LTE7410

LTE Outdoor CPE

Version 2.60
Edition 1, 1/2016

User's Guide

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

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Screenshots and graphics in this book may differ slightly from your product due to differences in your product firmware or your computer operating system. 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 get up and running right away.

Contents Overview

Table of Contents

PART I
User's Guide

1 Introduction

1.1 Overview

The LTE Device is an outdoors LTE (Long Term Evolution) router that also supports a Gigabit Ethernet connection. Its Voice over IP (VoIP) communication capabilities let you use a traditional analog telephone to make Internet calls. The LTE Device also includes a robust firewall that uses Stateful Packet Inspection (SPI) technology and protects against Denial of Service (DoS) attacks.

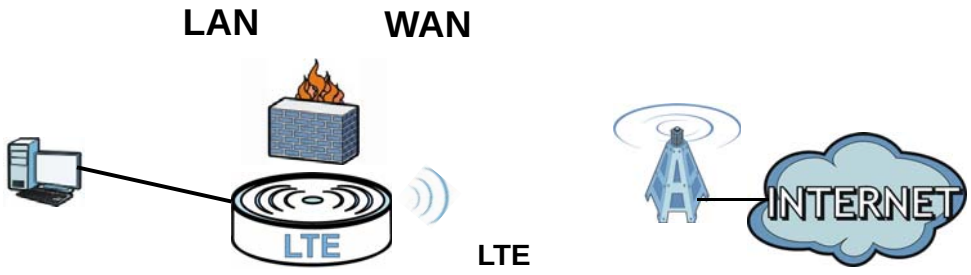
1.2 Applications for the LTE Device

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

1.2.1 Internet Access

Your LTE Device provides shared Internet access by connecting to an LTE network. Computers can connect to the LTE Device's PoE injector.

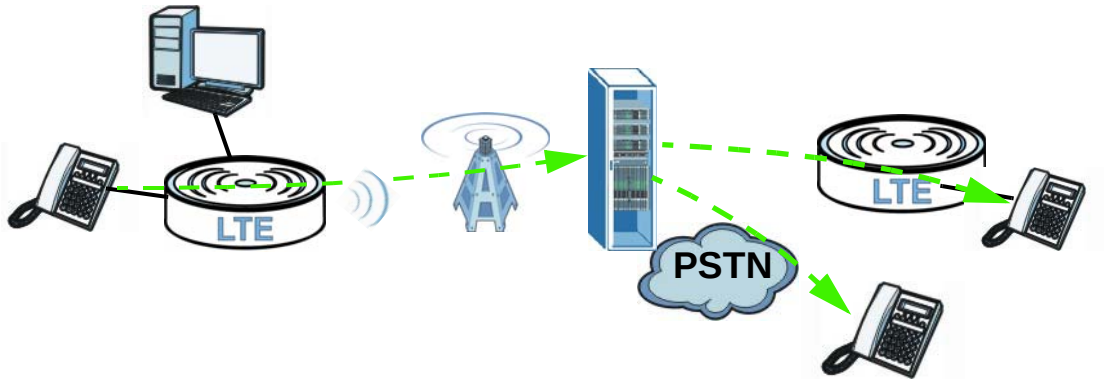
Figure 1 LTE Device's Internet Access Application



1.2.2 VoIP Features

Use SIP (Session Initiation Protocol) accounts with the LTE Device to make and receive VoIP telephone calls.

Figure 2 LTE Device's VoIP Application



The LTE Device sends your call to a VoIP service provider's SIP server which forwards your calls towards the destination VoIP or PSTN phones.

1.3 Ways to Manage the LTE Device

Use the following method to manage the LTE Device.

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

1.4 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. Keep in mind that backing up a configuration file will not back up passwords used to set up VoIP. Write down any information your ISP provides you.

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 8.0 and later versions, Chrome 40 and later versions, Mozilla Firefox 36 and later versions, or Safari 7.0 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).

2.1.1 Accessing the Web Configurator

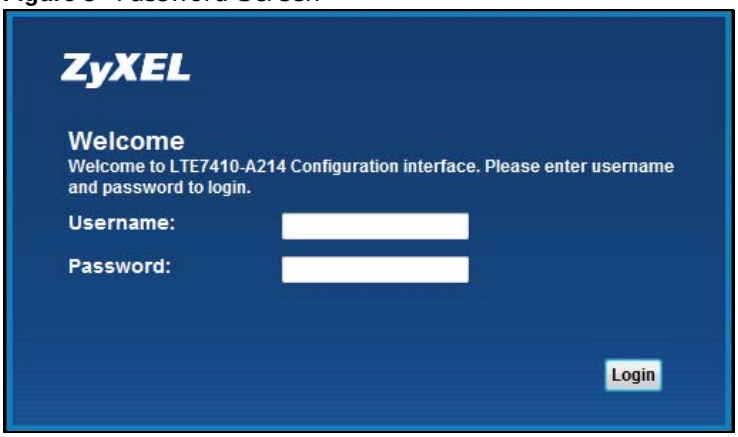
1 Make sure your LTE Device hardware is properly connected (refer to the Quick Start Guide).

2 Launch your web browser.

3 Type "https://192.168.1.1" as the URL. For security reason, the default setting of the URL uses the secure version of Hyper Text Transfer Protocol (HTTP).

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**.

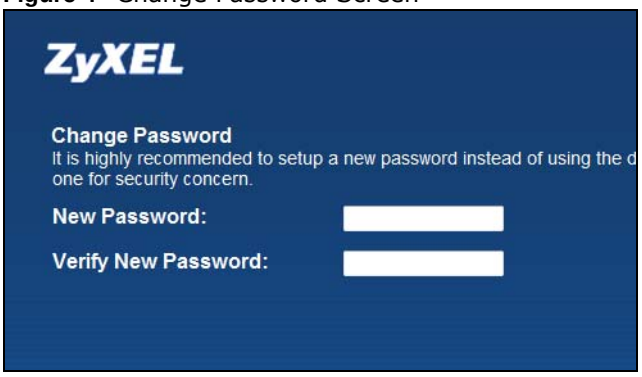
Figure 3 Password Screen



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**.

Figure 4 Change Password Screen



6 The **Connection Status** screen appears.

Figure 5 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.

Figure 6 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 **Logout** icons in the upper right corner.

Click the **Logout** 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.

Click **LAN Device** on the **System Info** screen (**a** in Figure 6 on page 16) to display the **Connection Status** screen. See Chapter 3 on page 20 for more information on the **System Info** and **Connection Status** screens.

PART II
Technical Reference

3

Connection Status and System Info

3.1 Overview

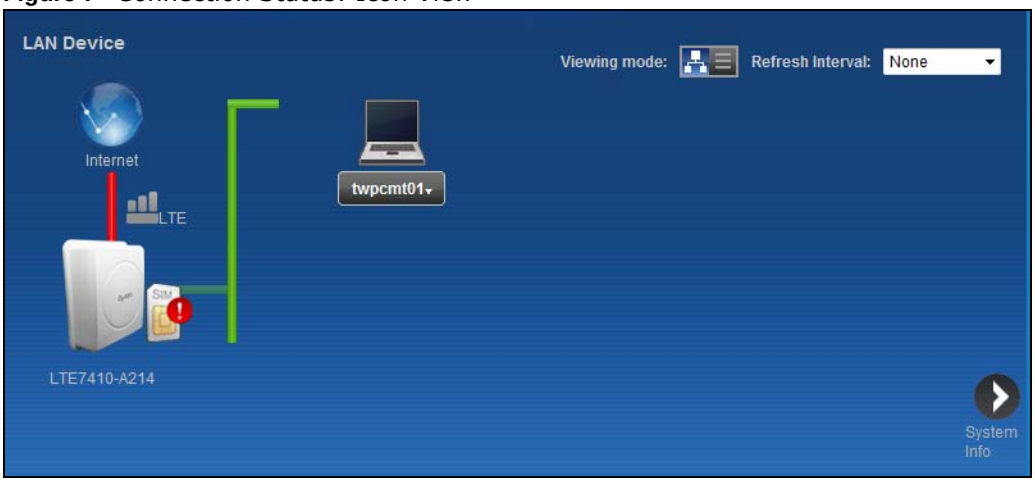
After you log into the web configurator, the **Connection Status** screen appears. This shows the network connection status of the LTE Device and clients connected to it.

Use the **System Info** screen to look at the current status of the device, system resources, interfaces (LAN and WAN), and SIP accounts. You can also register and unregister SIP accounts.

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. You can configure how often you want the LTE Device to update this screen in **Refresh Interval**.

Figure 7 Connection Status: Icon View



To view the connected LAN devices in a list, click **List View** in the **Viewing mode** selection box.

