at the receiving end. When using **ESP** protocol with authentication, the packet contents (in this case, the entire original packet) are encrypted. The encrypted contents, but not the new headers, are signed with a hash value appended to the packet.

**Tunnel** mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device.

**Transport** mode **ESP** with authentication is not compatible with NAT.

**Table 51** VPN and NAT

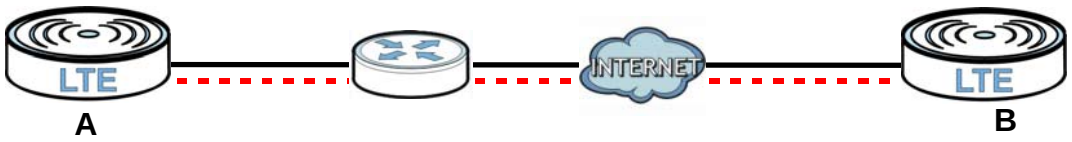
| SECURITY PROTOCOL | MODE | NAT |
|---|---|---|
| AH | Transport | N |
| AH | Tunnel | N |
| ESP | Transport | N |
| ESP | Tunnel | Y |

## 14.3.6 VPN, NAT, and NAT Traversal

NAT is incompatible with the AH protocol in both transport and tunnel mode. An IPSec VPN using the AH protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet, but a NAT device between the IPSec endpoints rewrites the source or destination address. As a result, the VPN device at the receiving end finds a mismatch between the hash value and the data and assumes that the data has been maliciously altered.

NAT is not normally compatible with ESP in transport mode either, but the LTE Device's **NAT Traversal** feature provides a way to handle this. NAT traversal allows you to set up an IKE SA when there are NAT routers between the two IPSec routers.

**Figure 72** NAT Router Between IPSec Routers




Normally you cannot set up an IKE SA with a NAT router between the two IPSec routers because the NAT router changes the header of the IPSec packet. NAT traversal solves the problem by adding a UDP port 500 header to the IPSec packet. The NAT router forwards the IPSec packet with the UDP port 500 header unchanged. In the above figure, when IPSec router **A** tries to establish an IKE SA, IPSec router **B** checks the UDP port 500 header, and IPSec routers **A** and **B** build the IKE SA.

For NAT traversal to work, you must:

- Use ESP security protocol (in either transport or tunnel mode).
- Use IKE keying mode.
- Enable NAT traversal on both IPSec endpoints.
- Set the NAT router to forward UDP port 500 to IPSec router **A**.

Finally, NAT is compatible with ESP in tunnel mode because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device. The compatibility of AH and ESP with NAT in tunnel and transport modes is summarized in the following table.

**Table 52** VPN and NAT

| SECURITY PROTOCOL | MODE | NAT |
|---|---|---|
| AH | Transport | N |
| AH | Tunnel | N |
| ESP | Transport | Y* |
| ESP | Tunnel | Y |

Y* - This is supported in the LTE Device if you enable NAT traversal.

## 14.3.7 ID Type and Content

With aggressive negotiation mode (see Section 14.3.4 on page 122), the LTE Device identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the LTE Device to distinguish between multiple rules for SAs that connect from remote IPSec routers that have dynamic WAN IP addresses.

Regardless of the ID type and content configuration, the LTE Device does not allow you to save multiple active rules with overlapping local and remote IP addresses.

With main mode (see Section 14.3.4 on page 122), the ID type and content are encrypted to provide identity protection. In this case the LTE Device can distinguish between different incoming SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. The LTE Device

can distinguish different incoming SAs and you can select between different encryption algorithms, authentication algorithms and key groups when you configure a VPN rule. The ID type and content act as an extra level of identification for incoming SAs.

The type of ID can be a domain name, an IP address or an e-mail address. The content is the IP address, domain name, or e-mail address.

**Table 53** Local ID Type and Content Fields

| LOCAL ID TYPE= | CONTENT= |
|---|---|
| IP | Type the IP address of your computer. |
| DNS | Type a domain name (up to 31 characters) by which to identify this LTE Device. |
| E-mail | Type an e-mail address (up to 31 characters) by which to identify this LTE Device. |
| | The domain name or e-mail address that you use in the **Local ID Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address. |

#### 14.3.7.1 ID Type and Content Examples

Two IPSec routers must have matching ID type and content configuration in order to set up a VPN tunnel.

The two LTE Devices in this example can complete negotiation and establish a VPN tunnel.

**Table 54** Matching ID Type and Content Configuration Example

| LTE Device A | LTE Device B |
|---|---|
| Local ID type: E-mail | Local ID type: IP |
| Local ID content: tom@yourcompany.com | Local ID content: 1.1.1.2 |
| Remote ID type: IP | Remote ID type: E-mail |
| Remote ID content: 1.1.1.2 | Remote ID content: tom@yourcompany.com |

The two LTE Devices in this example cannot complete their negotiation because LTE Device B's **Local ID type** is **IP**, but LTE Device A's **Remote ID type** is set to **E-mail**. An "ID mismatched" message displays in the IPSEC LOG.

**Table 55** Mismatching ID Type and Content Configuration Example

| LTE DEVICE A | LTE DEVICE B |
|---|---|
| Local ID type: IP | Local ID type: IP |
| Local ID content: 1.1.1.10 | Local ID content: 1.1.1.2 |
| Remote ID type: E-mail | Remote ID type: IP |
| Remote ID content: aa@yahoo.com | Remote ID content: 1.1.1.0 |

### 14.3.8 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see Section 14.3.3 on page 122 for more on IKE phases). It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.

### 14.3.9 Diffie-Hellman (DH) Key Groups

Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys.

# 15 Logs

## 15.1 Overview

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

### 15.1.1 What You Can Do in this Chapter

- Use the **System Log** screen to see the system logs for the categories that you select (Section 15.2 on page 128).

### 15.1.2 What You Need To Know

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

#### Alerts and Logs

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

#### Syslog Overview

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

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

**Table 56** Syslog Severity Levels

| CODE | SEVERITY |
|---|---|
| 0 | Emergency (EMERG): The system is unusable. |
| 1 | Alert (ALERT): Action must be taken immediately. |
| 2 | Critical (CRIT): The system condition is critical. |
| 3 | Error (ERROR): There is an error condition on the system. |
| 4 | Warning (WARNING): There is a warning condition on the system. |
| 5 | Notice (NOTICE): There is a normal but significant condition on the system. |

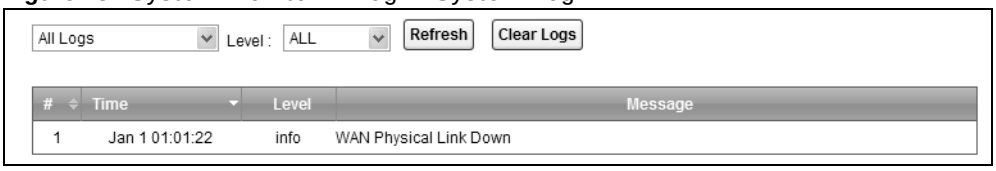
**Table 56** Syslog Severity Levels (continued)

| CODE | SEVERITY |
|---|---|
| 6 | Informational (INFO): The syslog contains an informational message. |
| 7 | Debug (DEBUG): The message is intended for debug-level purposes. |

# 15.2 The System Log Screen

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

**Figure 73** System Monitor > Log > System Log




The following table describes the fields in this screen.

**Table 57** System Monitor > Log > System Log

| LABEL | DESCRIPTION |
|---|---|
| | Select the type of the logs that you want to search in the first drop-down list box. |
| Level | Select a severity level from this drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the LTE Device searches through all logs of that severity or higher. See Table 56 on page 127 for more information about severity levels. |
| Refresh | Click this to renew the log screen. |
| Clear Logs | Click this to delete all the logs. |
| # | This field is a sequential value and is not associated with a specific entry. |
| Time | This field displays the date and time the log was recorded. |
| Level | This field displays the severity level of the logs that the device is to send to this syslog server. |
| Message | This field states the reason for the log. |

# 16

# Traffic Status

## 16.1 Overview

Use the **Traffic Status** screens to look at network traffic status and statistics of the WAN, LAN interfaces and NAT.

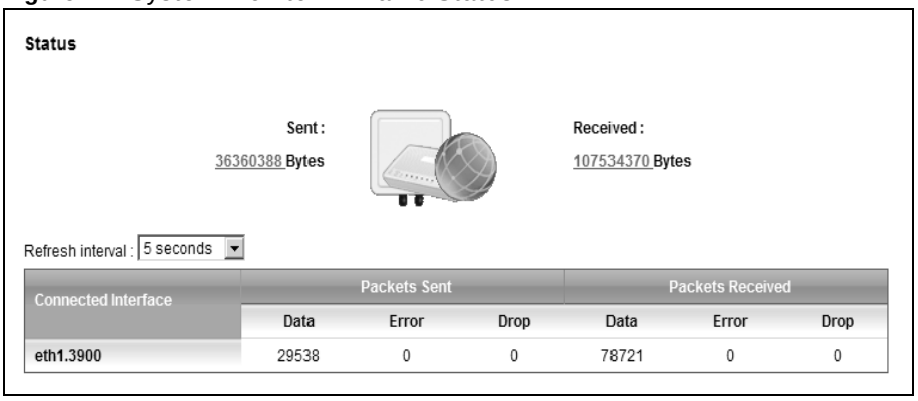
### 16.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics (Section 16.2 on page 129).
- Use the **LAN** screen to view the LAN traffic statistics (Section 16.3 on page 130).
- Use the **NAT** screen to view the NAT status of the LTE Device's client(s) (Section 16.4 on page 131).

## 16.2 The WAN Status Screen

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

**Figure 74** System Monitor > Traffic Status > WAN




The following table describes the fields in this screen.

**Table 58** System Monitor > Traffic Status > WAN

| LABEL | DESCRIPTION |
|---|---|
| Status | This shows the number of bytes received and sent through the WAN interface of the LTE Device. |
| Refresh Interval | Select how often you want the LTE Device to update this screen from the drop-down list box. |

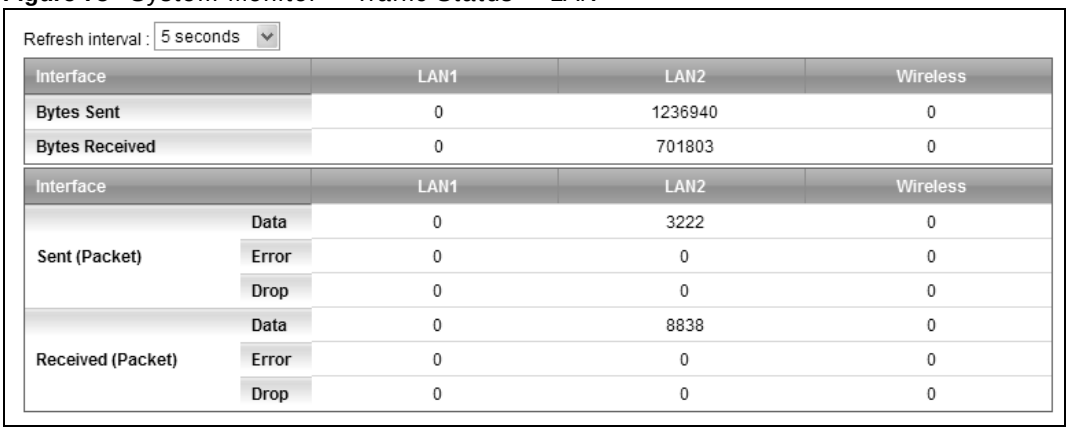
**Table 58** System Monitor > Traffic Status > WAN (continued)

| LABEL | DESCRIPTION |
|---|---|
| Connected Interface | This shows the name of the WAN interface that is currently connected. |
| Packets Sent | |
| Data | This indicates the number of transmitted packets on this interface. |
| Error | This indicates the number of frames with errors transmitted on this interface. |
| Drop | This indicates the number of outgoing packets dropped on this interface. |
| Packets Received | |
| Data | This indicates the number of received packets on this interface. |
| Error | This indicates the number of frames with errors received on this interface. |
| Drop | This indicates the number of received packets dropped on this interface. |

# 16.3 The LAN Status Screen

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

**Figure 75** System Monitor > Traffic Status > LAN




The following table describes the fields in this screen.

**Table 59** System Monitor > Traffic Status > LAN

| LABEL | DESCRIPTION |
|---|---|
| Refresh Interval | Select how often you want the LTE Device to update this screen from the drop-down list box. |
| Interface | This shows the LAN interface. |
| Bytes Sent | This indicates the number of bytes transmitted on this interface. |
| Bytes Received | This indicates the number of bytes received on this interface. |
| Interface | This shows the LAN interface. |
| Sent (Packet) | |
| Data | This indicates the number of transmitted packets on this interface. |
| Error | This indicates the number of frames with errors transmitted on this interface. |
| Drop | This indicates the number of outgoing packets dropped on this interface. |

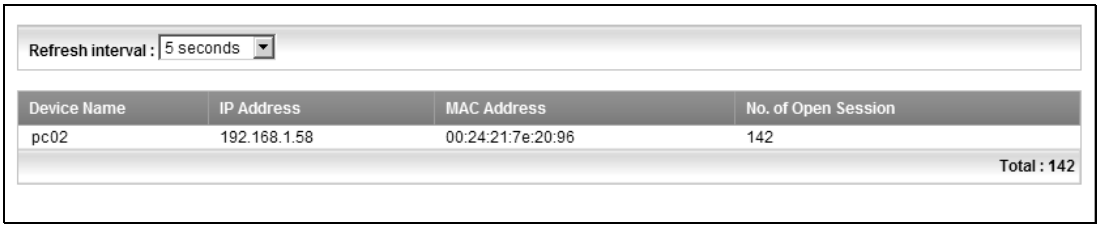
**Table 59** System Monitor > Traffic Status > LAN (continued)

| LABEL | DESCRIPTION |
|---|---|
| Received (Packet) | |
| Data | This indicates the number of received packets on this interface. |
| Error | This indicates the number of frames with errors received on this interface. |
| Drop | This indicates the number of received packets dropped on this interface. |

# 16.4 The NAT Status Screen

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

**Figure 76** System Monitor > Traffic Status > NAT




The following table describes the fields in this screen.

**Table 60** System Monitor > Traffic Status > NAT

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

# 17

# User Account

## 17.1 Overview

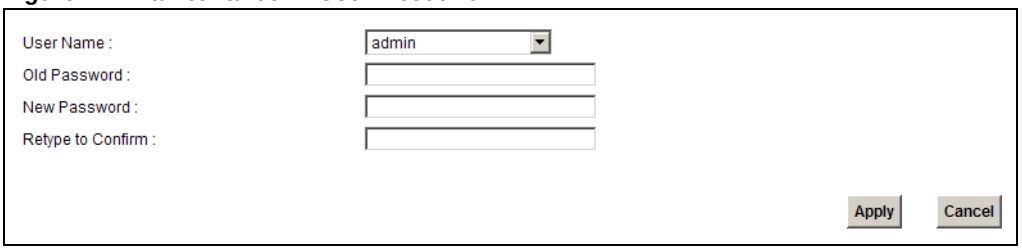
You can configure system password for different user accounts in the **User Account** screen.

## 17.2 The User Account Screen

Use the **User Account** screen to configure system password.

Click **Maintenance > User Account** to open the following screen.

**Figure 77** Maintenance > User Account




The following table describes the labels in this screen.

**Table 61** Maintenance > User Account

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

# 18

# Remote MGMT

## 18.1 Overview

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

- LAN
- WAN only

Note: The LTE Device is managed using the web configurator.

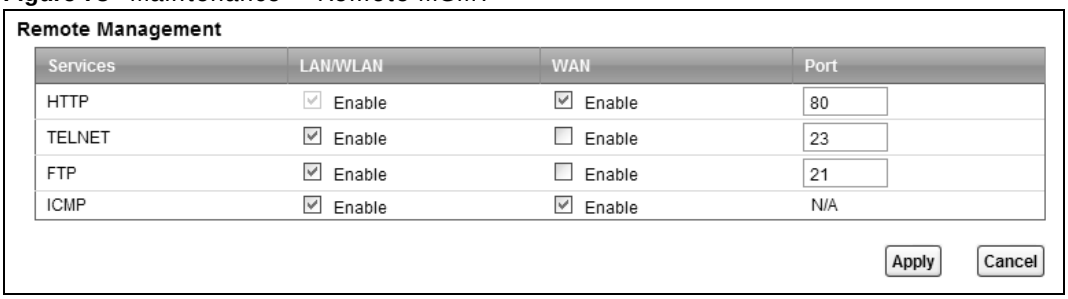
### 18.1.1 What You Need to Know

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

## 18.2 The Remote MGMT Screen

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

**Figure 78** Maintenance > Remote MGMT




The following table describes the fields in this screen.

**Table 62** Maintenance > Remote MGMT

| LABEL | DESCRIPTION |
|---|---|
| Services | This is the service you may use to access the LTE Device. |
| LAN/WLAN | Select the **Enable** check box for the corresponding services that you want to allow access to the LTE Device from the LAN or WLAN. |
| WAN | Select the **Enable** check box for the corresponding services that you want to allow access to the LTE Device from the WAN. |

**Table 62** Maintenance > Remote MGMT (continued)

| LABEL | DESCRIPTION |
|---|---|
| Port | You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

# 19

# System

## 19.1 Overview

You can configure system settings, including the host name, domain name and the inactivity time-out interval in the **System** screen.

### 19.1.1 What You Need to Know

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

#### Domain Name

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

## 19.2 The System Screen

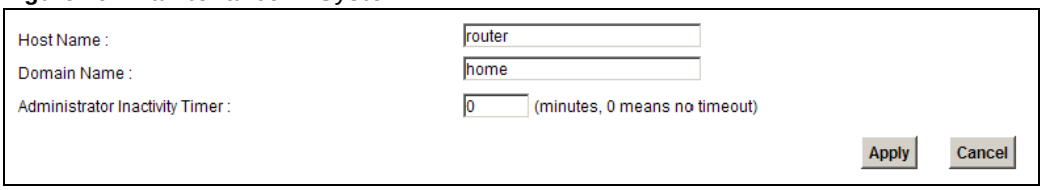
Use the **System** screen to configure the system’s host name, domain name, and inactivity time-out interval.