Figure 8 Connection Status: List View

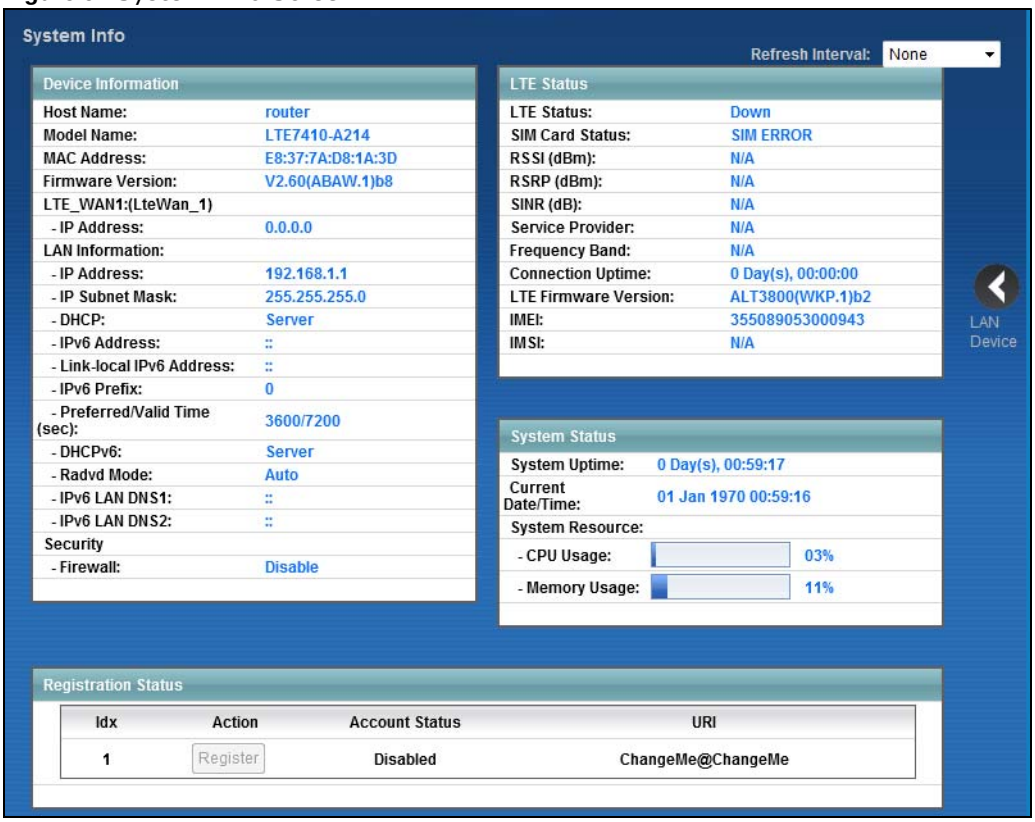
In **Icon View**, if you want to view information about a client, click the client's name and **Info**.

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 9 System Info Screen



Each field is described in the following table.

Table 1 System Info Screen

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the LTE Device to update this screen from the drop-down list box.
Device Information	
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.
Firmware 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.
LTE_WAN1 ~ LTE_WAN3 - IP Address	This field displays the current LTE IP address of the LTE Device in the WAN.

Table 1 System Info Screen (continued)

LABEL	DESCRIPTION
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	This field displays what DHCP services the LTE Device is providing to the LAN: **Server** - The LTE Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. **None** - The LTE Device is not providing any DHCP services to the LAN.
IPv6 Address	This is the current IPv6 address of the LTE Device in the LAN.
Link-local IPv6 Address	This is the current LAN IPv6 link-local address of the LTE Device.
IPv6 Prefix	This is the current IPv6 prefix length in the LAN.
Preferred/Valid Time (sec)	This is the preferred lifetime and valid lifetime in the LAN.
DHCPv6	This field displays what DHCPv6 services the LTE Device is providing to the LAN: **Server** - The Device is a DHCPv6 server in the LAN. It assigns IP addresses to other computers in the LAN. **None** - The LTE Device is not providing any DHCPv6 services to the LAN.
Radvd Mode	This shows the status of RADVD (Router Advertisement Daemon).
IPv6 LAN DNS1/ DNS2	This is the first/second DNS server IPv6 address the LTE Device passes to the DHCP clients.
Security	
Firewall	This shows whether or not the firewall is enabled (on).
LTE Status	
LTE Status	This displays **UP** for an LTE connection. **Down** displays when the LTE Device does not have a cellular connection.
SIM Card Status	This displays the SIM card status: **PIN DISABLE** - the SIM card has no PIN code security. **PIN REQUIRED** - the SIM card has PIN code security, but you did not enter the PIN code yet. **PIN VERIFIED** - the SIM card has PIN code security, and you entered the correct PIN code. **PIN locked** - you entered an incorrect PIN code too many times, so the SIM card has been locked; call the ISP for a PUK (Pin Unlock Key) to unlock the SIM card. **SIM ERROR** - the LTE Device does not detect that there is a SIM card inserted.
RSSI (dBm)	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.
RSRP (dBm)	This displays the LTE RSRP (Reference Signal Received Power).
SINR (dB)	This displays the Signal to Interference plus Noise Ratio in dB.
Service Provider	This displays the service provider's name of the connected LTE network.
Frequency Band	This displays the frequency band of the cellular connection. **LTE** displays for an LTE connection.
Connection Uptime	This displays how long the LTE connection has been available since it was last established successfully.
LTE Firmware Version	This displays the version of the firmware on the LTE module.

Table 1 System Info Screen (continued)

LABEL	DESCRIPTION
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 installed SIM card. An IMSI is a unique ID used to identify a mobile subscriber in a mobile network.
System Status	
System UpTime	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**).
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 22 on page 130, or turn off the device (unplug the power) for a few seconds.
Registration Status	
Idx	This is the index number of each SIP account in the LTE Device.
Action	This field displays the current registration status of the SIP account. You have to register SIP accounts with a SIP server to use VoIP. If the SIP account is already registered with the SIP server, • Click **Unregister** to delete the SIP account's registration in the SIP server. This does not cancel your SIP account, but it deletes the mapping between your SIP identity and your IP address or domain name. • The second field displays **Registered**. If the SIP account is not registered with the SIP server, • Click **Register** to have the LTE Device attempt to register the SIP account with the SIP server. • The second field displays the reason the account is not registered. **Inactive** - The SIP account is not active. You can activate it in **VoIP > SIP > SIP Settings**. **Register Fail** - The last time the LTE Device tried to register the SIP account with the SIP server, the attempt failed. The LTE Device automatically tries to register the SIP account when you turn on the LTE Device or when you activate it.
Account Status	This shows **Active** when the SIP account has been registered and ready for use or **In-Active** when the SIP account is not yet registered.
URI	This field displays the account number and service domain of the SIP account. You can change these in **VoIP > SIP > SIP Settings**.

4

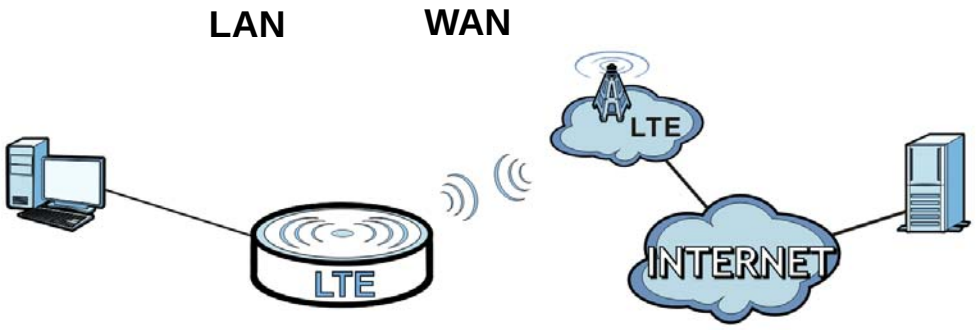
Broadband

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.

Figure 10 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 25).
- Use the **SIM** screen to enter the PIN of your SIM card (Section 4.3 on page 27).

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. The ISP dynamically assigns it each time the LTE Device tries to access the Internet.

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

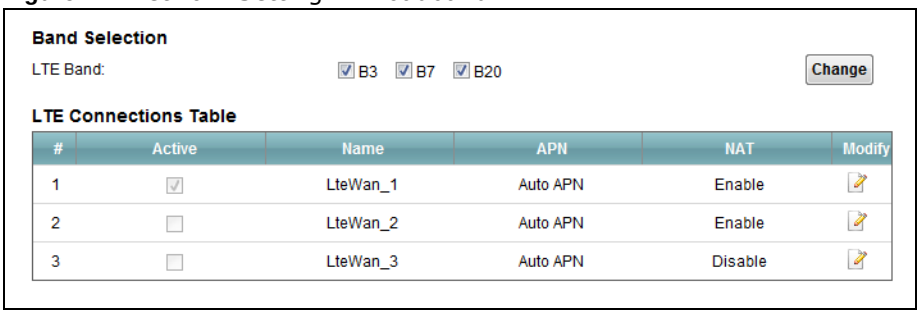
You may need to know your Internet access settings such as LTE APN, WAN IP address and SIM card's PIN code if the **INTERNET** light on your LTE Device is off. Get this information from your service provider.

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 manage WAN interfaces.

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

Figure 11 Network Setting > Broadband



The following table describes the fields in this screen.

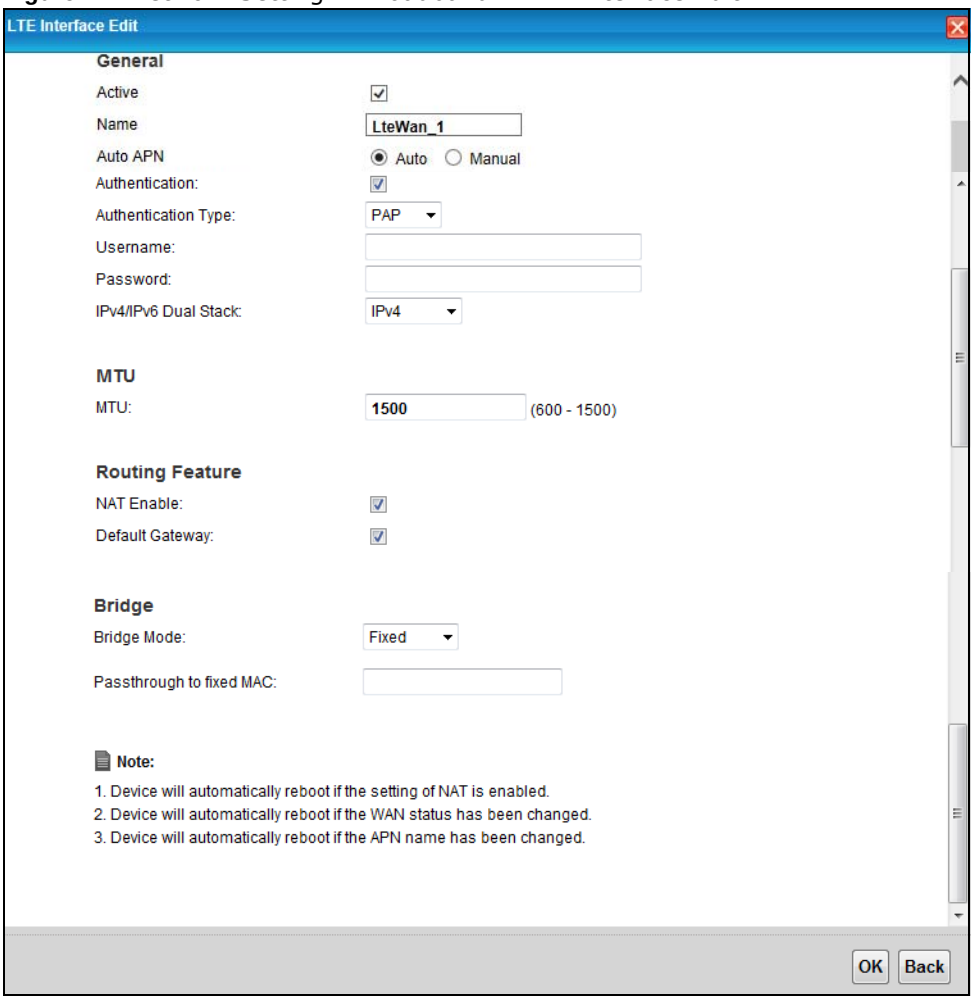
Table 2 Network Setting > Broadband

LABEL	DESCRIPTION
Band Selection	
LTE Band	Select the LTE bands to use for the LTE Device's WAN connection.
LTE Connections Table	
#	This is the index number of the connection.
Active	This shows whether the LTE connection is activated.
Name	This is the service name of the connection.
APN	This field displays the name of the LTE network to which the LTE Device connects.
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.

4.2.1 Edit LTE Connection

In **Network Setting > Broadband**, click the **Edit** icon next to an LTE connection to display the following screen. Use this screen to configure an LTE WAN connection.

Figure 12 Network Setting > Broadband > LTE Interface Edit



The following table describes the fields in this screen.

Table 3 Network Setting > Broadband > LTE Interface Edit

LABEL	DESCRIPTION
General	
Active	Select this to have the LTE Device use the LTE connection.
Name	Specify the name for this WAN interface.
Auto APN	Select **Auto** to have the LTE Device configure the APN (Access Point Name) of an LTE network automatically. Otherwise, select **Manual** and enter the APN manually in the field below.
Authentication	Select this if your LTE service provider requires you to use a user name and password for the LTE connection.

Table 3 Network Setting > Broadband > LTE Interface Edit (continued)

LABEL	DESCRIPTION
Authentication Type	When you select **Authentication**, specify the type of authentication the LTE Device accepts for the LTE connection. The Device supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP provides more security than PAP; however, PAP has higher availability on more platforms.
Username	Enter the user name provided by your LTE service provider.
Password	Enter the password provided by your LTE service provider.
IPv4/IPv6 Dual Stack	Select **IPv4** if you want the LTE Device to run IPv4 only. Select I**Pv6 / IPv4** to allow the LTE Device to run IPv4 and IPv6 at the same time. Select **IPv6** if you want the LTE Device to run IPv6 only.
MTU	
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.
Routing Feature	
NAT Enable	Select this to activate NAT on this WAN interface.
Default Gateway	Select this option to have the LTE Device use the WAN interface of this connection as the system default gateway.
Bridge Mode	Bridge mode allows a LAN computer on the local network of the LTE Device to have access to web services using the public IP address. When bridge mode is configured, all traffic is forwarded to the computer and will not go through NAT. Select the **Bridge Mode** for this LTE connection. Select **None** to disable this feature. Select **Dynamic** to allow the first connected LAN computer to have access to web services using the public IP address. Select **Fixed** to set the bridge mode to pass traffic through to a fixed MAC address. This allows the LAN computer with the MAC address specified in the **Passthrough to fixed MAC** field to have access to web services using the public IP address.
OK	Click this to save your changes.
Back	Click this to exit this screen without saving.

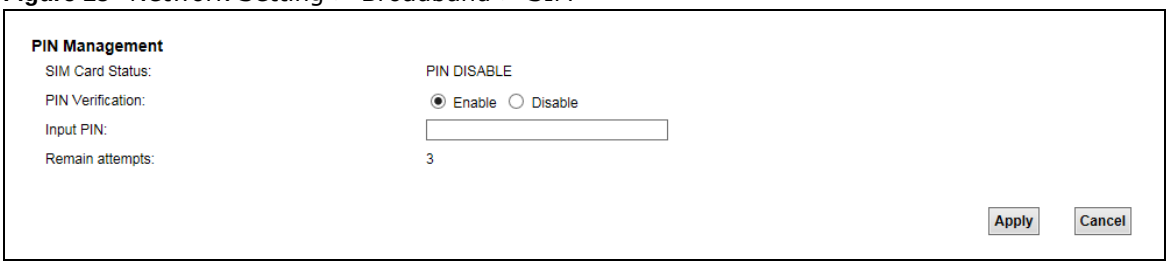
4.3 SIM Screen

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

Entering the wrong PIN code 3 times locks the SIM card after which you need a PUK from the service provider to unlock it.

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

Figure 13 Network Setting > Broadband > SIM



The following table describes the fields in this screen.

Table 4 Network Setting > Broadband > SIM

LABEL	DESCRIPTION
SIM card status	This displays the SIM card status: **PIN DISABLE** - the SIM card has no PIN code security. **PIN REQUIRED** - the SIM card has PIN code security, but you did not enter the PIN code yet. **PIN VERIFIED** - the SIM card has PIN code security, and you entered the correct PIN code. **PIN locked** - you entered an incorrect PIN code too many times, so the SIM card has been locked; call the ISP for a PUK (Pin Unlock Key) to unlock the SIM card. **SIM ERROR** - the LTE Device does not detect that there is a SIM card inserted.
PIN verification	A PIN (Personal Identification Number) code is a key to a 4G card. Without the PIN code, you cannot use the 4G card. Select **Enable** if the 4G service provider requires you to enter a PIN to use the SIM card. Select **Disable** if the 4G service provider lets you use the SIM without inputting a PIN.
Input PIN	If you enabled PIN verification, enter the 4-digit PIN code (0000 for example) provided by your ISP. If you enter the PIN code incorrectly too many times, the ISP may block your SIM card and not ley you use the account to access the Internet.
Remain attempts	This is how many more times you can try to enter the PIN code before the ISP blocks your SIM card.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to return to the previous screen without saving.