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

In Windows XP, click **start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the LTE Device **System Name**.

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

**Figure 79** Maintenance > System



The following table describes the labels in this screen.

**Table 63** Maintenance > System

| LABEL | DESCRIPTION |
|---|---|
| Host Name | Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted. |
| Domain Name | Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP.<br>The domain name entered by you is given priority over the ISP assigned domain name. |
| Administrator Inactivity Timer | Type how many minutes a management session (either via the web configurator) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended). |
| Apply | Click this to save your changes back to the LTE Device. |
| Cancel | Click this to begin configuring this screen afresh. |

# 20

# Time Setting

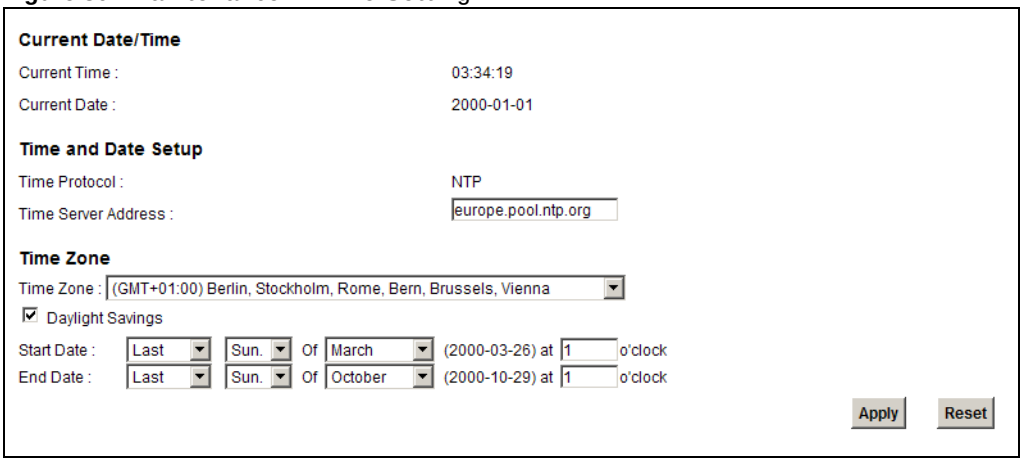
## 20.1 Overview

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

## 20.2 The Time Setting Screen

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

**Figure 80** Maintenance > Time Setting




The following table describes the fields in this screen.

**Table 64** Maintenance > System > Time Setting

| LABEL | DESCRIPTION |
|---|---|
| Current Date/Time | |
| Current Time | This field displays the time of your LTE Device. |
| Current Date | This field displays the date of your LTE Device. |
| Time and Date Setup | |
| Time Protocol | This shows the time service protocol that your time server sends when you turn on the LTE Device. |
| Time Server Address | Enter the IP address or URL (up to 31 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information. |
| Time Zone | Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT). |

**Table 64** Maintenance > System > Time Setting (continued)

| LABEL | DESCRIPTION |
|---|---|
| Daylight Savings | Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.Select this option if you use Daylight Saving Time. |
| Start Date | Configure the day and time when Daylight Saving Time starts if you selected **Daylight Savings**. The **o'clock** 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 type **2** in the **o'clock** 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 type in the **o'clock** field depends on your time zone. In Germany for instance, you would type **2** because Germany's time zone is one hour ahead of GMT or UTC (GMT+1). |
| End Date | Configure the day and time when Daylight Saving Time ends if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples:<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 type **2** in the **o'clock** 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 type in the **o'clock** field depends on your time zone. In Germany for instance, you would type **2** because Germany's time zone is one hour ahead of GMT or UTC (GMT+1). |
| Apply | Click **Apply** to save your changes. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 21

# Log Setting

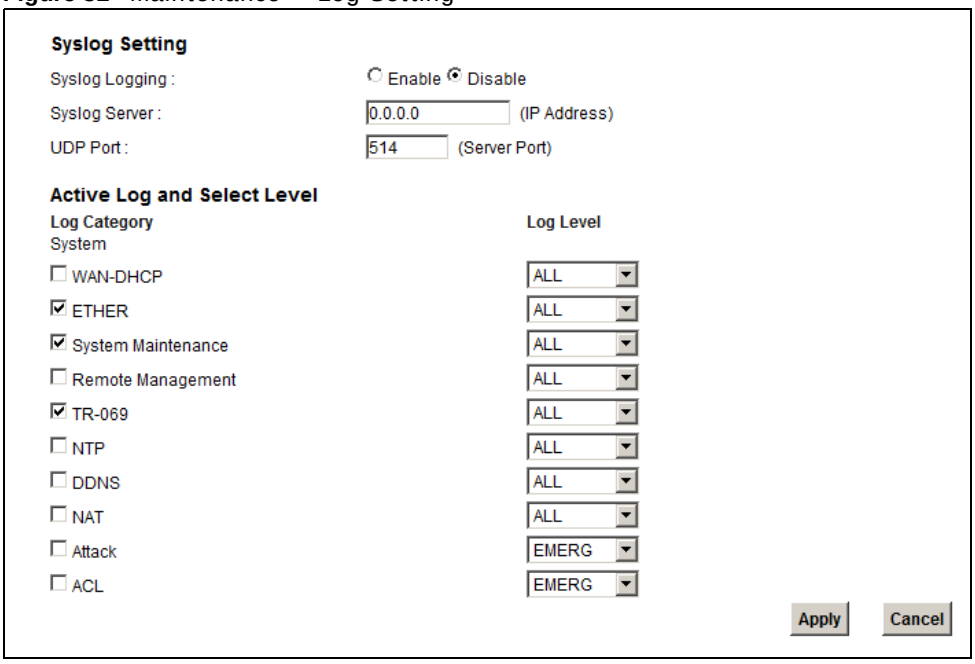
## 21.1 Overview

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

## 21.2 The Log Setting Screen

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

**Figure 81** Maintenance > Log Setting




The following table describes the fields in this screen.

**Table 65** Maintenance > Log Setting

| LABEL | DESCRIPTION |
|---|---|
| Syslog Setting | |
| Syslog Logging | The LTE Device sends a log to an external syslog server. Select the **Enable** check box to enable syslog logging. |
| Syslog Server | Enter the server name or IP address of the syslog server that will log the selected categories of logs. |

**Table 65** Maintenance > Log Setting (continued)

| LABEL | DESCRIPTION |
|---|---|
| UDP Port | Enter the port number used by the syslog server. |
| Active Log and Select Level | |
| Log Category | Select the categories of logs that you want to record. |
| Log Level | Select the severity level of logs that you want to record. If you want to record all logs, select **ALL**. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

# 22

# Firmware Upgrade

## 22.1 Overview

This chapter explains how to upload new firmware to your LTE Device. You can download new firmware releases from your nearest ZyXEL FTP site (or www.zyxel.com) to use to upgrade your device's performance.

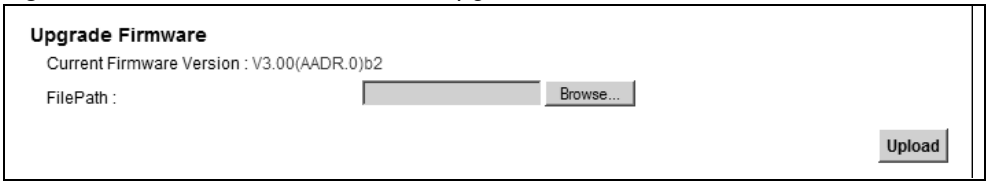
**Only use firmware for your device's specific model. Refer to the label on the bottom of your LTE Device.**

## 22.2 The Firmware Upgrade Screen

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

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

**Figure 82** Maintenance > Firmware Upgrade



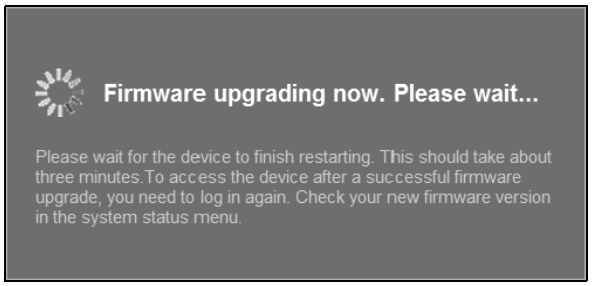

The following table describes the labels in this screen.

**Table 66** Maintenance > Firmware Upgrade

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

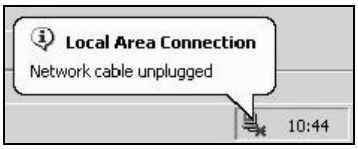
After you see the firmware updating screen, wait a few minutes before logging into the LTE Device again.

**Figure 83** Firmware Uploading




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

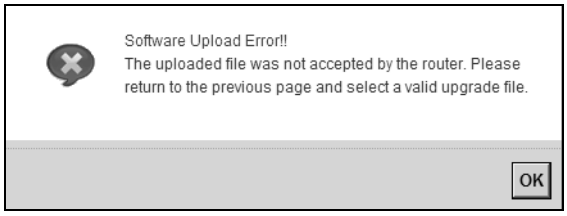
**Figure 84** Network Temporarily Disconnected




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

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

**Figure 85** Error Message



# 23

# Backup/Restore

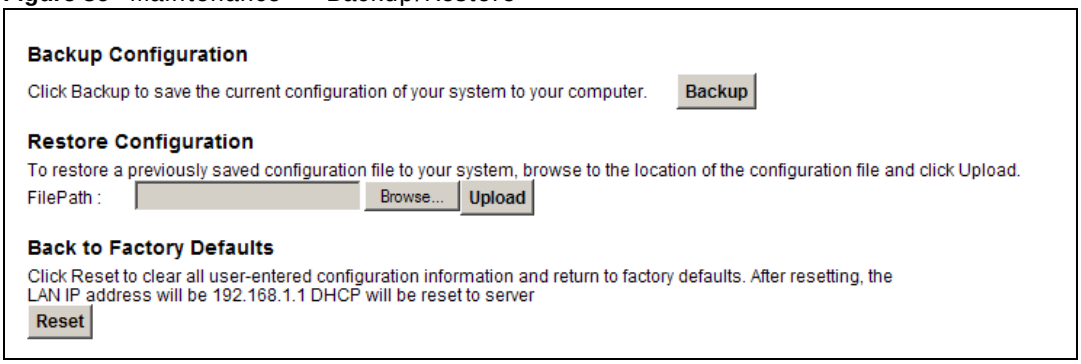
## 23.1 Overview

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

## 23.2 The Backup/Restore Screen

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

**Figure 86** Maintenance > Backup/Restore




### Backup Configuration

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

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

## Restore Configuration

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

**Table 67** Restore Configuration

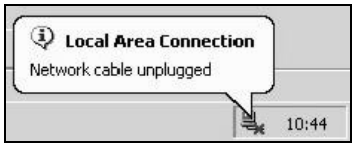
| LABEL | DESCRIPTION |
|---|---|
| File Path | Type in the location of the file you want to upload in this field or click **Browse ...** to find it. |
| Browse... | Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them. |
| Upload | Click this to begin the upload process. |
| Reset | Click this to reset your device settings back to the factory default. |

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

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

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

**Figure 87** Network Temporarily Disconnected




If you restore the default configuration, you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1). See Appendix B on page 167 for details on how to set up your computer's IP address.

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

### Reset to Factory Defaults

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

**Figure 88** Reset Warning Message

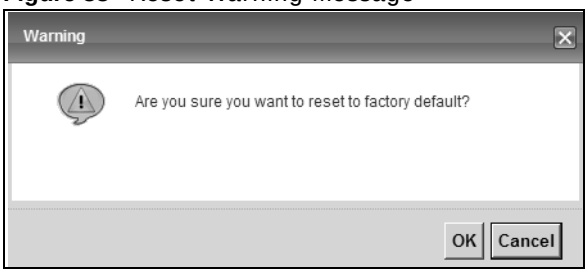
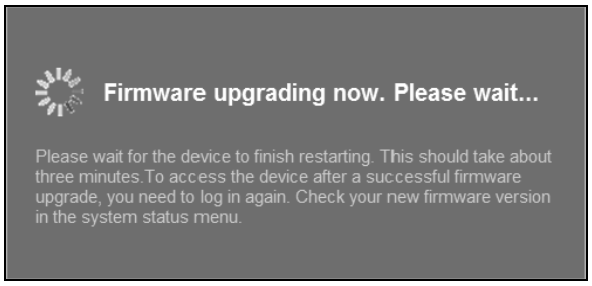



**Figure 89** Reset In Process Message




You can also press the **RESET** button on the back panel to reset the factory defaults of your LTE Device. Refer to Section 1.7 on page 16 for more information on the **RESET** button.

## 23.3 The Reboot Screen

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

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

# 24

# Diagnostic

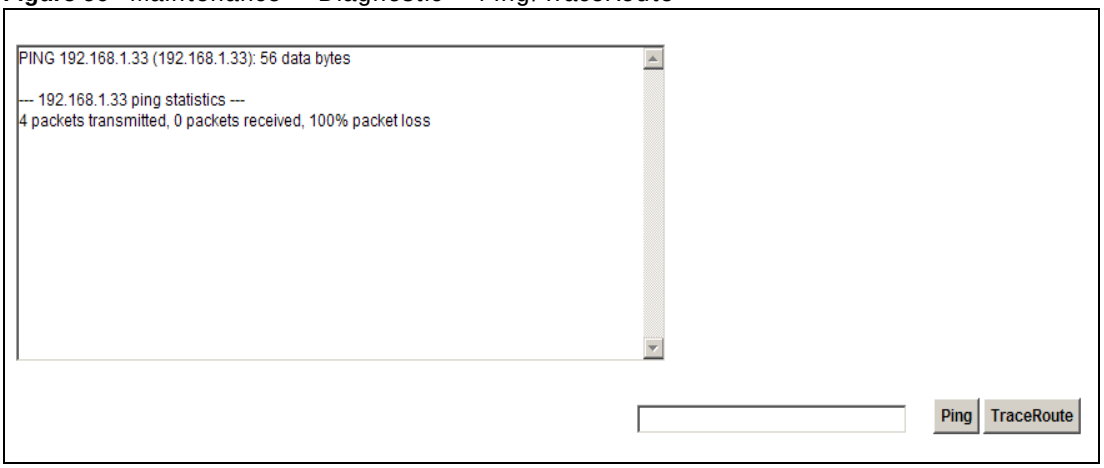
## 24.1 Overview

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

## 24.2 The Ping/TraceRoute Screen

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

**Figure 90** Maintenance > Diagnostic > Ping/TraceRoute




The following table describes the fields in this screen.

**Table 68** Maintenance > Diagnostic > Ping/TraceRoute

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

# 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
- LTE Device Access and Login
- Internet Access
- Wireless Internet Access
- UPnP

## 25.2 Power, Hardware Connections, and LEDs

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

1. Make sure the LTE Device is turned on.
2. Make sure you are using the power adaptor or cord included with the LTE Device.
3. Make sure the power adaptor or cord is connected to the LTE Device and plugged in to an appropriate power source. Make sure the power source is turned on.
4. Turn the LTE Device off and on.
5. 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 1.6 on page 15.
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. Turn the LTE Device off and on.

5 If the problem continues, contact the vendor.

## 25.3 LTE Device Access and Login

### I forgot the IP address for the LTE Device.

1 The default IP address is 192.168.1.1.

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

3 If this does not work, you have to reset the device to its factory defaults. See Section 1.7 on page 16.

### I forgot the password.

1 The default admin password is **1234** and the default user password is **1234**.

2 If you can't remember the password, you have to reset the device to its factory defaults. See Section 1.7 on page 16.

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

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.1.1.
- If you changed the IP address, use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the LTE Device.

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 C on page 197.

4 Reset the device to its factory defaults, and try to access the LTE Device with the default IP address. See Section 1.7 on page 16.

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

**Advanced Suggestions**

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

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

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

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

3 Turn the LTE Device off and on.

4 If this does not work, you have to reset the device to its factory defaults. See Section 25.2 on page 151.

## 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 and Section 1.6 on page 15.

2 Make sure you entered your service provider's LTE APN information correctly.

3 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.

4 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the LTE Device), 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 1.6 on page 15.

2 Turn the LTE Device off and on.

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 1.6 on page 15. If the LTE Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

2 Turn the LTE Device off and on.

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

**Advanced Suggestions**

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

## 25.5 Wireless Internet Access

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.

### What wireless security modes does my LTE Device support?

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

The available security modes in your device are as follows:

- **WPA2-PSK**: (recommended) This uses a pre-shared key with the WPA2 standard.
- **WPA-PSK**: This has the device use either WPA-PSK or WPA2-PSK depending on which security mode the wireless client uses.
- **WPA2**: WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA. It requires the use of a RADIUS server and is mostly used in business networks.
- **WPA**: Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. It requires the use of a RADIUS server and is mostly used in business networks.
- **WEP**: Wired Equivalent Privacy (WEP) encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private.

## 25.6 UPnP

### When using UPnP and the LTE Device reboots, my computer cannot detect UPnP and refresh **My Network Places > Local Network**.

1. Disconnect the Ethernet cable from the LTE Device's LAN port or from your computer.
2. Re-connect the Ethernet cable.

### The **Local Area Connection** icon for UPnP disappears in the screen.

Restart your computer.

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

1. Wait more than three minutes.
2. Restart the applications.

A

# IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (such as computers, servers, routers, and printers) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

## Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

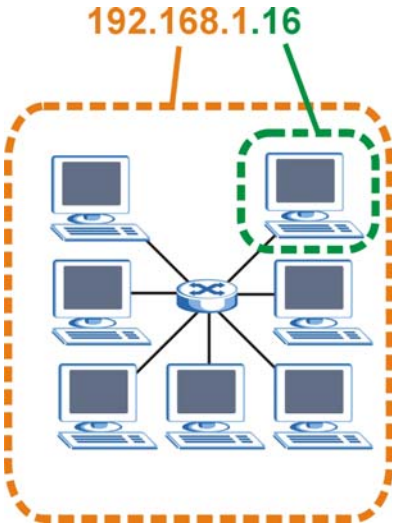
## Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

**Figure 91** Network Number and Host ID




How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

## Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term “subnet” is short for “sub-network”.

A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

**Table 69** IP Address Network Number and Host ID Example

| | 1ST OCTET: (192) | 2ND OCTET: (168) | 3RD OCTET: (1) | 4TH OCTET (2) |
|---|---|---|---|---|
| IP Address (Binary) | 11000000 | 10101000 | 00000001 | 00000010 |
| Subnet Mask (Binary) | **11111111** | **11111111** | **11111111** | 00000000 |
| Network Number | **11000000** | **10101000** | **00000001** | |
| Host ID | | | | 00000010 |

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a “1” value). For example, an “8-bit mask” means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

**Table 70** Subnet Masks

| | BINARY | | | | DECIMAL |
|---|---|---|---|---|---|
| | 1ST OCTET | 2ND OCTET | 3RD OCTET | 4TH OCTET | |
| 8-bit mask | 11111111 | 00000000 | 00000000 | 00000000 | 255.0.0.0 |
| 16-bit mask | 11111111 | 11111111 | 00000000 | 00000000 | 255.255.0.0 |
| 24-bit mask | 11111111 | 11111111 | 11111111 | 00000000 | 255.255.255.0 |
| 29-bit mask | 11111111 | 11111111 | 11111111 | 11111000 | 255.255.255.248 |

## Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

**Table 71** Maximum Host Numbers

| SUBNET MASK | | HOST ID SIZE | | MAXIMUM NUMBER OF HOSTS |
|---|---|---|---|---|
| 8 bits | 255.0.0.0 | 24 bits | $2^{24} – 2$ | 16777214 |
| 16 bits | 255.255.0.0 | 16 bits | $2^{16} – 2$ | 65534 |
| 24 bits | 255.255.255.0 | 8 bits | $2^{8} – 2$ | 254 |
| 29 bits | 255.255.255.248 | 3 bits | $2^{3} – 2$ | 6 |

## Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a “/” followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

**Table 72** Alternative Subnet Mask Notation

| SUBNET MASK | ALTERNATIVE NOTATION | LAST OCTET (BINARY) | LAST OCTET (DECIMAL) |
|---|---|---|---|
| 255.255.255.0 | /24 | 0000 0000 | 0 |
| 255.255.255.128 | /25 | 1000 0000 | 128 |
| 255.255.255.192 | /26 | 1100 0000 | 192 |
| 255.255.255.224 | /27 | 1110 0000 | 224 |
| 255.255.255.240 | /28 | 1111 0000 | 240 |
| 255.255.255.248 | /29 | 1111 1000 | 248 |
| 255.255.255.252 | /30 | 1111 1100 | 252 |

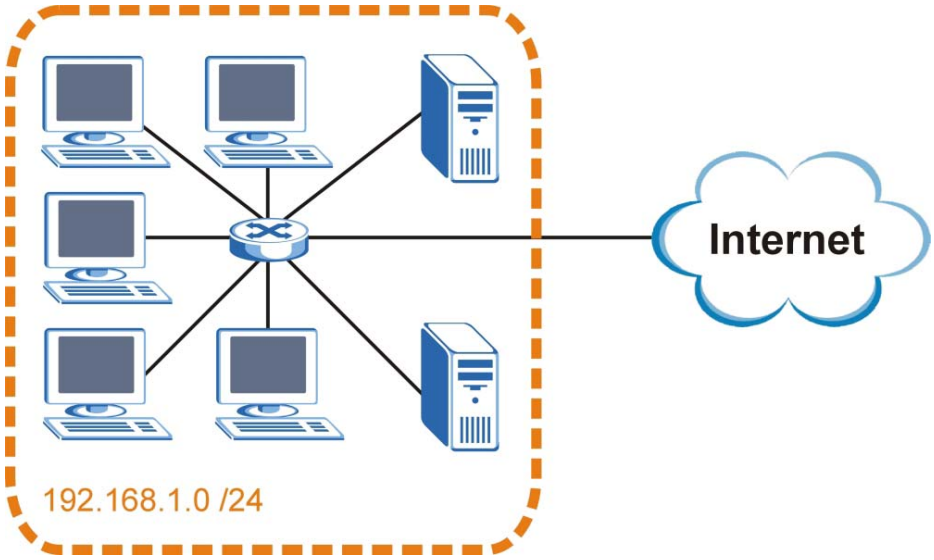
## Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8 - 2$ or 254 possible hosts.

The following figure shows the company network before subnetting.

**Figure 92** Subnetting Example: Before Subnetting

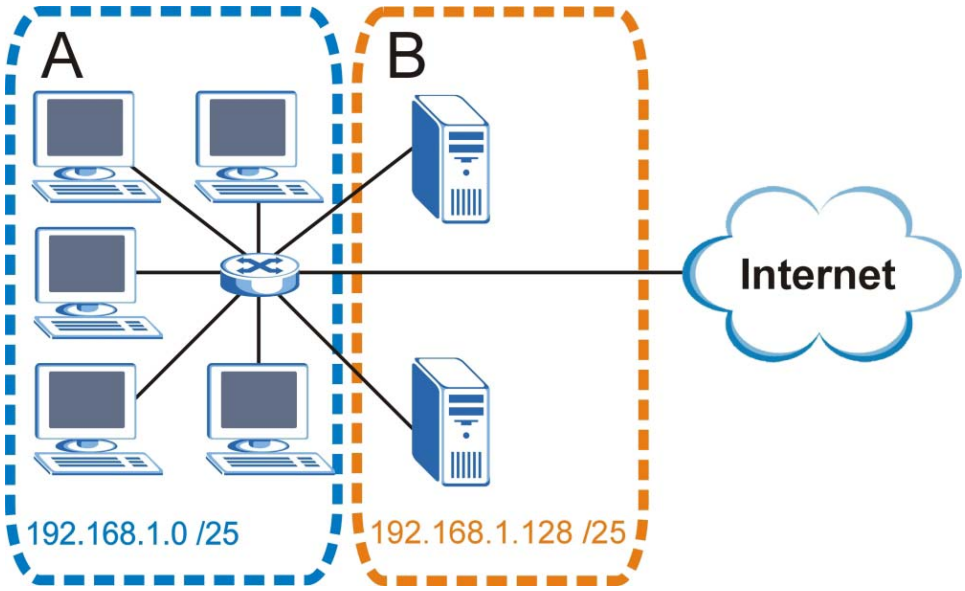



You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

**Figure 93** Subnetting Example: After Subnetting




In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7$ – 2 or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

## Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving $2^6$ - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

**Table 73** Subnet 1

| IP/SUBNET MASK | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| IP Address (Decimal) | 192.168.1. | 0 |
| IP Address (Binary) | 11000000.10101000.00000001. | **00**000000 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | **11**000000 |

**Table 73** Subnet 1 (continued)

| IP/SUBNET MASK | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| Subnet Address: 192.168.1.0 | Lowest Host ID: 192.168.1.1 | |
| Broadcast Address: 192.168.1.63 | Highest Host ID: 192.168.1.62 | |

**Table 74** Subnet 2

| IP/SUBNET MASK | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| IP Address | 192.168.1. | 64 |
| IP Address (Binary) | 11000000.10101000.00000001. | **01**000000 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | **11**000000 |
| Subnet Address: 192.168.1.64 | Lowest Host ID: 192.168.1.65 | |
| Broadcast Address: 192.168.1.127 | Highest Host ID: 192.168.1.126 | |

**Table 75** Subnet 3

| IP/SUBNET MASK | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| IP Address | 192.168.1. | 128 |
| IP Address (Binary) | 11000000.10101000.00000001. | **10**000000 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | **11**000000 |
| Subnet Address: 192.168.1.128 | Lowest Host ID: 192.168.1.129 | |
| Broadcast Address: 192.168.1.191 | Highest Host ID: 192.168.1.190 | |

**Table 76** Subnet 4

| IP/SUBNET MASK | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| IP Address | 192.168.1. | 192 |
| IP Address (Binary) | 11000000.10101000.00000001. | **11**000000 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | **11**000000 |
| Subnet Address: 192.168.1.192 | Lowest Host ID: 192.168.1.193 | |
| Broadcast Address: 192.168.1.255 | Highest Host ID: 192.168.1.254 | |

## Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

**Table 77** Eight Subnets

| SUBNET | SUBNET ADDRESS | FIRST ADDRESS | LAST ADDRESS | BROADCAST ADDRESS |
|---|---|---|---|---|
| 1 | 0 | 1 | 30 | 31 |
| 2 | 32 | 33 | 62 | 63 |
| 3 | 64 | 65 | 94 | 95 |
| 4 | 96 | 97 | 126 | 127 |
| 5 | 128 | 129 | 158 | 159 |
| 6 | 160 | 161 | 190 | 191 |
| 7 | 192 | 193 | 222 | 223 |
| 8 | 224 | 225 | 254 | 255 |

## Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

**Table 78** 24-bit Network Number Subnet Planning

| NO. "BORROWED" HOST BITS | SUBNET MASK | NO. SUBNETS | NO. HOSTS PER SUBNET |
|---|---|---|---|
| 1 | 255.255.255.128 (/25) | 2 | 126 |
| 2 | 255.255.255.192 (/26) | 4 | 62 |
| 3 | 255.255.255.224 (/27) | 8 | 30 |
| 4 | 255.255.255.240 (/28) | 16 | 14 |
| 5 | 255.255.255.248 (/29) | 32 | 6 |
| 6 | 255.255.255.252 (/30) | 64 | 2 |
| 7 | 255.255.255.254 (/31) | 128 | 1 |

The following table is a summary for subnet planning on a network with a 16-bit network number.

**Table 79** 16-bit Network Number Subnet Planning

| NO. "BORROWED" HOST BITS | SUBNET MASK | NO. SUBNETS | NO. HOSTS PER SUBNET |
|---|---|---|---|
| 1 | 255.255.128.0 (/17) | 2 | 32766 |
| 2 | 255.255.192.0 (/18) | 4 | 16382 |
| 3 | 255.255.224.0 (/19) | 8 | 8190 |
| 4 | 255.255.240.0 (/20) | 16 | 4094 |
| 5 | 255.255.248.0 (/21) | 32 | 2046 |
| 6 | 255.255.252.0 (/22) | 64 | 1022 |
| 7 | 255.255.254.0 (/23) | 128 | 510 |
| 8 | 255.255.255.0 (/24) | 256 | 254 |
| 9 | 255.255.255.128 (/25) | 512 | 126 |
| 10 | 255.255.255.192 (/26) | 1024 | 62 |
| 11 | 255.255.255.224 (/27) | 2048 | 30 |
| 12 | 255.255.255.240 (/28) | 4096 | 14 |

**Table 79** 16-bit Network Number Subnet Planning (continued)

| NO. "BORROWED" HOST BITS | SUBNET MASK | NO. SUBNETS | NO. HOSTS PER SUBNET |
|---|---|---|---|
| 13 | 255.255.255.248 (/29) | 8192 | 6 |
| 14 | 255.255.255.252 (/30) | 16384 | 2 |
| 15 | 255.255.255.254 (/31) | 32768 | 1 |

## Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the LTE Device.

Once you have decided on the network number, pick an IP address for your LTE Device that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your LTE Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the LTE Device unless you are instructed to do otherwise.

## Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

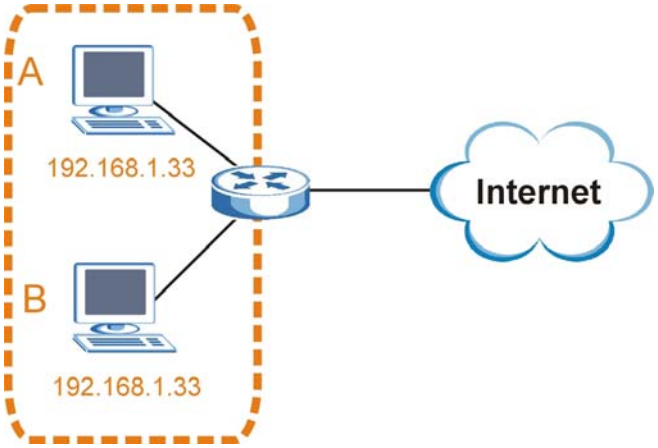
## IP Address Conflicts

Each device on a network must have a unique IP address. Devices with duplicate IP addresses on the same network will not be able to access the Internet or other resources. The devices may also be unreachable through the network.

## Conflicting Computer IP Addresses Example

More than one device can not use the same IP address. In the following example computer **A** has a static (or fixed) IP address that is the same as the IP address that a DHCP server assigns to computer **B** which is a DHCP client. Neither can access the Internet. This problem can be solved by assigning a different static IP address to computer **A** or setting computer **A** to obtain an IP address automatically.

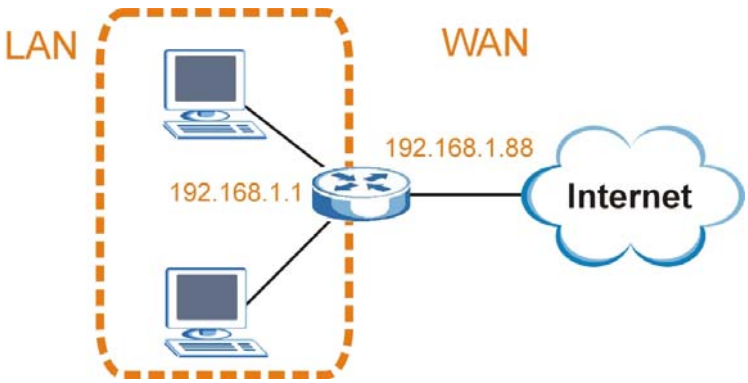
**Figure 94** Conflicting Computer IP Addresses Example




## Conflicting Router IP Addresses Example

Since a router connects different networks, it must have interfaces using different network numbers. For example, if a router is set between a LAN and the Internet (WAN), the router's LAN and WAN addresses must be on different subnets. In the following example, the LAN and WAN are on the same subnet. The LAN computers cannot access the Internet because the router cannot route between networks.

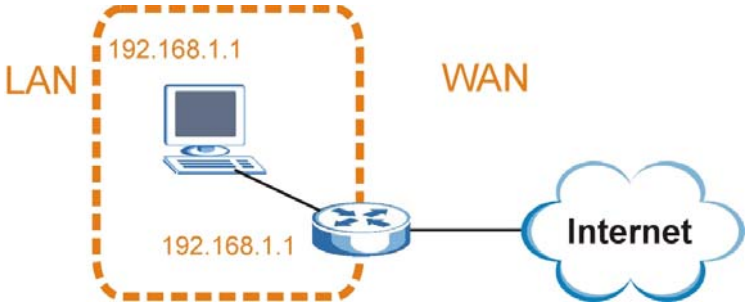
**Figure 95** Conflicting Computer IP Addresses Example



## Conflicting Computer and Router IP Addresses Example

More than one device can not use the same IP address. In the following example, the computer and the router's LAN port both use 192.168.1.1 as the IP address. The computer cannot access the Internet. This problem can be solved by assigning a different IP address to the computer or the router's LAN port.

**Figure 96** Conflicting Computer and Router IP Addresses Example



B

# Setting Up Your Computer's IP Address

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

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

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

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

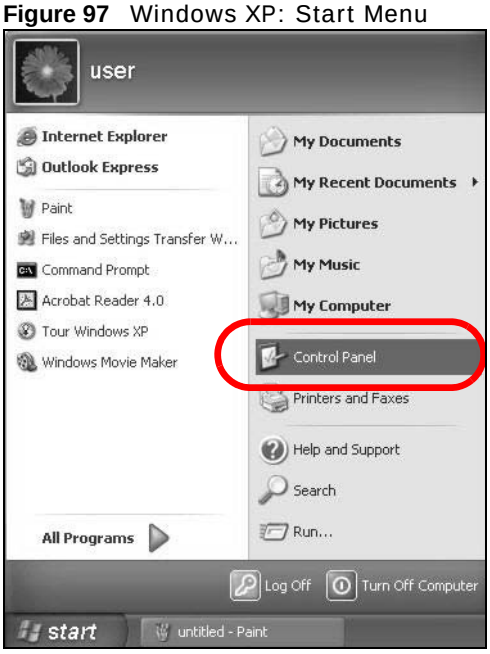

- Windows XP/NT/2000 on page 167
- Windows Vista on page 171
- Windows 7 on page 175
- Mac OS X: 10.3 and 10.4 on page 179
- Mac OS X: 10.5 on page 182
- Linux: Ubuntu 8 (GNOME) on page 186
- Linux: openSUSE 10.3 (KDE) on page 190


## Windows XP/NT/2000

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

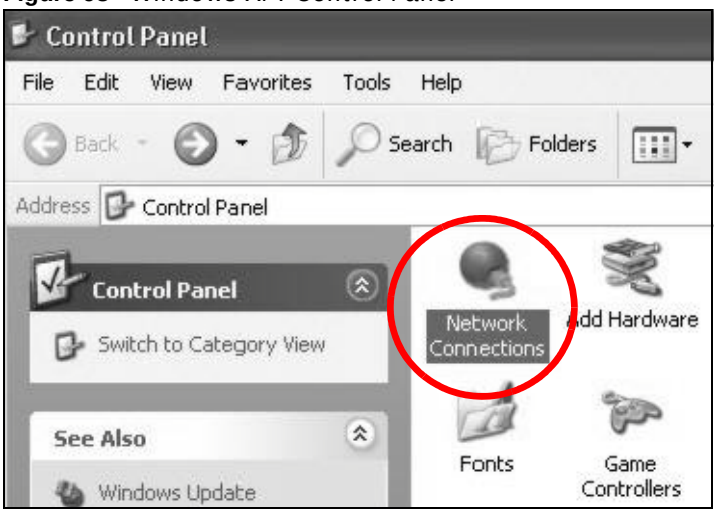
1 Click **Start** > **Control Panel**.