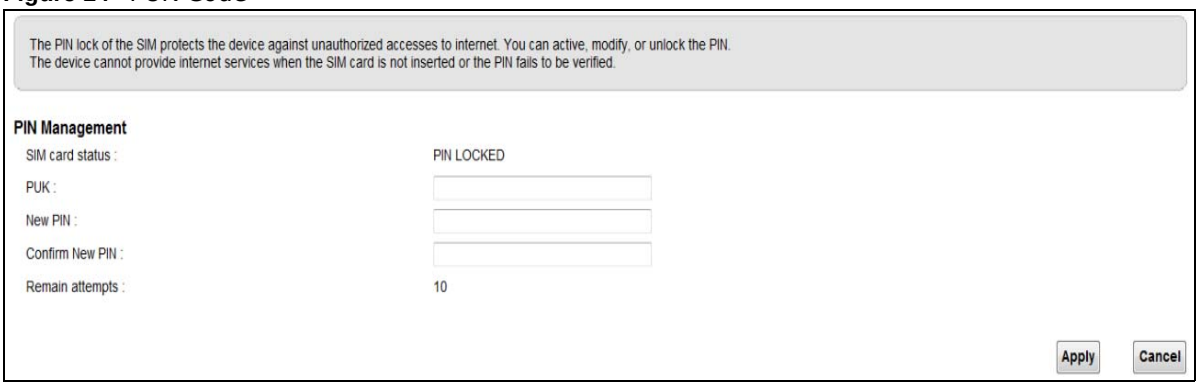
4.3.1 PUK Code Screen

If the SIM card is locked, use this screen to enter the PUK (Pin Unlock Key) code.

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

You will need a new SIM card if you enter the wrong PUK code too many times.

Figure 14 PUK Code



The following table describes the fields in this screen.

Table 5 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.
PUK remaining authentication times	This shows how many more times you can try to enter the PUK code before permanently damaging 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.

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.

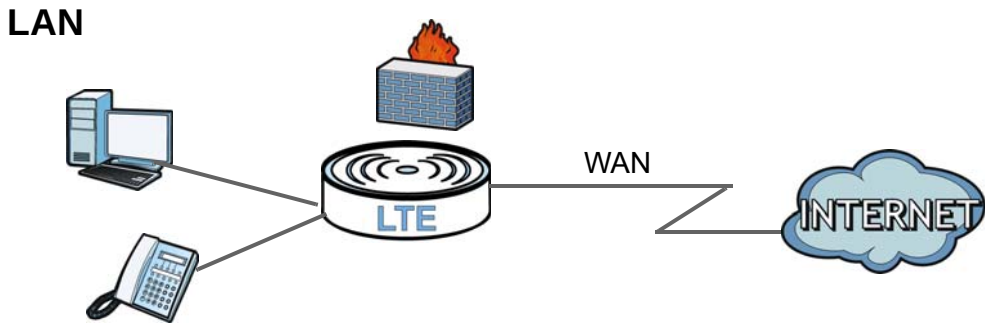
5

Home Networking

5.1 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.



5.1.1 What You Can Do in this Chapter

- Use the **LAN Setup** screen to set the LAN IP address, subnet mask, and DHCP settings (Section 5.2 on page 32).
- Use the **IPv6 LAN Setup** screen to configure the IPv6 settings on your Device's LAN interface (Section 5.3 on page 33).
- Use the **Static DHCP** screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses (Section 5.4 on page 37).
- Use the **UPnP** screen to enable UPnP (Section 5.5 on page 39).

5.1.2 What You Need To Know

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

5.1.2.1 About LAN

IP Address

An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication.

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.

5.1.2.2 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.

UPnP and ZyXEL

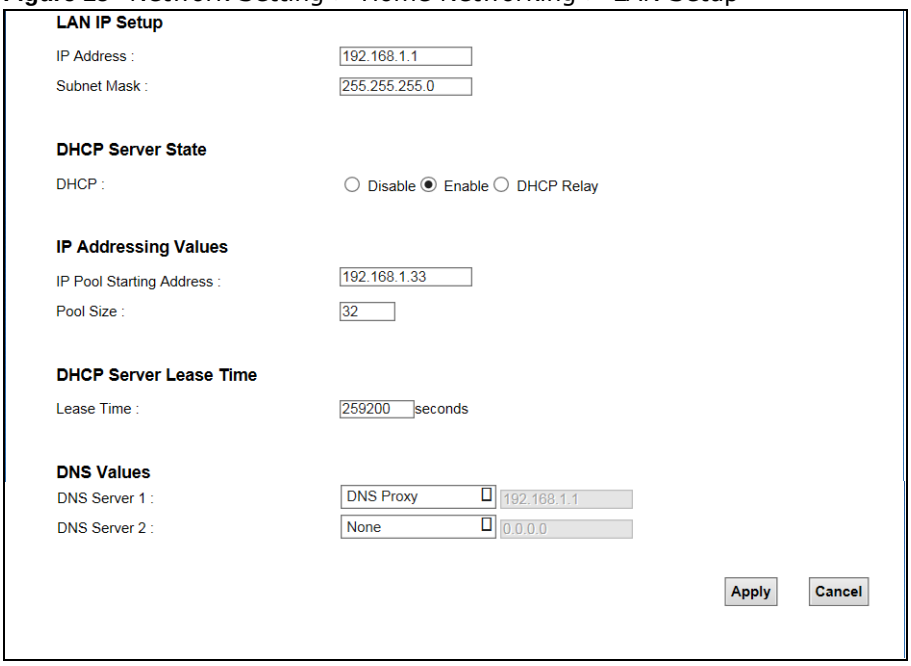
ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports Internet Gateway Device (IGD) 1.0.

See Section 5.7 on page 41 for examples of installing and using UPnP.

5.2 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 15 Network Setting > Home Networking > LAN Setup



The following table describes the fields in this screen.

Table 6 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).
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. If you select **Disable**, you need to manually configure the IP addresses of the computers and other devices on your LAN. If you select **DHCP Relay**, the LTE Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the **Remote DHCP Server** field in this case. When DHCP is used, the following fields need to be set:
IP Addressing Values	

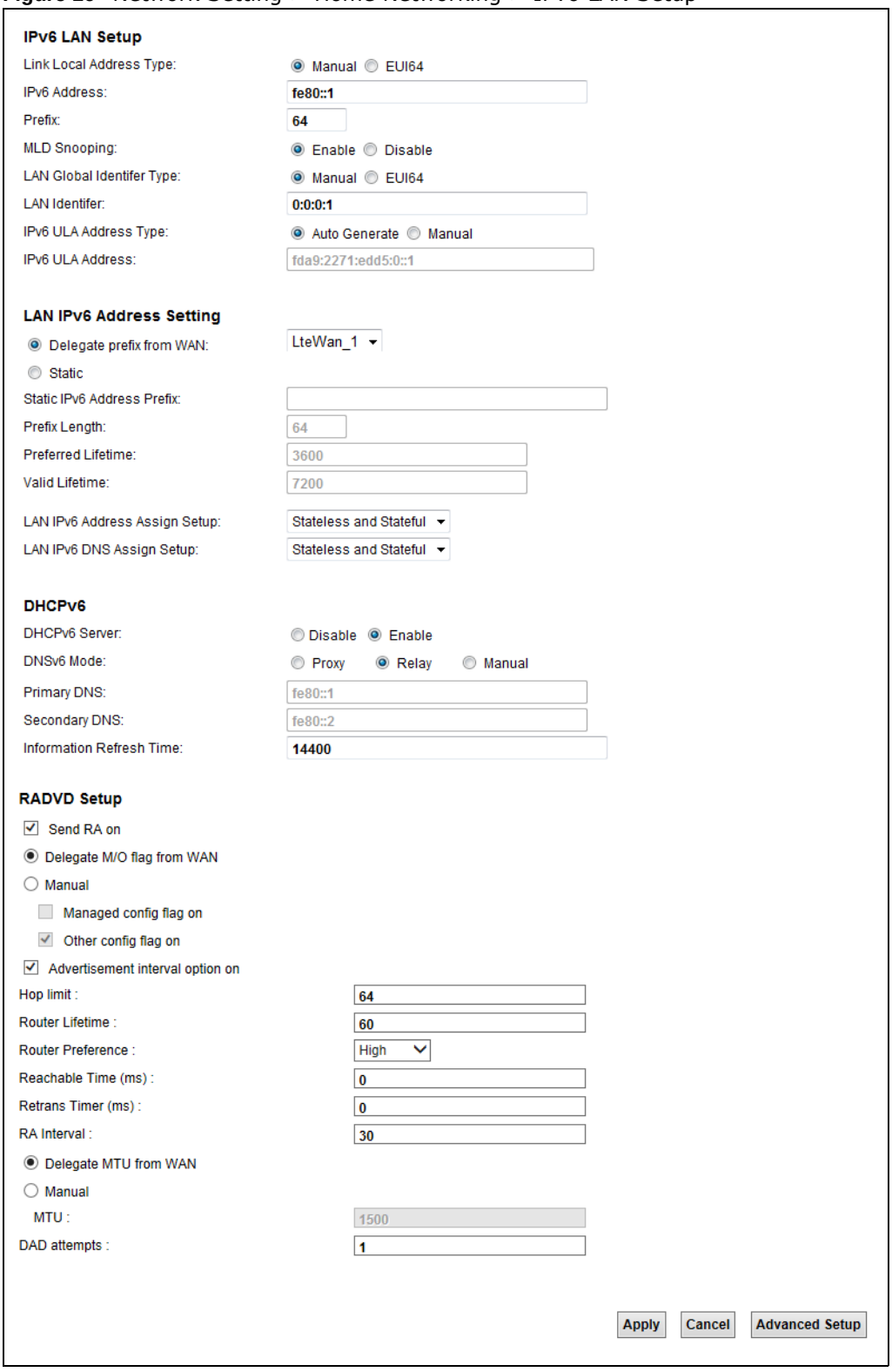
Table 6 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
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.
DHCP Server Lease Time	
Lease Time	DHCP server leases an address to a new device for a period of time, called the DHCP lease time. When the lease expires, the DHCP server might assign the IP address to a different device.
DNS Values	
DNS Server 1-2	The LTE Device supports DNS proxy by default. The LTE Device sends out its own LAN IP address to the DHCP clients as the first DNS server address. DHCP clients use this first DNS server to send domain-name queries to the LTE Device. The LTE Device sends a response directly if it has a record of the domain-name to IP address mapping. If it does not, the LTE Device queries an outside DNS server and relays the response to the DHCP client. Select **Obtained From ISP** if your ISP dynamically assigns DNS server information (and the LTE Device's WAN IP address). Select **UserDefined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. Select **DNS Proxy** to have the DHCP clients use the LTE Device's own LAN IP address. The LTE Device works as a DNS relay. Select **None** to not configure extra DNS servers.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