**Figure 97** Windows XP: Start Menu



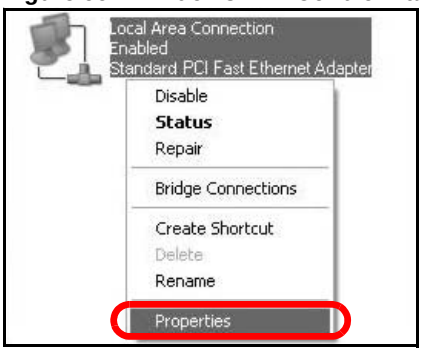

2 In the **Control Panel**, click the **Network Connections** icon.

**Figure 98** Windows XP: Control Panel



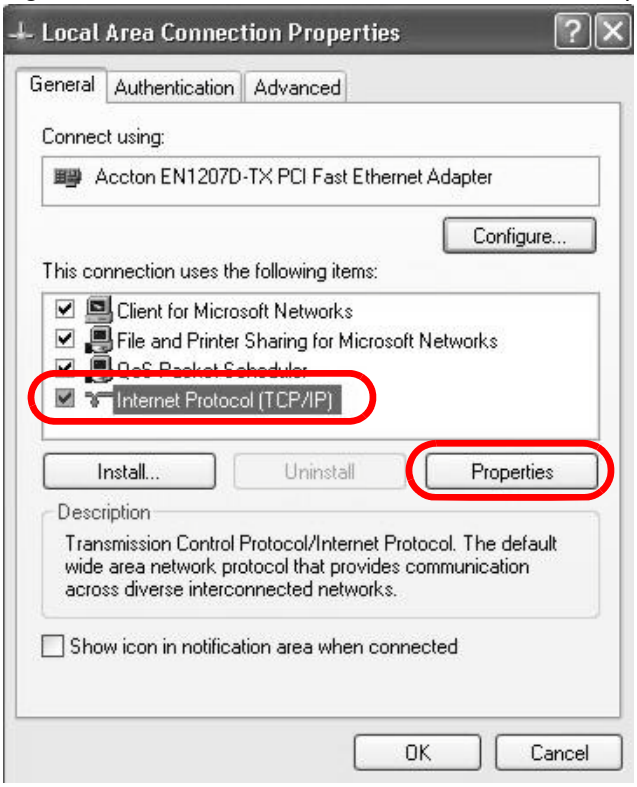
3 Right-click **Local Area Connection** and then select **Properties**.

**Figure 99** Windows XP: Control Panel > Network Connections > Properties



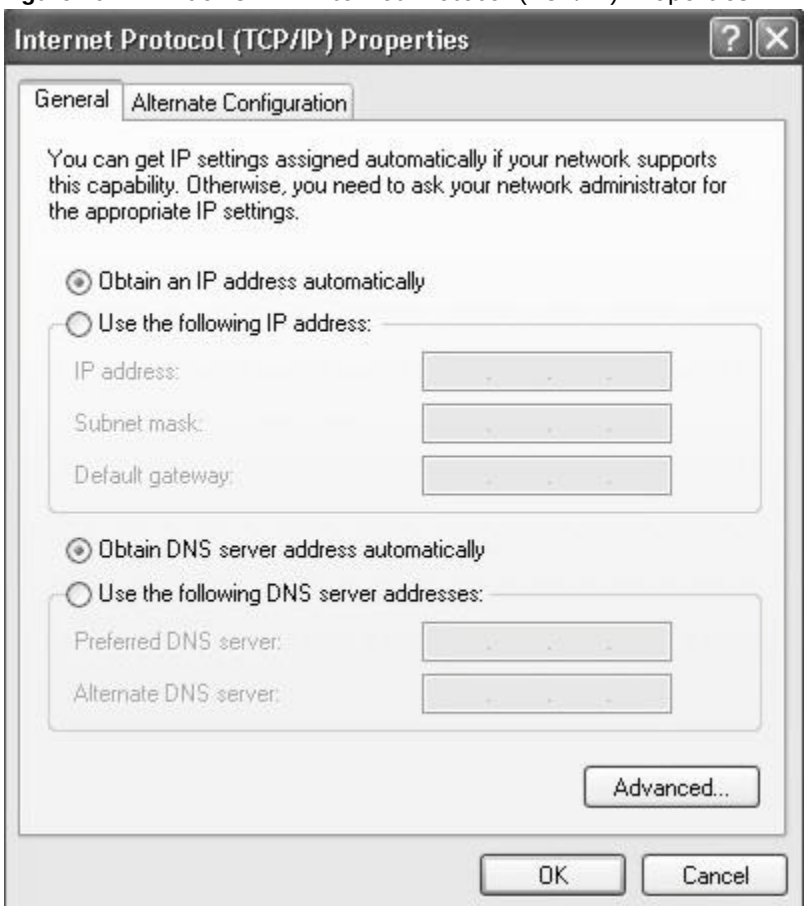

4 On the **General** tab, select **Internet Protocol (TCP/IP)** and then click **Properties**.

**Figure 100** Windows XP: Local Area Connection Properties



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

**Figure 101** Windows XP: Internet Protocol (TCP/IP) Properties




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].

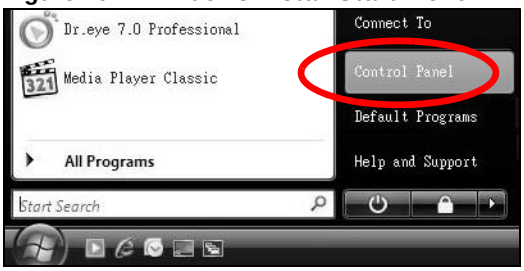
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

## Windows Vista

This section shows screens from Windows Vista Professional.

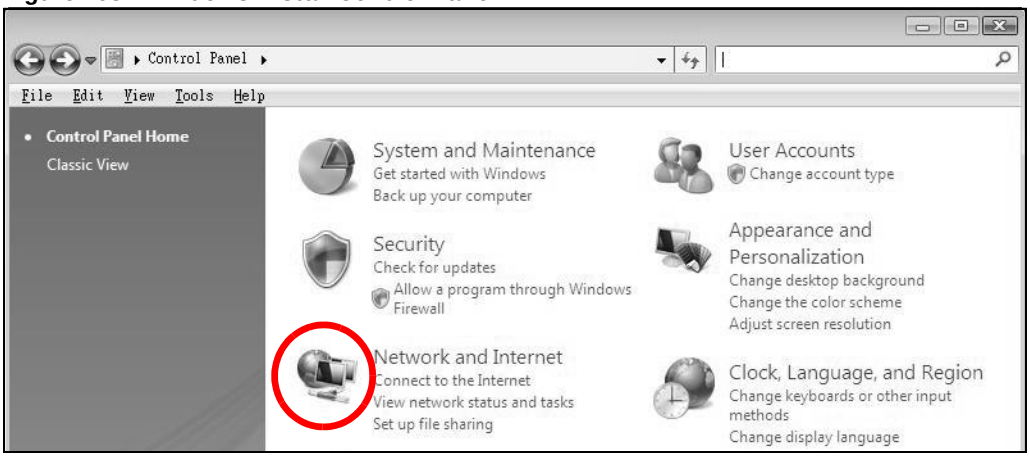
1 Click **Start** > **Control Panel**.

**Figure 102** Windows Vista: Start Menu



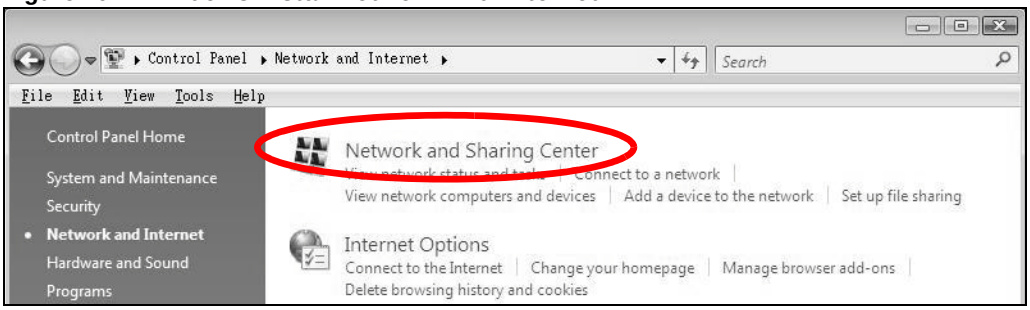

2 In the **Control Panel**, click the **Network and Internet** icon.

**Figure 103** Windows Vista: Control Panel



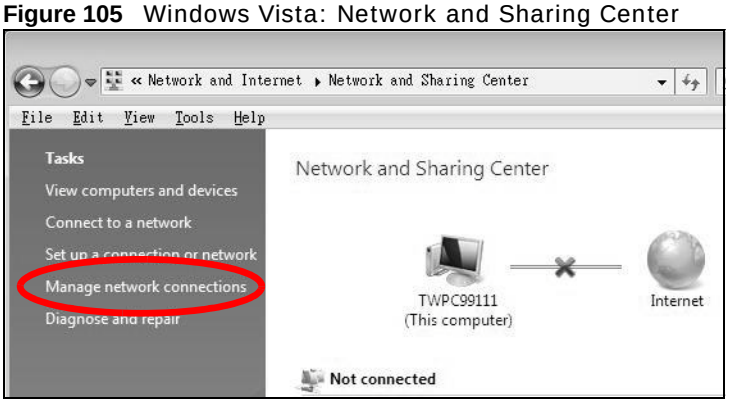

3 Click the **Network and Sharing Center** icon.

**Figure 104** Windows Vista: Network And Internet



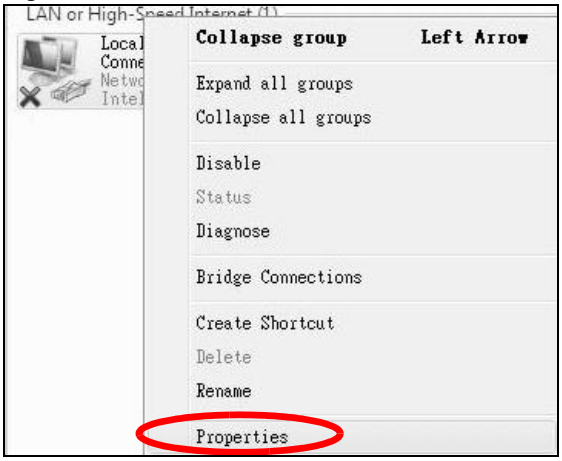
4 Click **Manage network connections**.

**Figure 105** Windows Vista: Network and Sharing Center




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

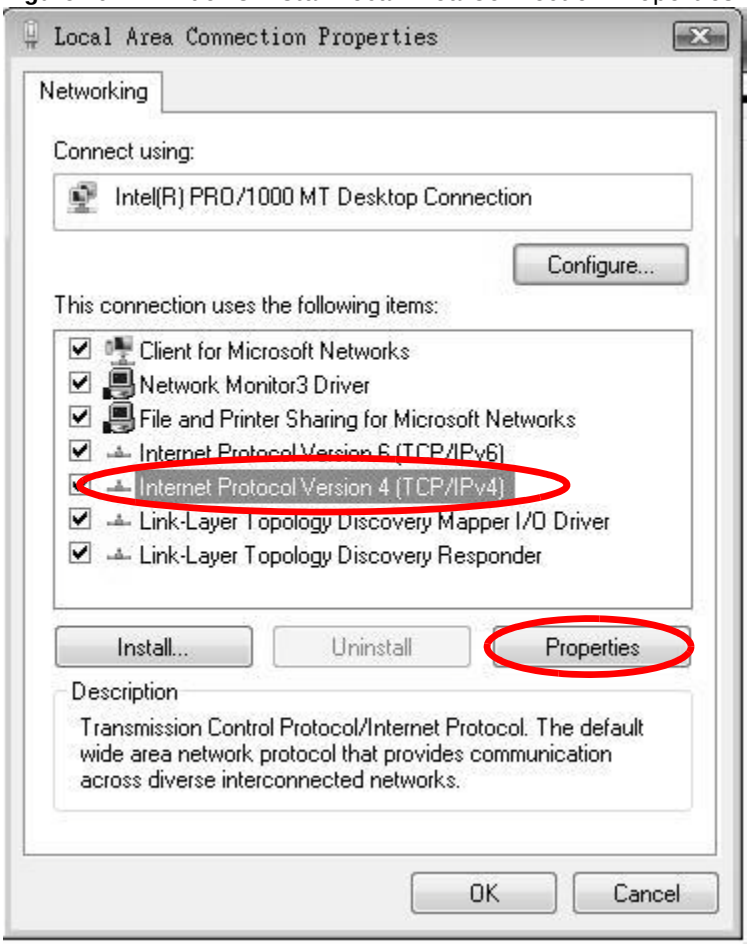
**Figure 106** Windows Vista: Network and Sharing Center




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

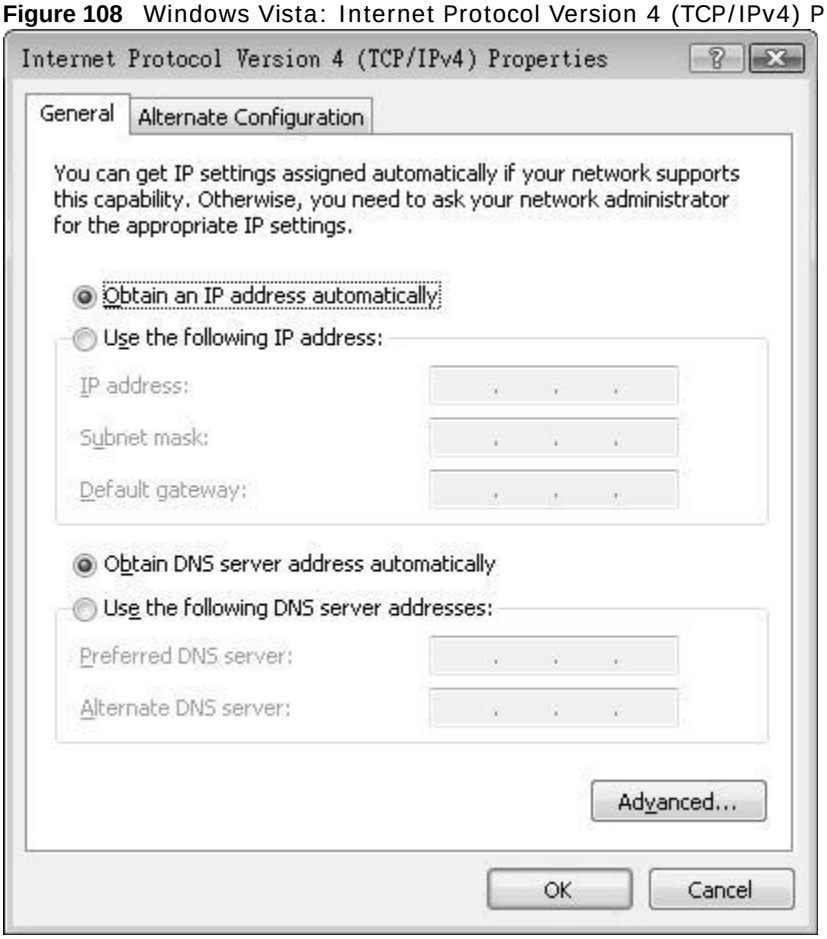
6 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

**Figure 107** Windows Vista: Local Area Connection Properties



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

**Figure 108** Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties




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].

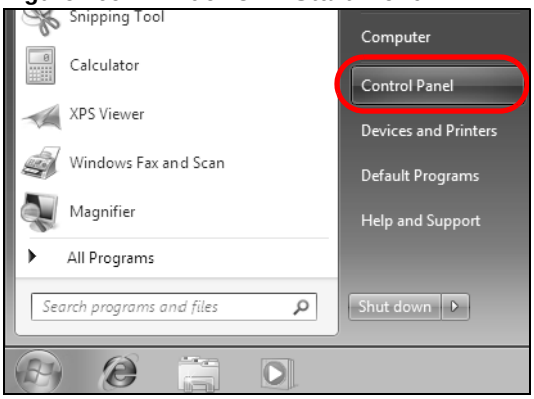
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

## Windows 7

This section shows screens from Windows 7 Enterprise.

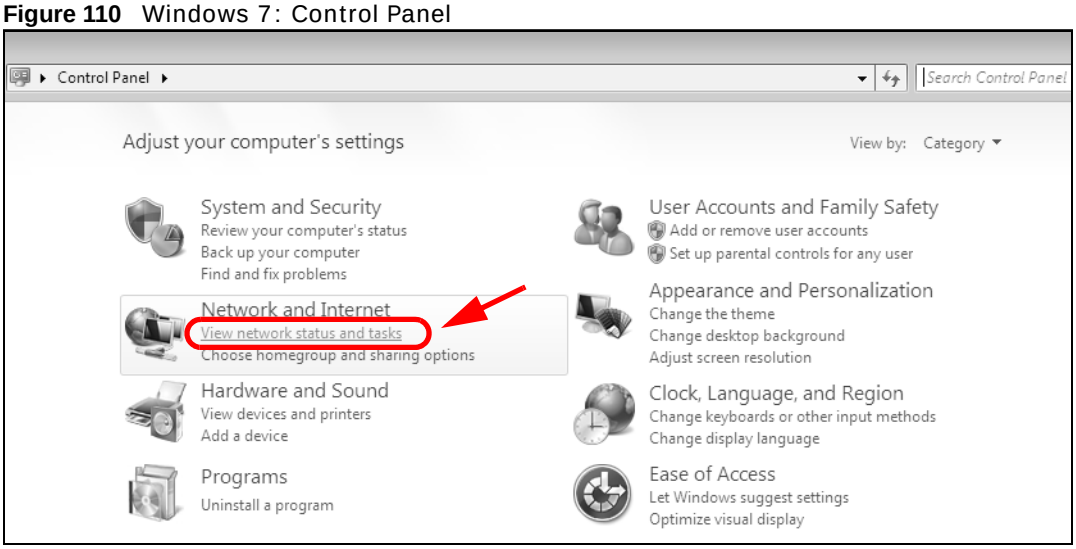
1 Click **Start** > **Control Panel**.

**Figure 109** Windows 7: Start Menu



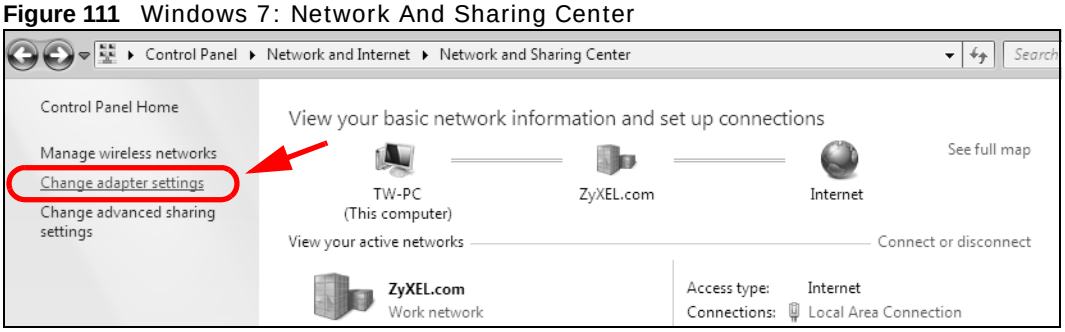

2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.