5.3 The IPv6 LAN Setup Screen

Use this screen to configure the IPv6 settings for your LTE Device's LAN interface.

Figure 16 Network Setting > Home Networking > IPv6 LAN Setup



The following table describes the labels in this screen.

Table 7 Network Setting > Home Networking > IPv6 LAN Setup

LABEL	DESCRIPTION
IPv6 LAN Setup	
Link Local Address Type	Select **Manual** to manually enter a link local address. Select **EUI64** to use the EUI-64 format to generate a link local address from the Ethernet MAC address.
IPv6 Address	If you selected **Manual** in the **Link Local Address Type** field, enter the LAN IPv6 address you want to assign to your LTE Device in hexadecimal notation, for example, fe80::1 (factory default).
Prefix	Enter the address prefix to specify how many most significant bits in an IPv6 address compose the network address.
MLD Snooping	Multicast Listener Discovery (MLD) allows an IPv6 switch or router to discover the presence of MLD hosts who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network. Select **Enable** to activate MLD snooping on the LTE Device. This allows the LTE Device to check MLD packets passing through it and learn the multicast group membership. It helps reduce multicast traffic.
LAN Global Identifier Type	Select **Manual** to manually enter a LAN identifier as the interface ID to identify the LAN interface. The LAN Identifier is appended to the IPv6 address prefix to create the routable global IPv6 address. Select **EUI64** to use the EUI-64 format to generate an interface ID from the Ethernet MAC address.
LAN Identifier	If you selected **Manual**, enter the LAN Identifier in this field. The LAN identifier should be unique and 64 bits in hexadecimal form. Every 16 bit block should be separated by a colon as in XXXX:XXXX:XXXX:XXXX where X is a hexadecimal character. Blocks of zeros can be represented with double colons as in XXXX:XXXX::XXXX.
IPv6 ULA Address Type	A unique local address (ULA) is a unique IPv6 address for use in private networks but not routable in the global IPv6 Internet. Select **Auto Generate** to have the Device automatically generate a globally unique address for the LAN IPv6 address. Select **Manual** to enter a static IPv6 ULA address. The address format is like fdxx:xxxx:xxxx:xxxx::/64.
IPv6 ULA Address	If **Manual** is selected in the **IPv6 ULA Address Type** field, enter the IPv6 address prefix that the LTE Device uses for the LAN IPv6 address.
LAN IPv6 Address Setting	
Delegate prefix from WAN	Select this option to automatically obtain an IPv6 network prefix from the service provider or an uplink router.
Static	Select this option to configure a fixed IPv6 address for the LTE Device's LAN IPv6 address.
Static IPv6 Address Prefix	If you select static IPv6 address, enter the IPv6 address prefix that the LTE Device uses for the LAN IPv6 address.
Prefix length	If you select static IPv6 address, enter the IPv6 prefix length that the LTE Device uses to generate the LAN IPv6 address. An IPv6 prefix length specifies how many most significant bits (starting from the left) in the address compose the network address. This field displays the bit number of the IPv6 subnet mask.
Preferred Lifetime	Enter the preferred lifetime for the prefix.
Valid Lifetime	Enter the valid lifetime for the prefix.

Table 7 Network Setting > Home Networking > IPv6 LAN Setup (continued)

LABEL	DESCRIPTION
LAN IPv6 Address Assign Setup	Select how you want to obtain an IPv6 address: • **Stateless:** The LTE Device uses IPv6 stateless autoconfiguration. RADVD (Router Advertisement Daemon) is enabled to have the LTE Device send IPv6 prefix information in router advertisements periodically and in response to router solicitations. DHCPv6 server is disabled. • **Stateful:** The LTE Device uses IPv6 stateful autoconfiguration. The DHCPv6 server is enabled to have the LTE Device act as a DHCPv6 server and pass IPv6 addresses to DHCPv6 clients. • **Stateless and Stateful:** The LTE Device uses both IPv6 stateless and stateful autoconfiguration. The LAN IPv6 clients can obtain IPv6 addresses either through router advertisements or through DHCPv6.
LAN IPv6 DNS Assign Setup	Select how the LTE Device provide DNS server and domain name information to the clients: • **Stateless:** The LTE Device uses IPv6 stateless autoconfiguration. RADVD (Router Advertisement Daemon) is enabled to have the LTE Device send IPv6 prefix information in router advertisements periodically and in response to router solicitations. DHCPv6 server is disabled. • **Stateful:** The LTE Device uses IPv6 stateful autoconfiguration. The DHCPv6 server is enabled to have the LTE Device act as a DHCPv6 server and pass IPv6 addresses to DHCPv6 clients. • **Stateless and Stateful:** The LTE Device uses both IPv6 stateless and stateful autoconfiguration. The LAN IPv6 clients can obtain IPv6 addresses either through router advertisements or through DHCPv6.
DHCPv6	
DHCPv6 Server	Use this field to **Enable** or **Disable** DHCPv6 server on the LTE Device.
DNSv6 Mode	Select the DNS role (**Proxy** or **Relay**) that you want the LTE Device to act in the IPv6 LAN network. Alternatively, select **Manual** and specify IPv6 addresses of the DNS servers in the fields below.
Primary DNS	This field is available if you choose **Manual** as the DNSv6 mode. Enter the first DNS server IPv6 address the LTE Device passes to the DHCP clients.
Secondary DNS	This field is available if you choose **Manual** as the DNSv6 mode. Enter the second DNS server IPv6 address the LTE Device passes to the DHCP clients.
Information Refresh Time	Enter the number of seconds a DHCPv6 client should wait before refreshing information retrieved from DHCPv6.
Advanced Setup	Click this to open the **IPv6 LAN Setup Advanced Setup** section.
RADVD Setup	
Send RA on	Select this to have the LTE Device send router advertisement messages to the LAN hosts. Router advertisement is a response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters, such as IPv6 prefix and DNS information. Router solicitation is a request from a host to locate a router that can act as the default router and forward packets. Note: The LAN hosts neither generate global IPv6 addresses nor communicate with other networks if you disable this feature.
Delegate M/O flag from WAN	Select this to have the LTE Device obtain the M/O (Managed/Other) flag setting from the service provider or uplink router.
Manual	Select this to specify the M/O flag setting manually.
Managed config flag on	Select this to have the LTE Device indicate to hosts to obtain network settings (such as prefix and DNS settings) through DHCPv6. Clear this to have the LTE Device indicate to hosts that DHCPv6 is not available and they should use the prefix in the router advertisement message.