**Figure 110** Windows 7: Control Panel



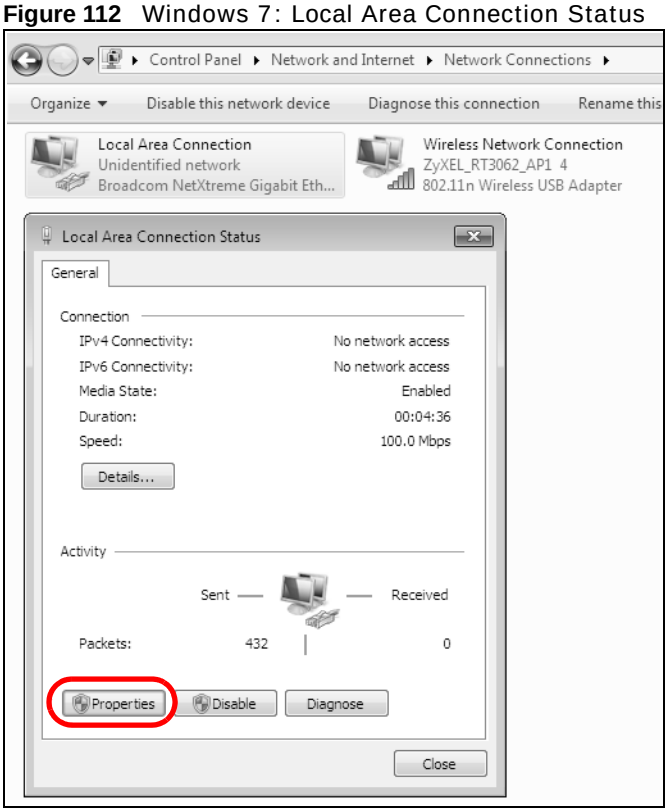

3 Click **Change adapter settings**.

**Figure 111** Windows 7: Network And Sharing Center



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

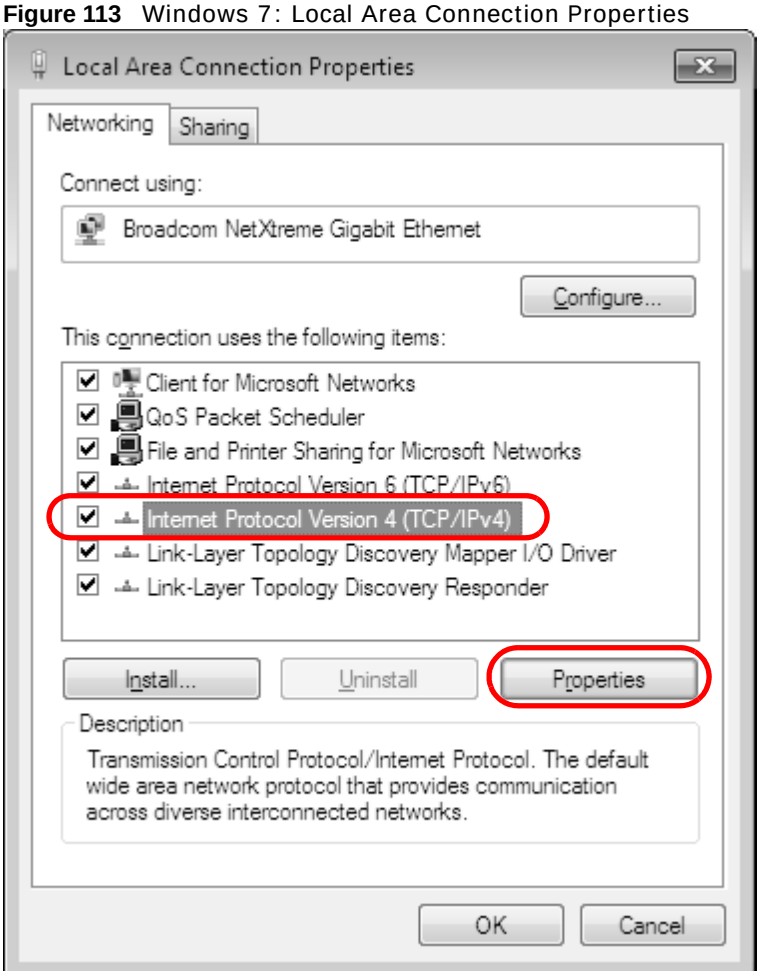
**Figure 112** Windows 7: Local Area Connection Status




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

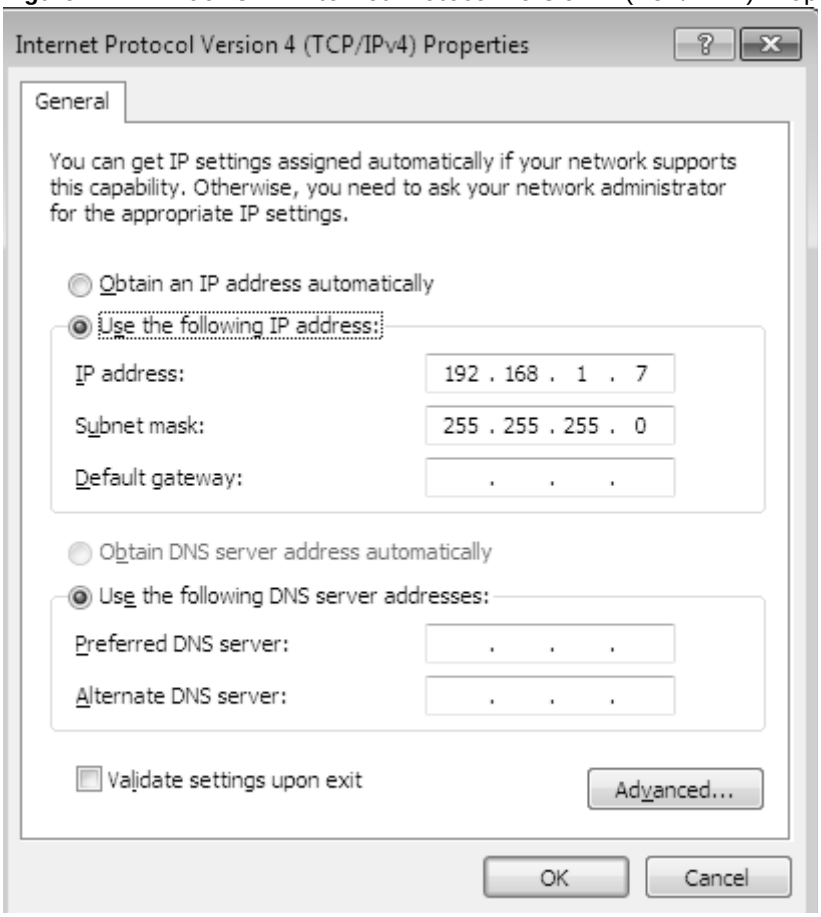
5 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

**Figure 113** Windows 7: Local Area Connection Properties



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

**Figure 114** Windows 7: Internet Protocol Version 4 (TCP/IPv4) Properties




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.

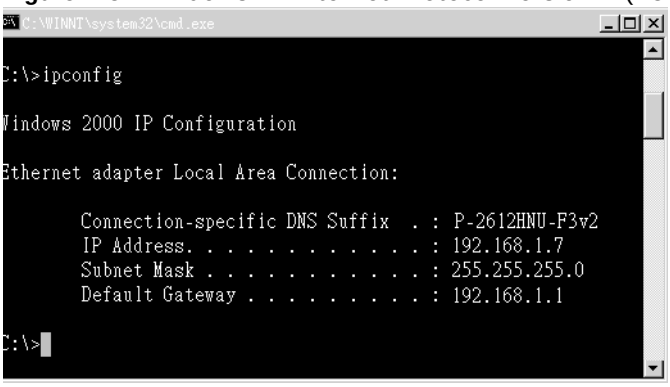
## Verifying Settings

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.

**Figure 115** Windows 7: Internet Protocol Version 4 (TCP/IPv4) Properties




## 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**.

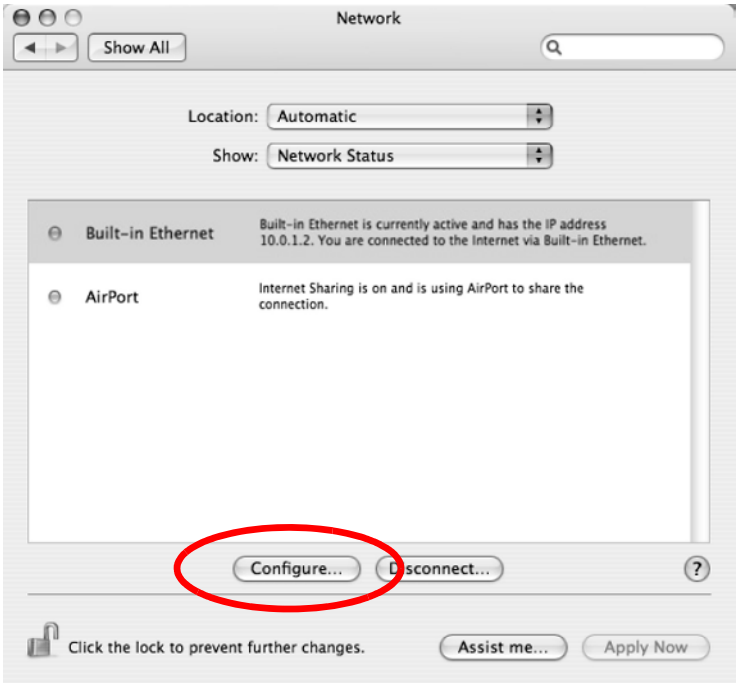
**Figure 116** Mac OS X 10.4: Apple Menu

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

**Figure 117** Mac OS X 10.4: System Preferences

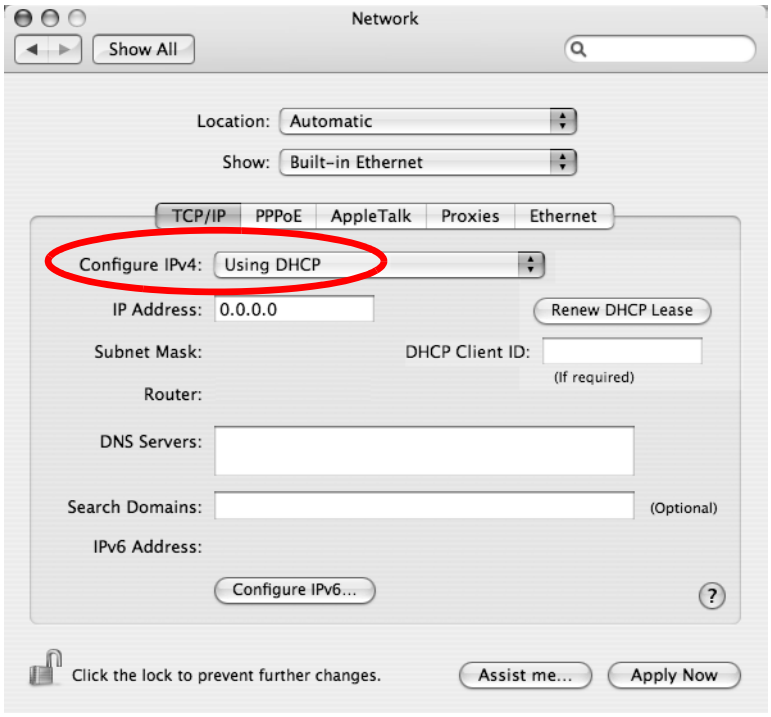

3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure.**

**Figure 118** Mac OS X 10.4: Network Preferences



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

**Figure 119** Mac OS X 10.4: Network Preferences > TCP/IP Tab.

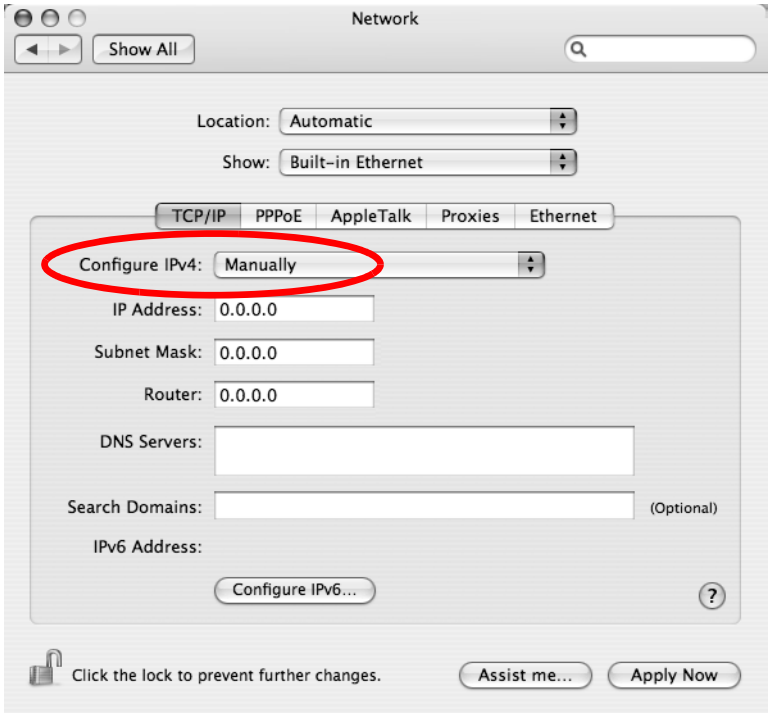



5 For statically assigned settings, do the following:

- 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.

**Figure 120** Mac OS X 10.4: Network Preferences > Ethernet

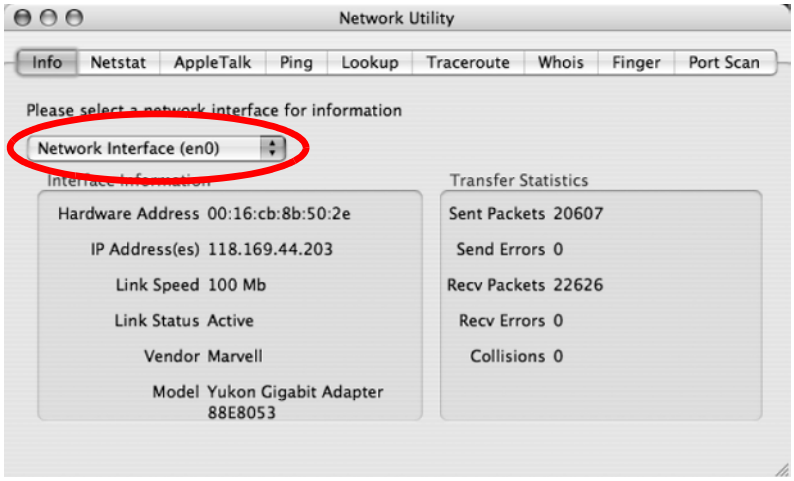



6 Click **Apply Now** and close the window.

## 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 121** Mac OS X 10.4: Network Utility

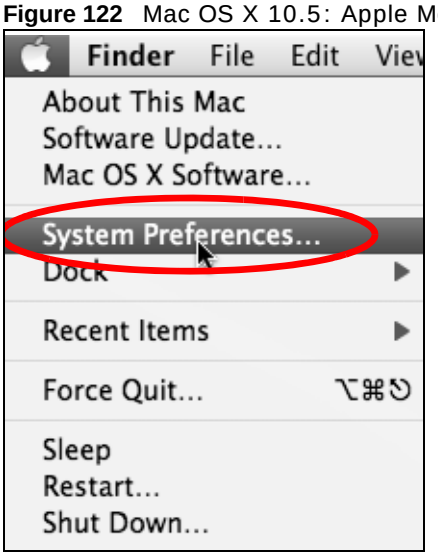



## Mac OS X: 10.5

The screens in this section are from Mac OS X 10.5.

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

**Figure 122** Mac OS X 10.5: Apple Menu

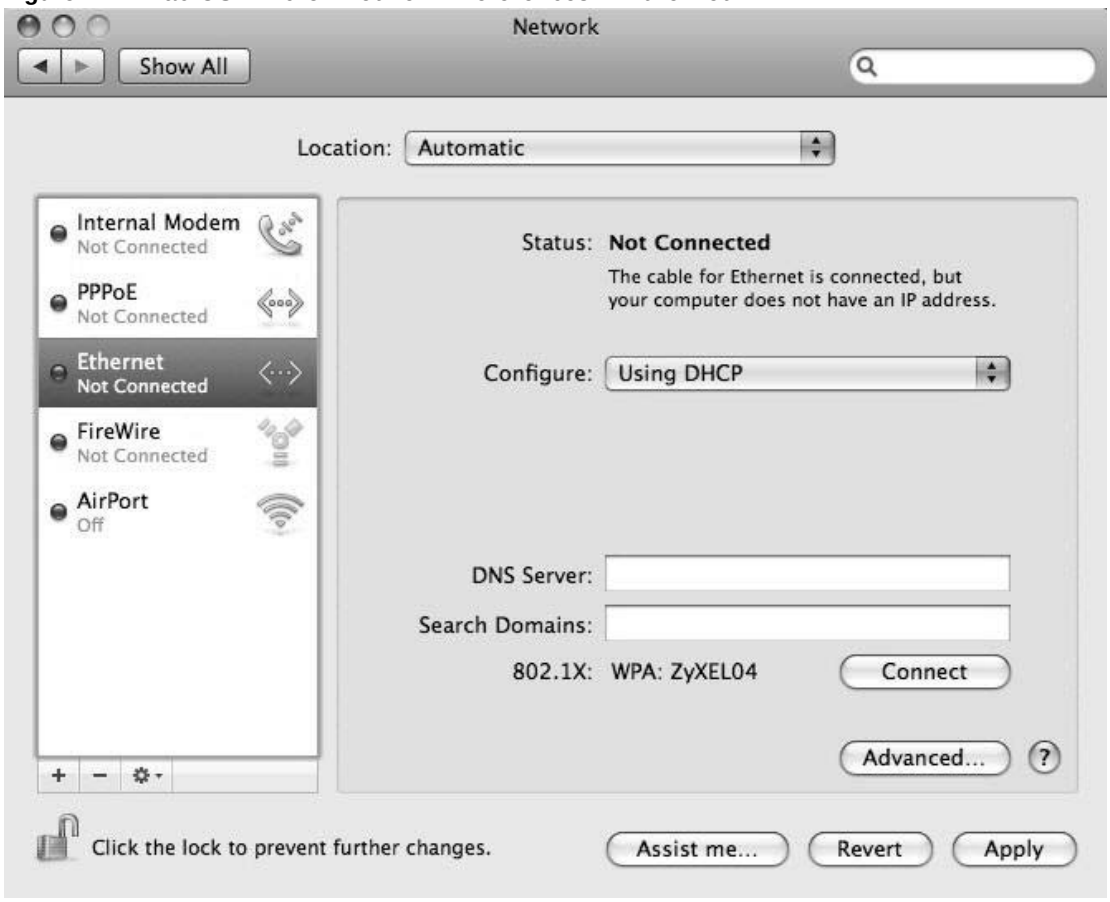



2 In **System Preferences**, click the **Network** icon.

**Figure 123** Mac OS X 10.5: Systems Preferences

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

**Figure 124** Mac OS X 10.5: Network Preferences > Ethernet



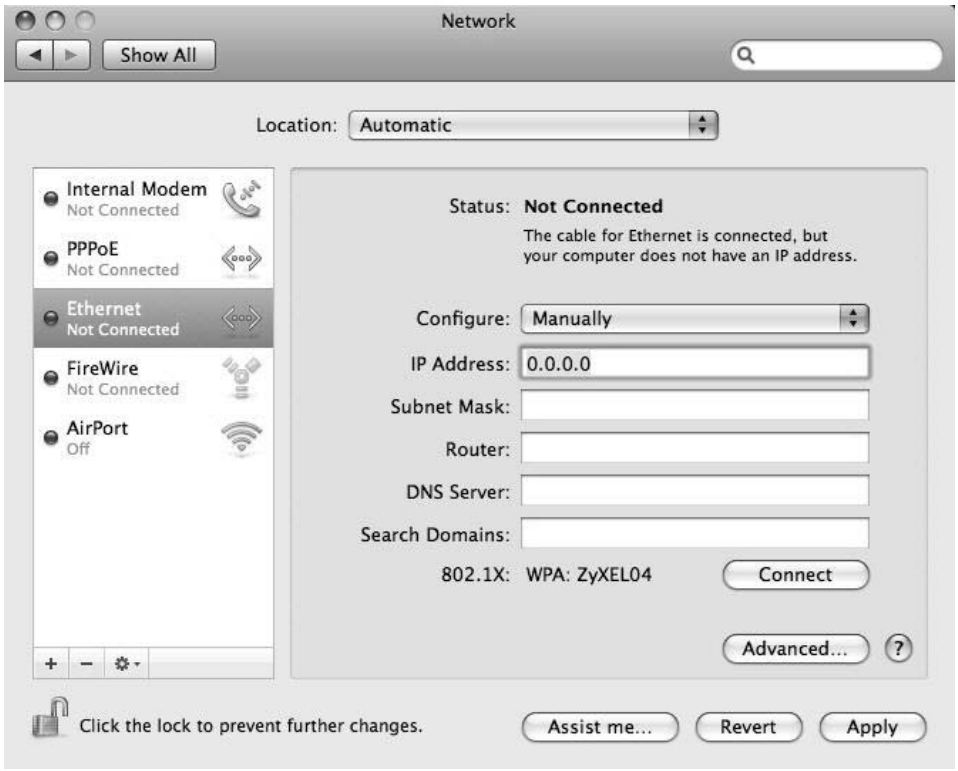

4 From the **Configure** list, select **Using DHCP** for dynamically assigned settings.

5 For statically assigned settings, do the following:

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

- In the **Router** field, enter the IP address of your LTE Device.

**Figure 125** Mac OS X 10.5: Network Preferences > Ethernet

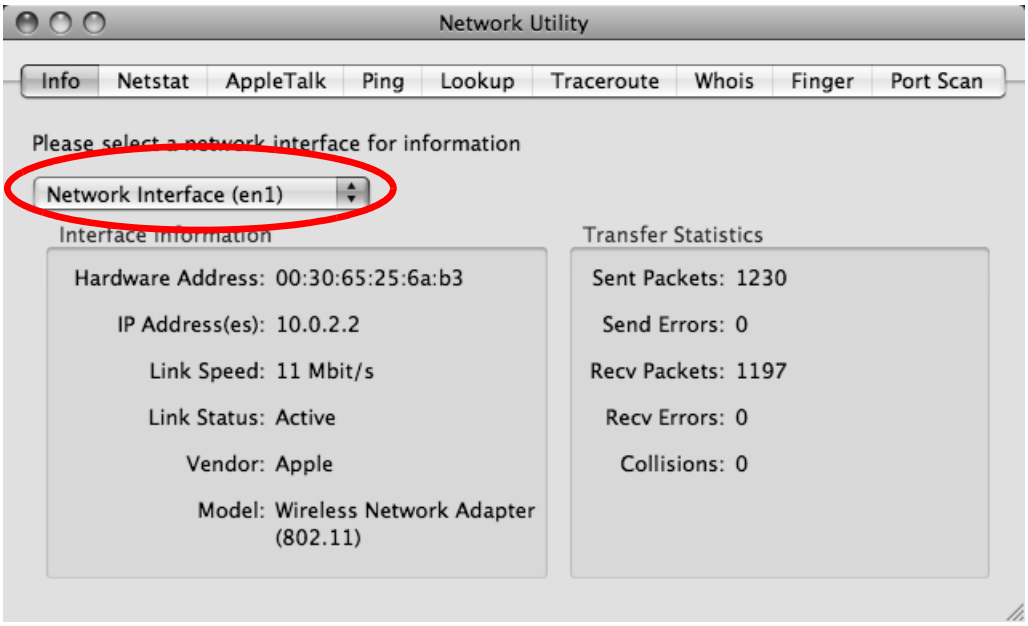



6 Click **Apply** and close the window.

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




## Linux: Ubuntu 8 (GNOME)

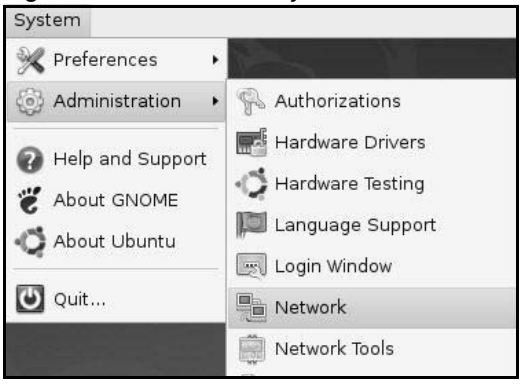
This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following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

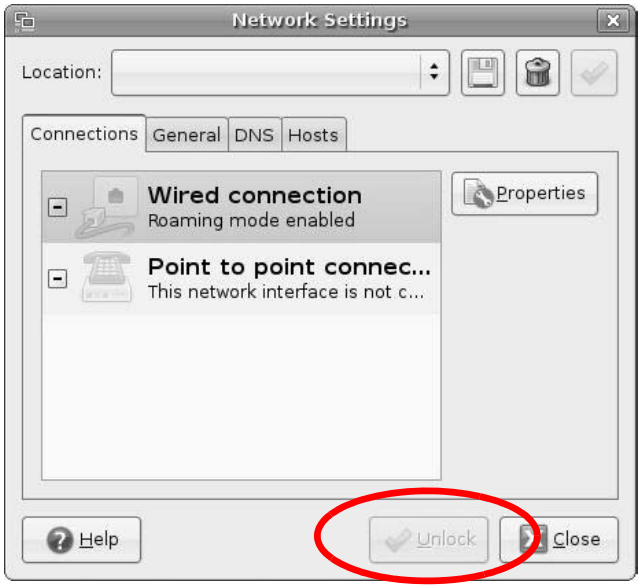
1 Click **System > Administration > Network**.

**Figure 127** Ubuntu 8: System > Administration Menu



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.

**Figure 128** Ubuntu 8: Network Settings > Connections

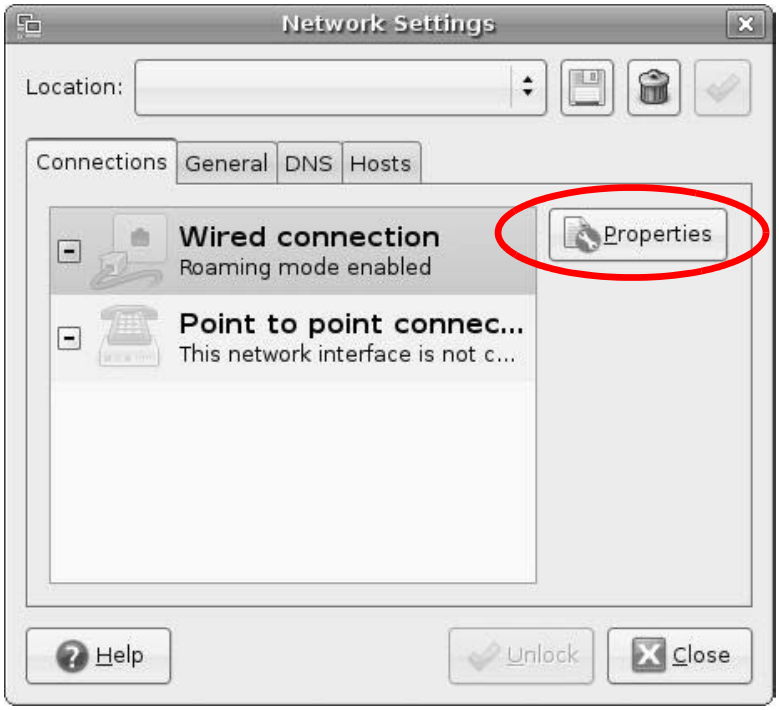



3 In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.

**Figure 129** Ubuntu 8: Administrator Account Authentication

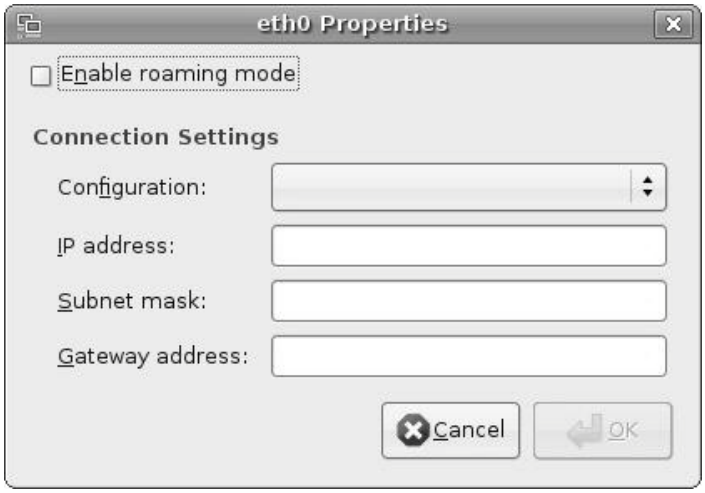
4 In the **Network Settings** window, select the connection that you want to configure, then click **Properties**.

**Figure 130** Ubuntu 8: Network Settings > Connections




5 The **Properties** dialog box opens.

**Figure 131** Ubuntu 8: Network Settings > Properties

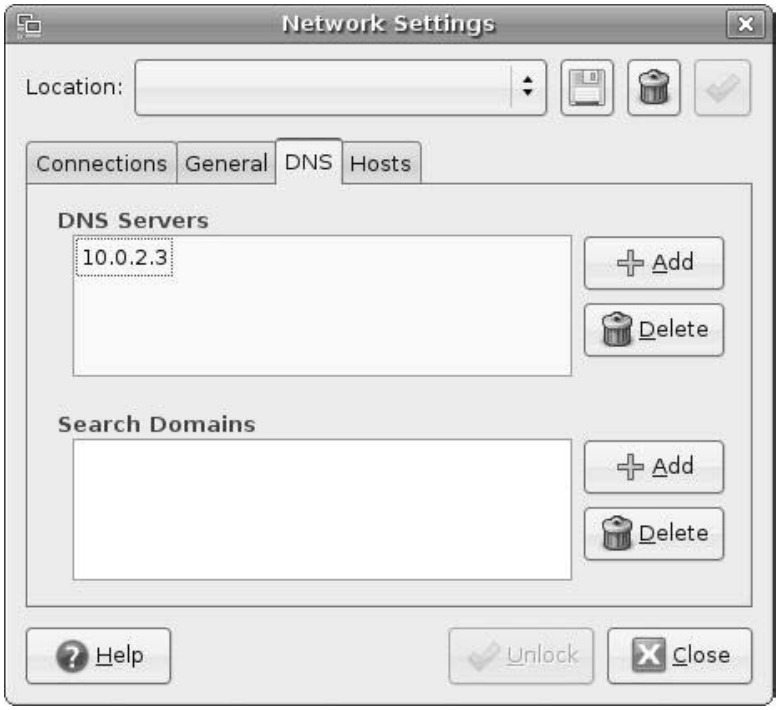



- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
- In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.

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.

**Figure 132** Ubuntu 8: Network Settings > DNS

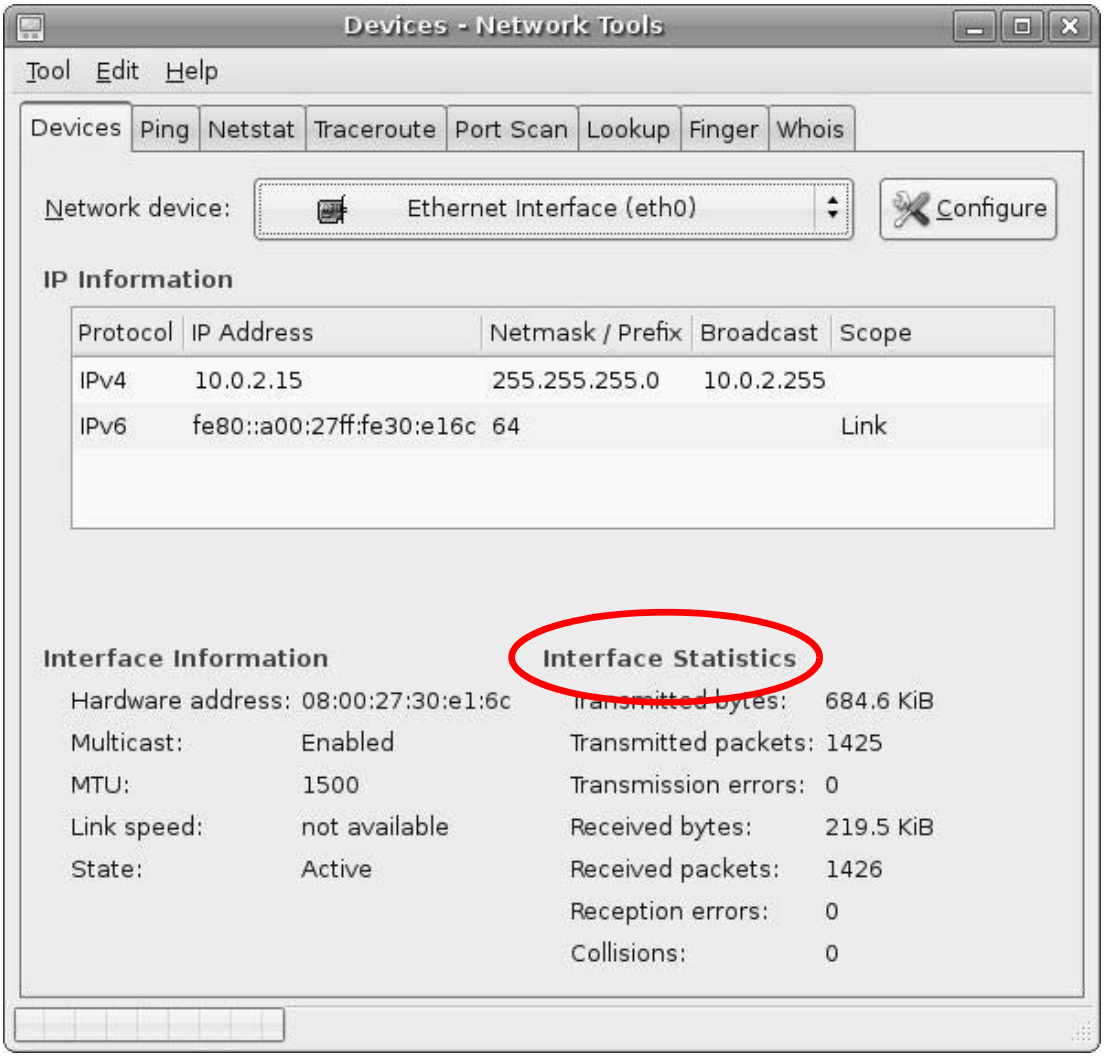



8 Click the **Close** button to apply the changes.

## 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 133** Ubuntu 8: Network Tools




## Linux: openSUSE 10.3 (KDE)

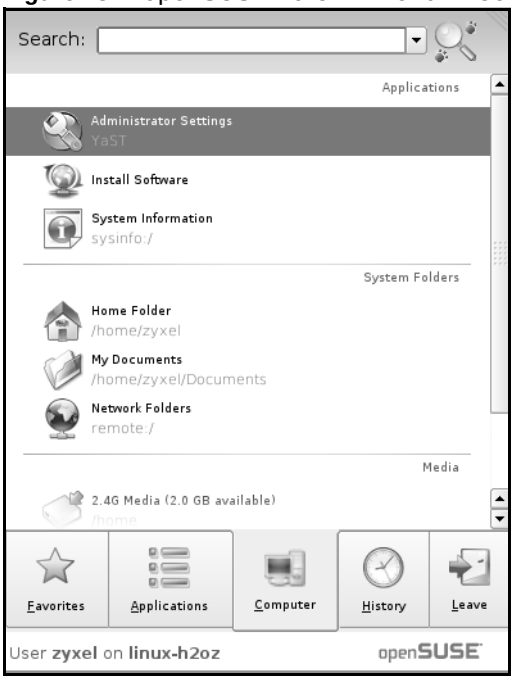
This section shows you how to configure your computer's TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following 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:

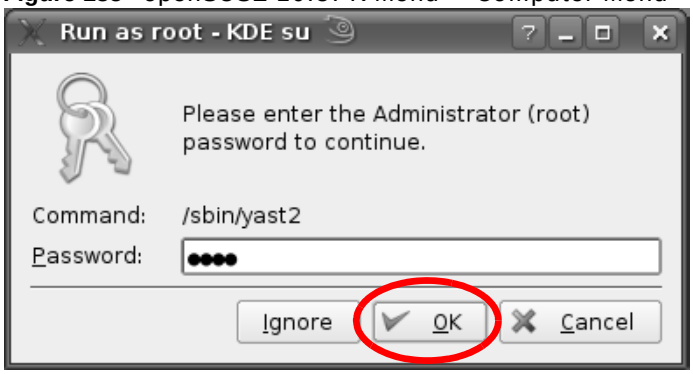
1 Click **K Menu > Computer > Administrator Settings (YaST)**.