Table 7 Network Setting > Home Networking > IPv6 LAN Setup (continued)

LABEL	DESCRIPTION
Other config flag on	Select this to have the LTE Device indicate to hosts to obtain DNS information through DHCPv6. Clear this to have the LTE Device indicate to hosts that DNS information is not available in this network.
Advertisement interval option on	Select this to have the Router Advertisement messages the LTE Device sends specify the allowed interval between Router Advertisement messages.
Hop limit	Enter the maximum number of network segments that a packet can cross before reaching the destination. When forwarding an IPv6 packet, IPv6 routers are required to decrease the hop limit by 1 and to discard the IPv6 packet when the Hop Limit is 0. Possible values for this field are 0-255.
Router Lifetime	Enter the time in seconds that hosts should consider the LTE Device to be the default router. Possible values for this field are 0-9000.
Router Preference	Select the router preference (**Low**, **Medium** or **High**) for the LTE Device. The LTE Device sends this preference in the router advertisements to tell hosts what preference they should use for the LTE Device. This helps hosts to choose their default router especially when there are multiple IPv6 routers in the network. Note: Make sure the hosts also support router preference to make this function work.
Reachable Time (ms)	Enter the time in milliseconds that can elapse before a neighbor is detected. Possible values for this field are 0-3600000.
Retrans Timer (ms)	Enter the time in milliseconds between neighbor solicitation packet retransmissions. Possible values for this field are 1000-4294967295.
RA Interval	Enter the time in seconds between router advertisement messages. Possible values for this field are 4-1800.
Delegate MTU from WAN	Select this to have the LTE Device obtain the MTU setting from the service provider or uplink router.
Manual	Select this to specify the MTU manually.
MTU	The Maximum Transmission Unit. Type the maximum size of each IPv6 data packet, in bytes, that can move through this interface. If a larger packet arrives, the LTE Device divides it into smaller fragments.
DAD attempts	Specify the number of DAD (Duplicate Address Detection) attempts before an IPv6 address is assigned to the LTE Device LAN interface. Possible values for this field are 1-7.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.
Advanced Setup	Click this to close the **IPv6 LAN Setup Advanced Setup** section.

5.4 The Static DHCP Screen

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

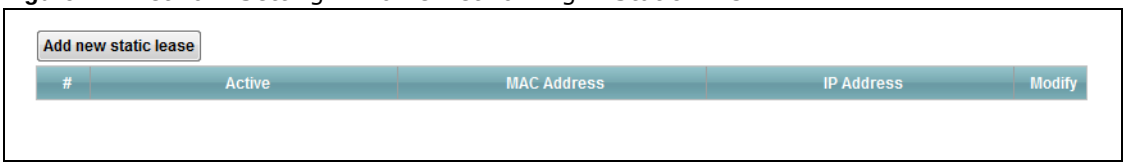
Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

5.4.1 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 17 Network Setting > Home Networking > Static DHCP



The following table describes the labels in this screen.

Table 8 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.
Active	Displays whether the static DHCP entry is on or off.
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). 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.
Modify	Click the **Edit** icon to configure the connection.

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

Figure 18 Static DHCP: Add New Static Lease

The following table describes the labels in this screen.

Table 9 Static DHCP: Add New Static Lease

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.

Table 9 Static DHCP: Add New Static Lease (continued)

LABEL	DESCRIPTION
OK	Click **Apply** to save your changes.
Back	Click **Back** to exit this screen without saving.

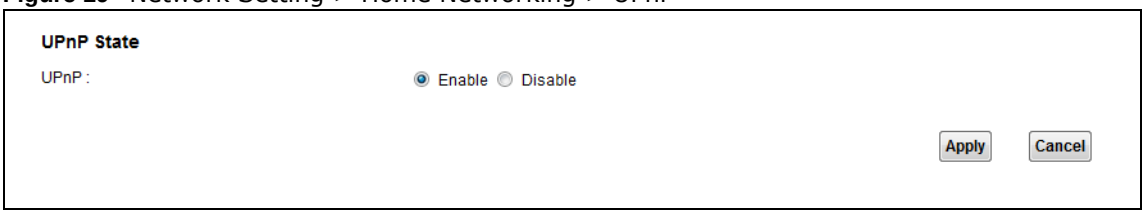
5.5 The UPnP Screen

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

See page 41 for more information on UPnP.

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 19 Network Setting > Home Networking > UPnP



The following table describes the labels in this screen.

Table 10 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.
Cancel	Click this to restore your previously saved settings.

5.6 Technical Reference

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

DHCP Setup

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

IP Pool Setup

The LTE Device is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

LAN TCP/IP

The LTE Device has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

IP Address and Subnet Mask

An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication.

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 and you must enable the Network Address Translation (NAT) feature of the LTE Device. 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. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your LTE Device, 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, for example, only between your two branch offices, 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

If you are part of a large organization, consult your network administrator for the appropriate IP addresses.

Note: 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".

5.7 Installing UPnP in Windows Example

This section shows how to install UPnP in Windows Me and Windows XP.

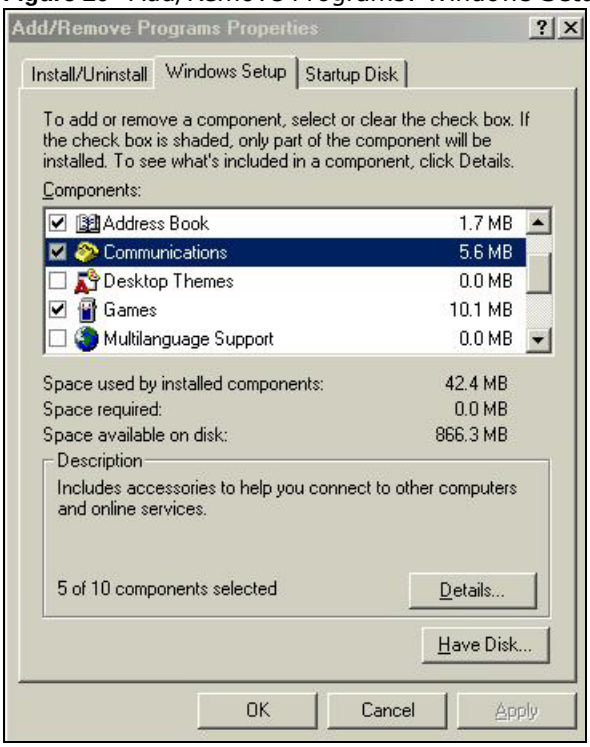
Installing UPnP in Windows Me

Follow the steps below to install the UPnP in Windows Me.

1 Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.

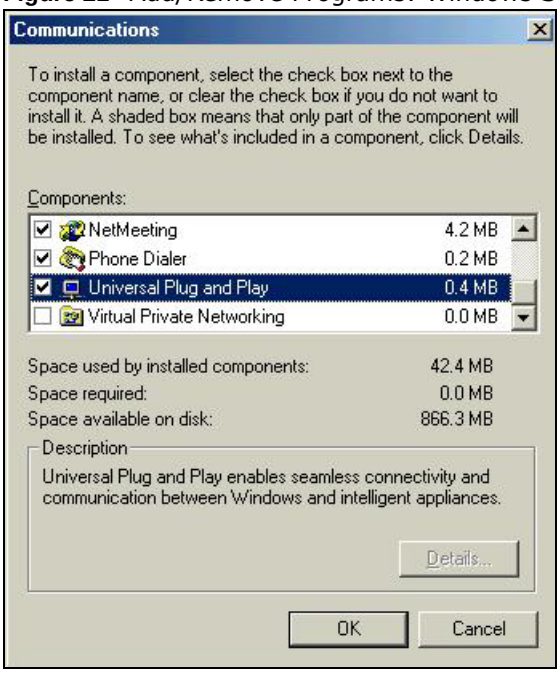
2 Click the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.

Figure 20 Add/Remove Programs: Windows Setup: Communication



3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.

Figure 21 Add/Remove Programs: Windows Setup: Communication: Components



4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.

5 Restart the computer when prompted.

Installing UPnP in Windows XP

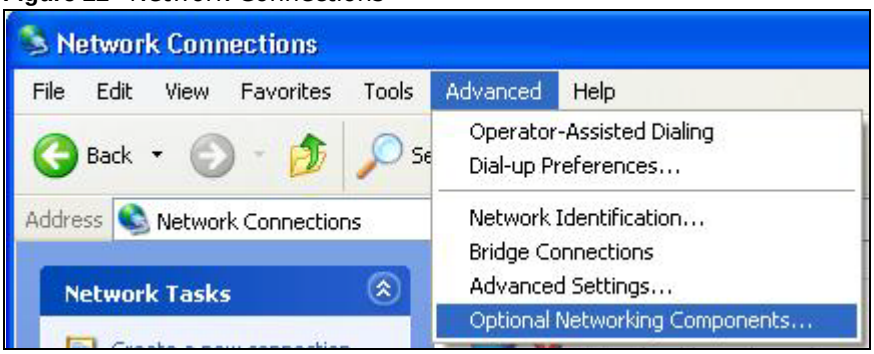
Follow the steps below to install the UPnP in Windows XP.