**Figure 134** openSUSE 10.3: K Menu > Computer Menu



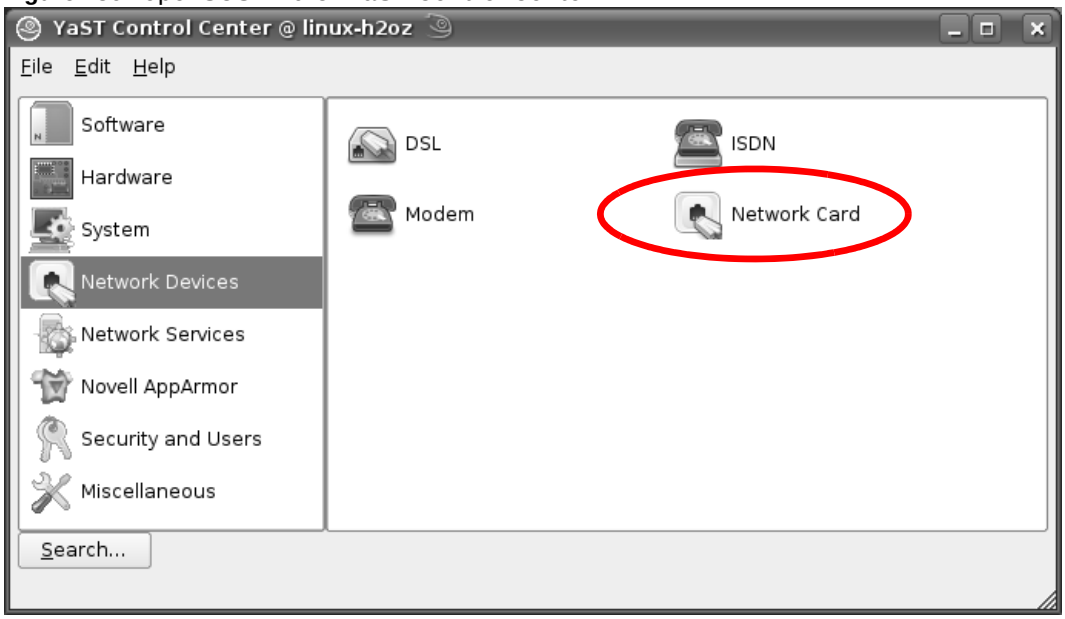

2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.

**Figure 135** openSUSE 10.3: K Menu > Computer Menu



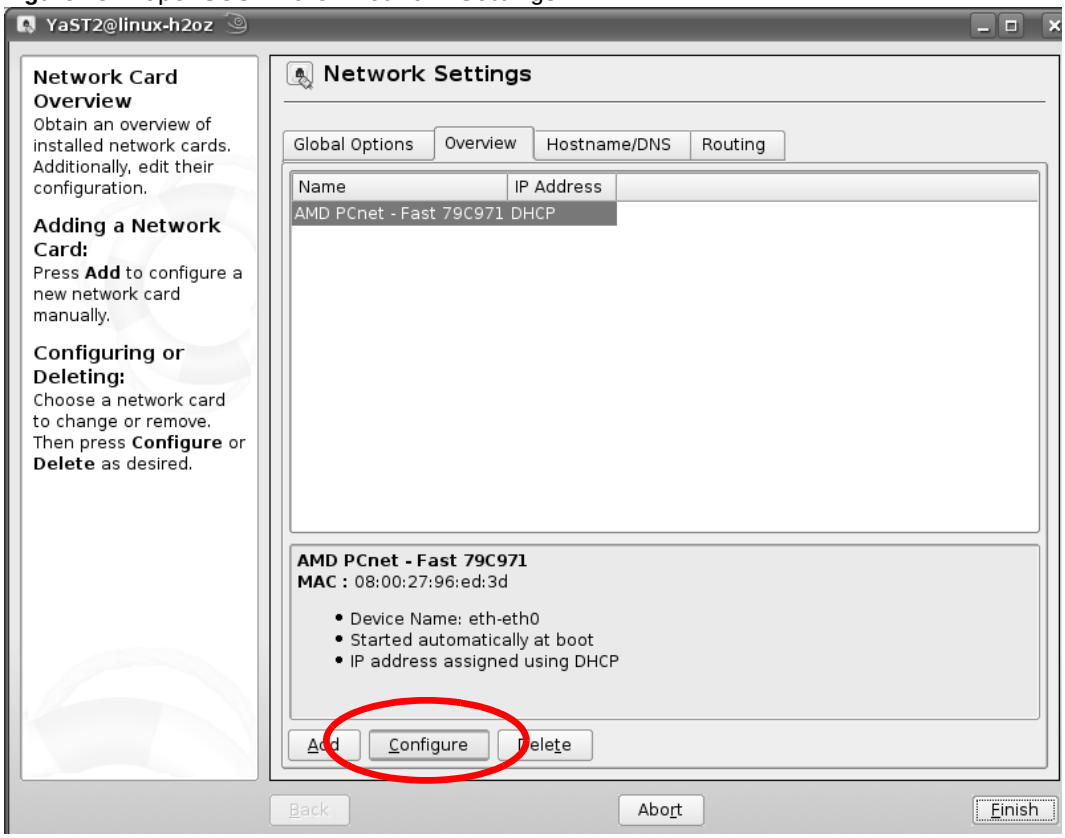
3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.

**Figure 136** openSUSE 10.3: YaST Control Center



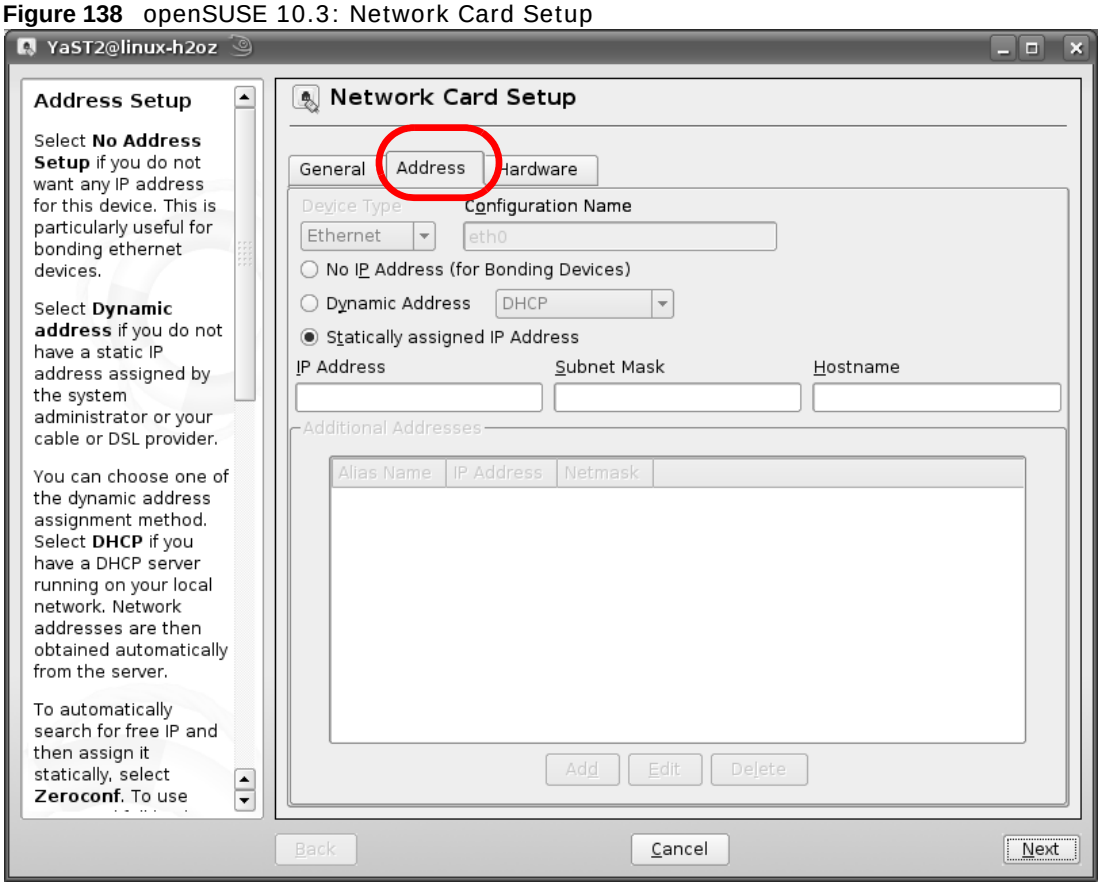

4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.

**Figure 137** openSUSE 10.3: Network Settings



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

**Figure 138** openSUSE 10.3: Network Card Setup



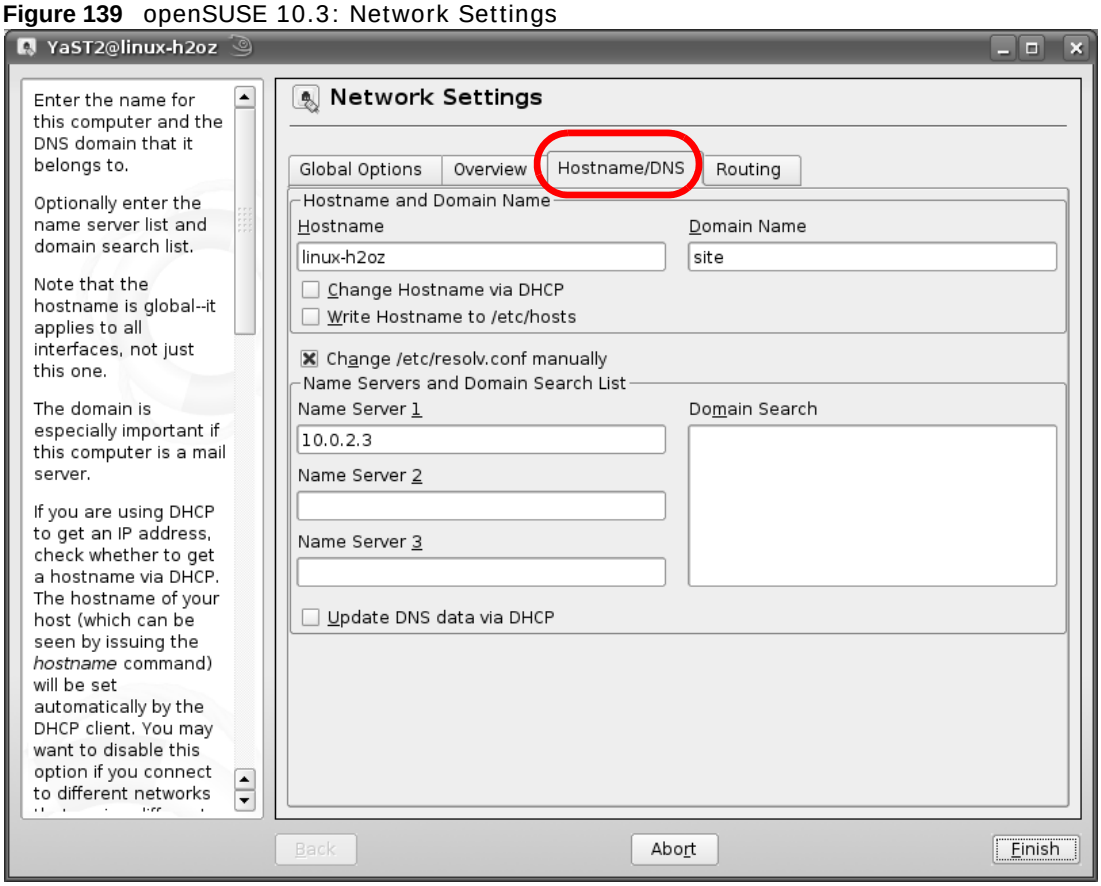

6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.

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.

**Figure 139** openSUSE 10.3: Network Settings

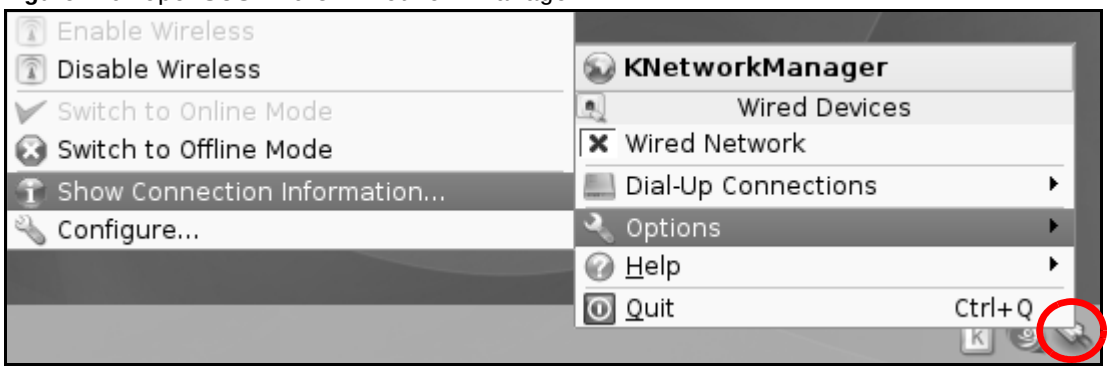



9 Click **Finish** to save your settings and close the window.

## Verifying Settings

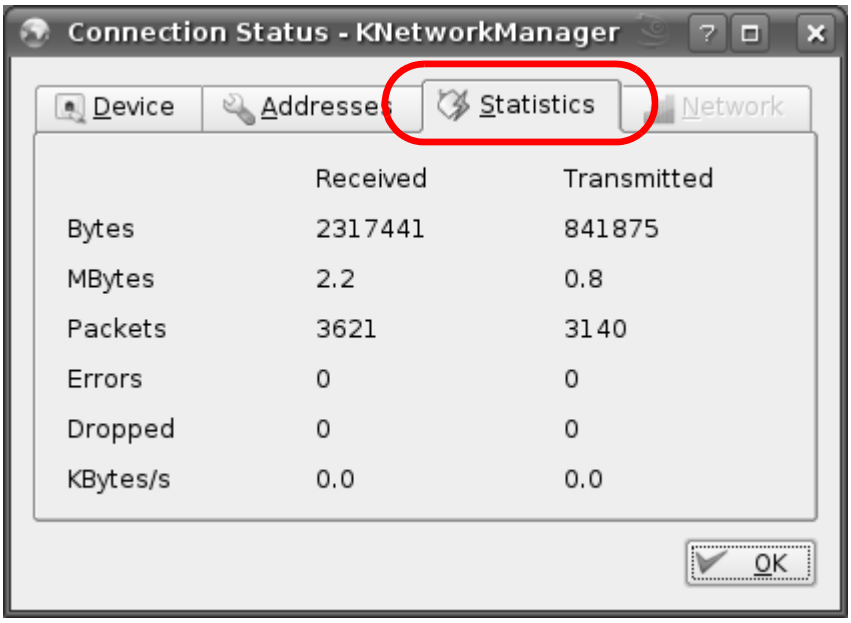
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

**Figure 140** 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 141** openSUSE: Connection Status - KNetwork Manager



C

# 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: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

## Internet Explorer Pop-up Blockers

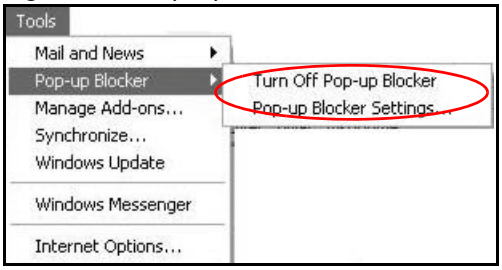
You may have to disable pop-up blocking to log into your device.