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

2 Double-click **Network Connections**.

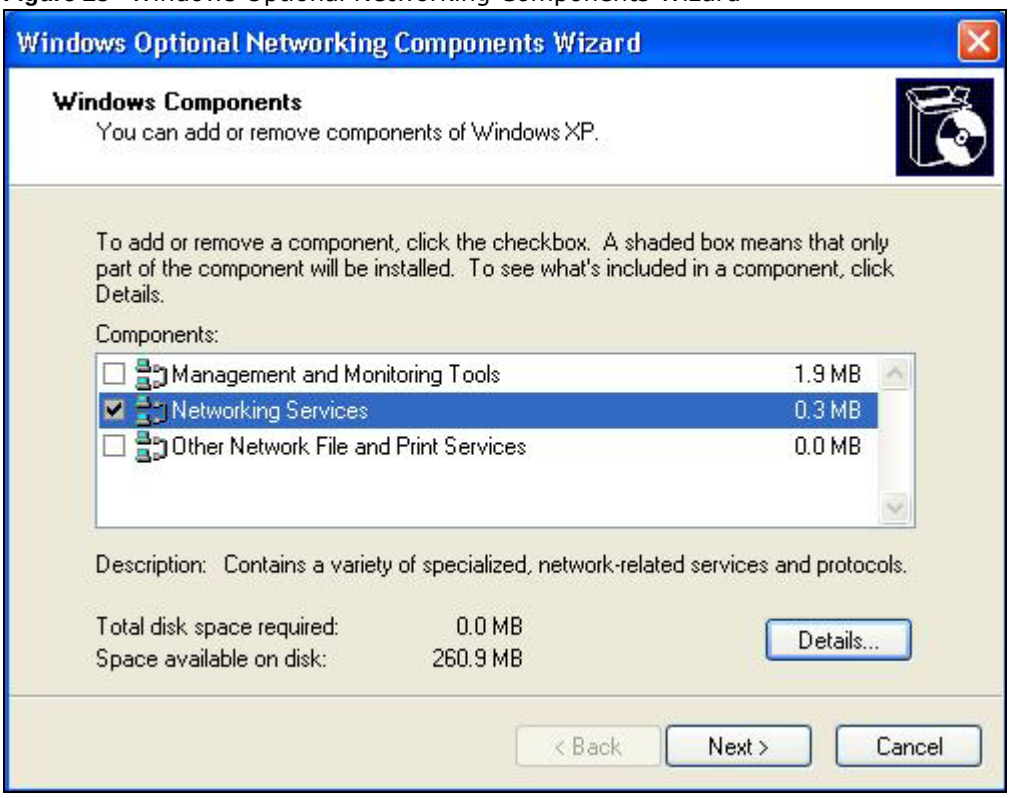
3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ...**.

Figure 22 Network Connections



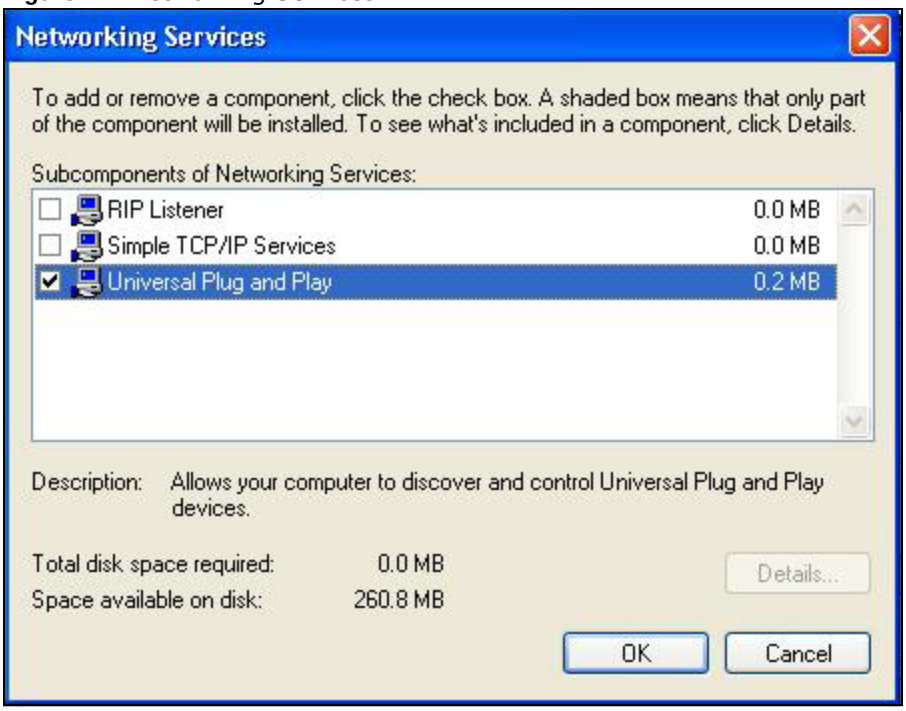
4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

Figure 23 Windows Optional Networking Components Wizard



5 In the **Networking Services** window, select the **Universal Plug and Play** check box.

Figure 24 Networking Services



6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

5.8 Using UPnP in Windows XP Example

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

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

Auto-discover Your UPnP-enabled Network Device

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

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

Figure 25 Network Connections

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

Figure 26 Internet Connection Properties

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

Figure 27 Internet Connection Properties: Advanced Settings

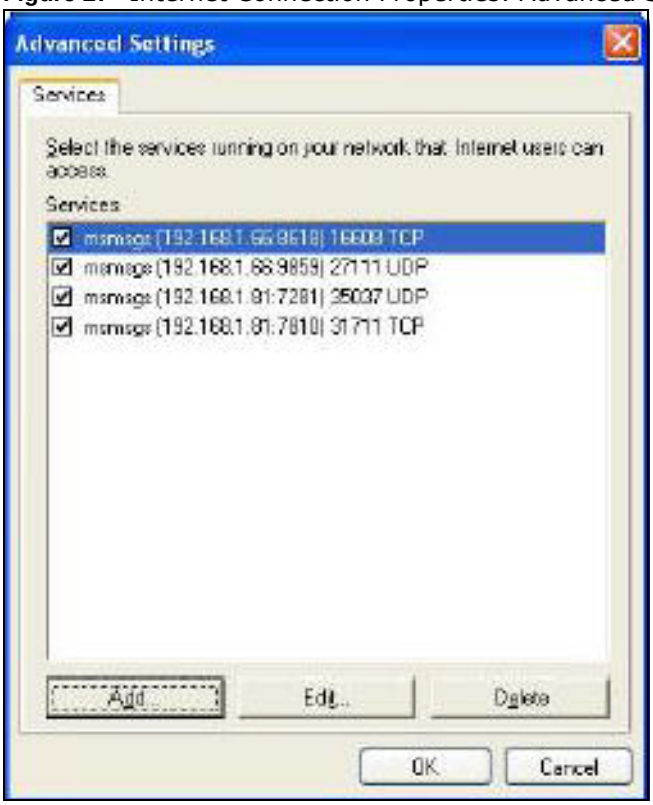
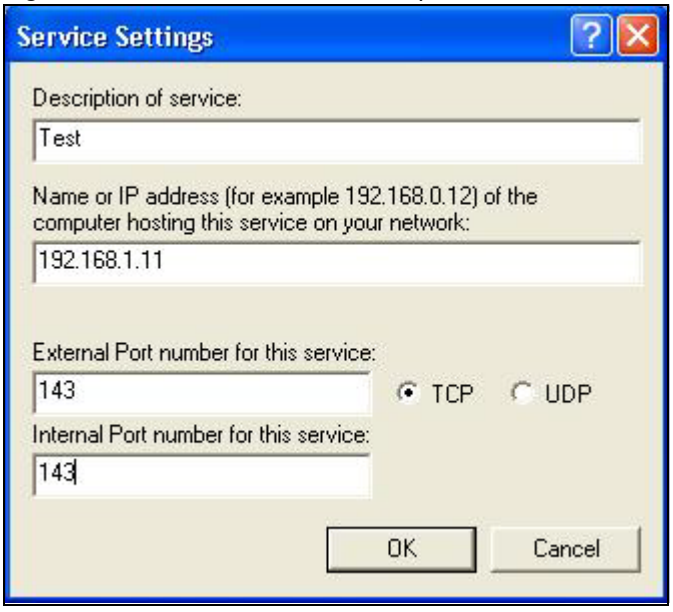