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 142** Pop-up Blocker

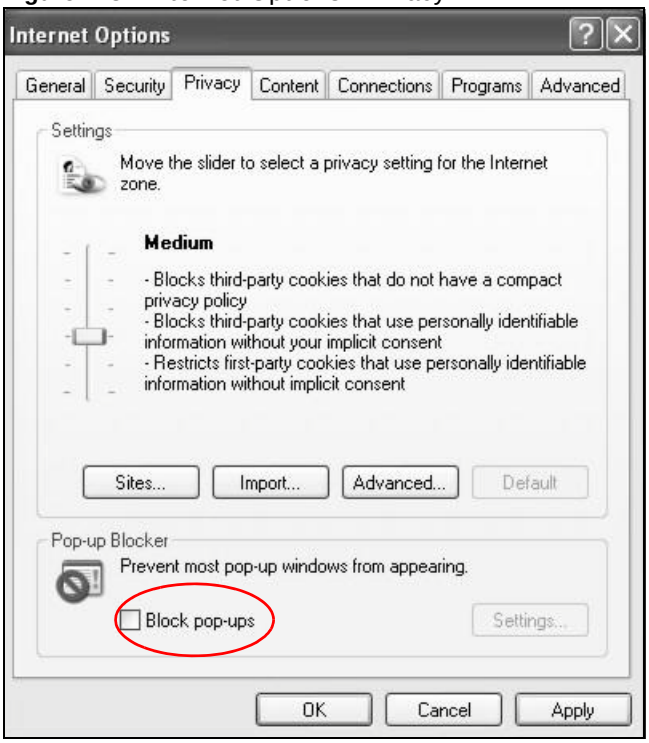



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

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 143** Internet Options: Privacy




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

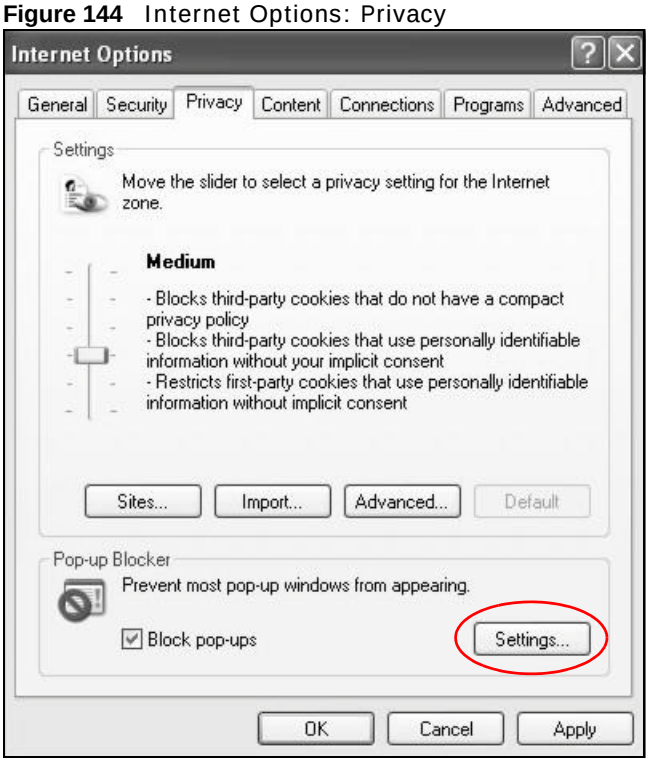
## Enable Pop-up Blockers with Exceptions

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.

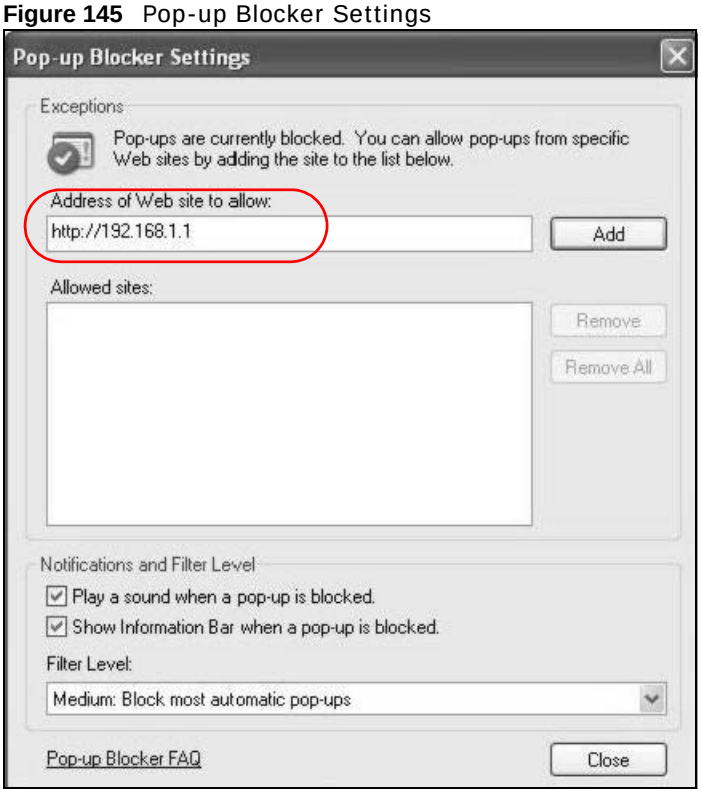
**Figure 144** Internet Options: Privacy




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 145** Pop-up Blocker Settings




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

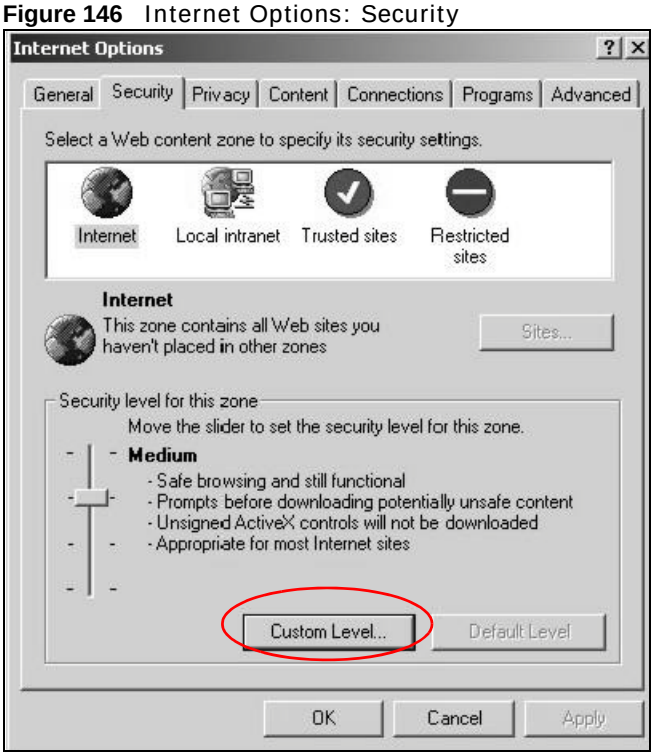
6 Click **Apply** to save this setting.

## 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 146** Internet Options: Security




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

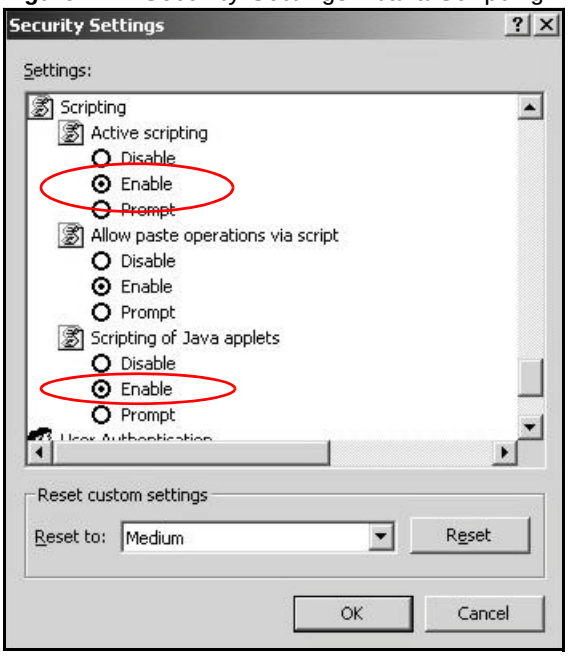
3 Scroll down to **Scripting**.

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 147** Security Settings - Java Scripting




## Java Permissions

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

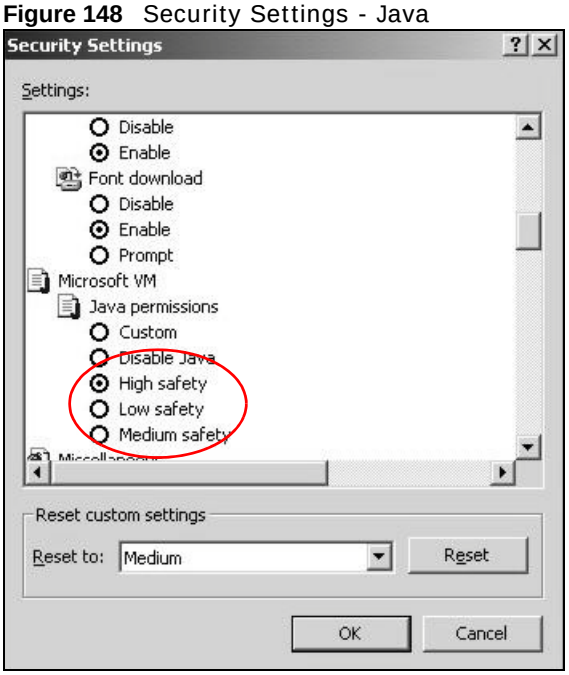
2 Click the **Custom Level...** button.

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 148** Security Settings - Java



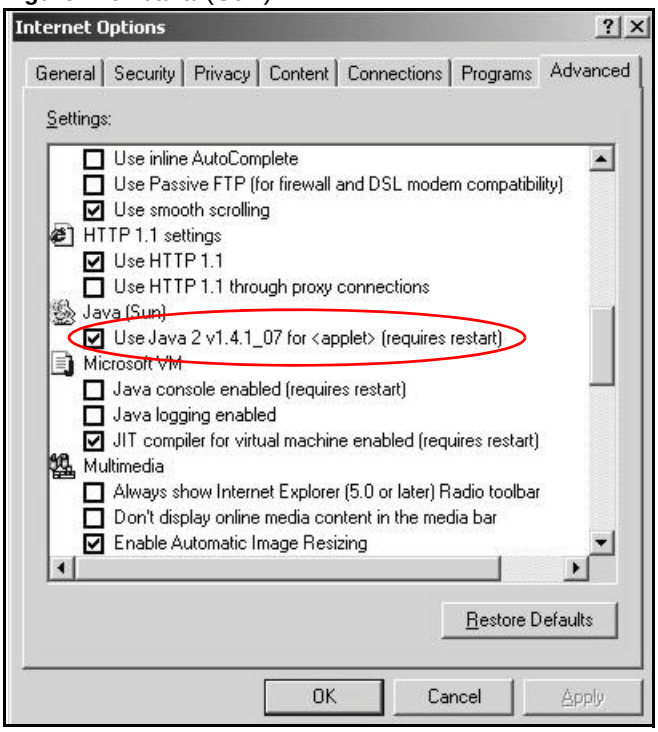

## JAVA (Sun)

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 149** Java (Sun)




## Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary.

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

**Figure 150** Mozilla Firefox: Tools > Options

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

**Figure 151** Mozilla Firefox Content Security

# 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 80** 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.example.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. |
| HTTPS | TCP | 443 | HTTPS is a secured http session often used in e-commerce. |

**Table 80** Commonly Used Services (continued)

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|---|---|---|---|
| ICMP | User-Defined | 1 | Internet Control Message Protocol is often used for diagnostic or routing purposes. |
| ICQ | UDP | 4000 | This is a popular Internet chat program. |
| IGMP (MULTICAST) | User-Defined | 2 | Internet Group Management Protocol is used when sending packets to a specific group of hosts. |
| IKE | UDP | 500 | The Internet Key Exchange algorithm is used for key distribution and management. |
| IRC | TCP/UDP | 6667 | This is another popular Internet chat program. |
| MSN Messenger | TCP | 1863 | Microsoft Networks' messenger service uses this protocol. |
| NEW-ICQ | TCP | 5190 | An Internet chat program. |
| NEWS | TCP | 144 | A protocol for news groups. |
| NFS | UDP | 2049 | Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments. |
| NNTP | TCP | 119 | Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service. |
| PING | User-Defined | 1 | Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable. |
| POP3 | TCP | 110 | Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other). |
| PPTP | TCP | 1723 | Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel. |
| PPTP_TUNNEL (GRE) | User-Defined | 47 | PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel. |
| RCMD | TCP | 512 | Remote Command Service. |
| REAL_AUDIO | TCP | 7070 | A streaming audio service that enables real time sound over the web. |
| REXEC | TCP | 514 | Remote Execution Daemon. |
| RLOGIN | TCP | 513 | Remote Login. |
| RTELNET | TCP | 107 | Remote Telnet. |
| RTSP | TCP/UDP | 554 | The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet. |
| SFTP | TCP | 115 | Simple File Transfer Protocol. |
| SMTP | TCP | 25 | Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another. |
| SNMP | TCP/UDP | 161 | Simple Network Management Program. |
| SNMP-TRAPS | TCP/UDP | 162 | Traps for use with the SNMP (RFC:1215). |
| SQL-NET | TCP | 1521 | Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers. |
| SSH | TCP/UDP | 22 | Secure Shell Remote Login Program. |
| STRM WORKS | UDP | 1558 | Stream Works Protocol. |
| SYSLOG | UDP | 514 | Syslog allows you to send system logs to a UNIX server. |

**Table 80** Commonly Used Services (continued)

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



### Disclaimers

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.

Your use of the LTE Device is subject to the terms and conditions of any related service providers.

Do not use the LTE Device for illegal purposes. Illegal downloading or sharing of files can result in severe civil and criminal penalties. You are subject to the restrictions of copyright laws and any other applicable laws, and will bear the consequences of any infringements thereof. ZyXEL bears NO responsibility or liability for your use of the download service feature.

### Trademarks

Trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

## Certifications

### Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device complies with part 15 of the FCC Rules.
- Operation is subject to the condition that this device does not cause harmful interference.

This device has been tested and found to comply with the limits 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 in accordance with 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/television reception, which can be determined 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:

1 Reorient or relocate the receiving antenna.

2 Increase the separation between the equipment and the receiver.

3 Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

4 Consult the dealer or an experienced radio/TV technician for help.

### FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

注意 ！

依據　低功率電波輻射性電機管理辦法

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，指依電信規定作業之無線電信。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。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。
減少電磁波影響，請妥適使用。

### Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

### Viewing Certifications

1 Go to http://www.zyxel.com.

2 Select your product on the ZyXEL home page to go to that product's page.

3 Select the certification you wish to view from this page.

## ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. 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.

#### 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.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- 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.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the indoor device (IDU) outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.
- Make sure that the cable system is grounded so as to provide some protection against voltage surges.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

# Index

## A

activation
SSID 49
wireless LAN
scheduling 54
administrator password 19
AH 120
algorithms 120
alternative subnet mask notation 160
applications
Internet access 13
authentication 55, 56
RADIUS server 56
automatic logout 20

## B

backup
configuration 145
bandwidth management 77
Basic Service Set, see BSS
blinking LEDs 16
Broadband 33
BSS 58
example 58

## C

certification
notices 212
viewing 212
channel scan 45
channel, wireless LAN 42
client list 70
configuration
backup 145
reset 147
restoring 146
copyright 211
CoS 85
CTS threshold 55

## D

data fragment threshold 55
default LAN IP address 19
Denials of Service, see DoS
DH 126
DHCP 30, 68, 95
diagnostic 149
Differentiated Services, see DiffServ
Diffie-Hellman key groups 126
DiffServ (Differentiated Services)
marking rule 86
DNS 68
DNS server address assignment 38
documentation
related 2
domain name system, see DNS
Domain Name System. See DNS.
DoS 98
DS (Differentiated Services) 85
DS field 85
DSCP 85
dynamic DNS 95
Dynamic Host Configuration Protocol, see DHCP
DYNDNS wildcard 95

## E

Encapsulation 37
encapsulation 121
encryption 57

ESP 120
Extended Service Set IDentification 44, 50

## F

FCC interference statement 211
filters
  MAC address 56
firewalls 97
  configuration 100
  DoS 98
  security 104
firmware 143
fragmentation threshold 55
FTP 88

## G

Guide
  Quick Start 2

## H

host 133
host name 30

## I

IANA 164
ID type and content 124
IKE phases 122
inside header 121
Internet access 13
Internet Assigned Numbers Authority, see IANA
Internet Key Exchange 122
IP address 30
  default 19
  WAN 34
IP Address Assignment 37
IP pool 69
IPSec
  algorithms 120
  architecture 120
  NAT 123
IPSec VPN 113

## L

LAN 67
  client list 70
  MAC address 71
limitations
  wireless LAN 57
  WPS 64
Local Area Network, see LAN
login
  passwords 19
logout 20
  automatic 20
logs 127, 141

## M

MAC 30, 107
MAC address 71
  filter 56
MAC address filtering 107
MAC filter 107
managing the device
  good habits 15
  using FTP. See FTP.
MBSSID 58
Media access control 107
Media Access Control, see MAC Address
model name 30
Multiple BSS, see MBSSID

## N

NAT 88, 164
  definitions 92
  how it works 93

IPSec 123
traversal 124
what it does 92
negotiation mode 122
Network Address Translation, see NAT
network map 23

## O

other documentation 2
outside header 121

## P

passphrase 46
passwords 19
PBC 59
PHB 86
PIN, WPS 59
example 61
ports 16
preamble 55
pre-shared key 125
product registration 213
Push Button Configuration, see PBC
push button, WPS 59

## Q

QoS 77, 85
Quality of Service, see QoS
Quick Start Guide 2, 19

## R

RADIUS server 56
registration
product 213
related documentation 2
reset 147
RESET button 16
restart 147
restoring configuration 146
RFC 1631 87
RFC 3164 127
router features 13
RTS threshold 55

## S

safety warnings 213
scan 45
scheduling
wireless LAN 54
security
wireless LAN 55
security, network 104
service access control 135
Service Set 44, 50
SSID 56
activation 49
MBSSID 58
static route 73
status 27
status indicators 16
subnet 157
subnet mask 158
subnetting 160
syslog
protocol 127
severity levels 127
system
firmware 143
passwords 19
status 27
System Info 29
system name 30, 138

## T

The 34

thresholds
data fragment 55
RTS/CTS 55
transport mode 121
tunnel mode 121

## U

Universal Plug and Play, see UPnP
upgrading firmware 143
UPnP 71
security issues 68

## V

version
firmware
version 30

## W

WAN
Wide Area Network, see WAN 33
warnings 213
Web Configurator 19
web configurator
passwords 19
WEP 46, 57
WEP Encryption 47
wireless LAN 41
authentication 55, 56
BSS 58
example 58
channel 42
encryption 57
example 42
fragmentation threshold 55
limitations 57
MAC address filter 56
MBSSID 58
preamble 55
RADIUS server 56
RTS/CTS threshold 55
scheduling 54
security 55
SSID 56
activation 49
WEP 57
WPA 57
WPA-PSK 57
WPS 59, 61
example 62
limitations 64
PIN 59
push button 59
wireless network
example 41
WLAN 41
auto-scan channel 45
passphrase 46
scheduling 54
see also wireless.
WEP 46
WPA 57
WPA-PSK 57
WPS 59, 61
example 62
limitations 64
PIN 59
example 61
push button 59