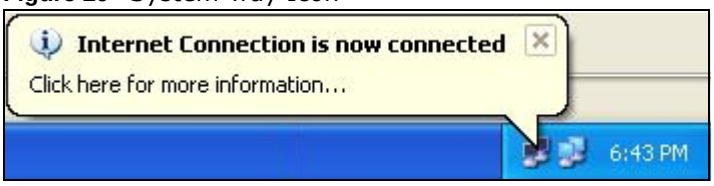
Figure 28 Internet Connection Properties: Advanced Settings: Add



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

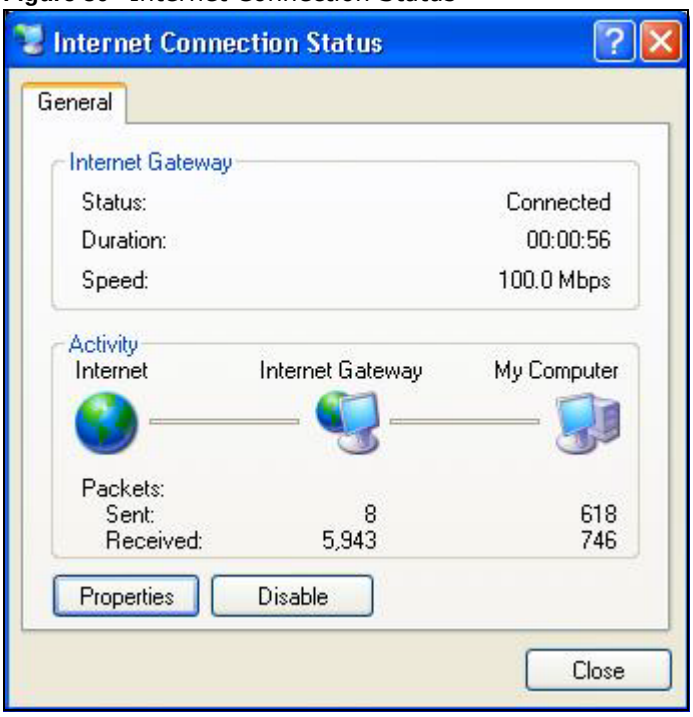
6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

Figure 29 System Tray Icon



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

Figure 30 Internet Connection Status



Web Configurator Easy Access

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

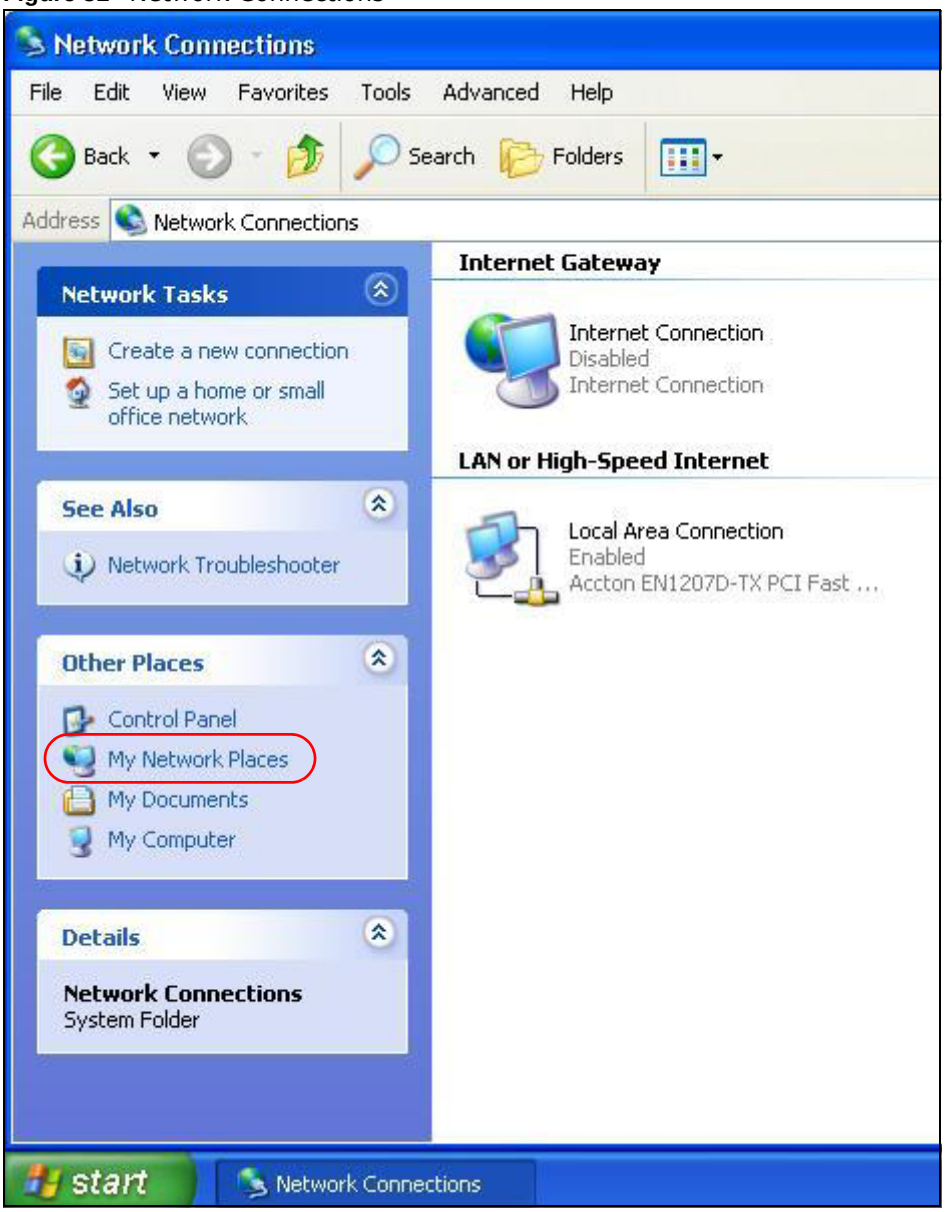
Follow the steps below to access the web configurator.

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

2 Double-click **Network Connections**.

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

Figure 31 Network Connections



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

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

Figure 32 Network Connections: My Network Places

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

Figure 33 Network Connections: My Network Places: Properties: Example

6

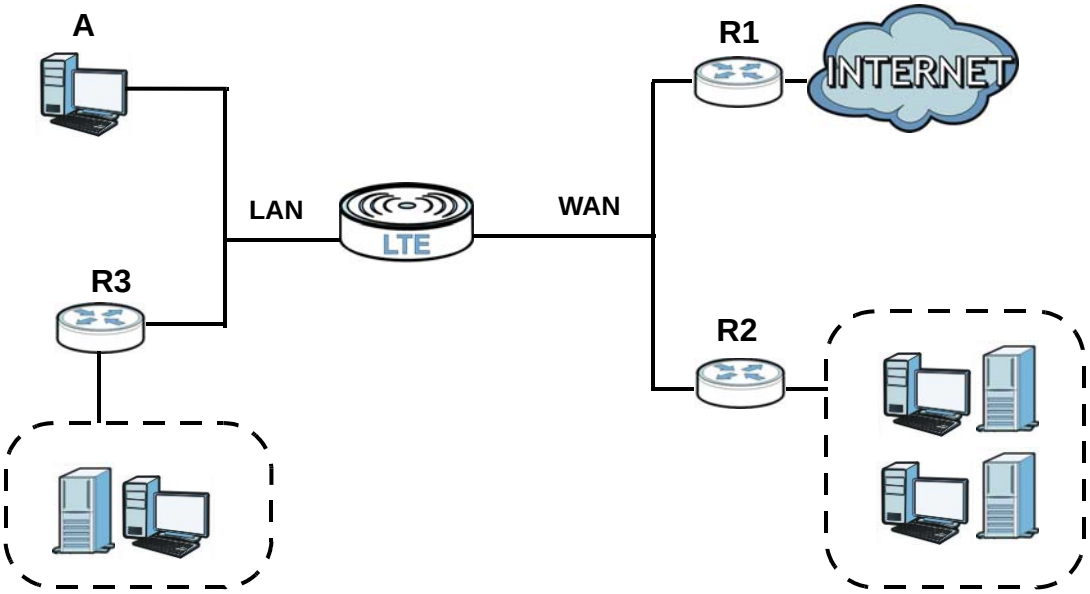
Static Route

6.1 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.

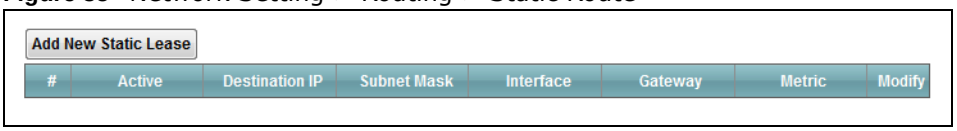
Figure 34 Example of Static Routing Topology



6.2 Configuring Static Route

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

Figure 35 Network Setting > Routing > Static Route



The following table describes the labels in this screen.

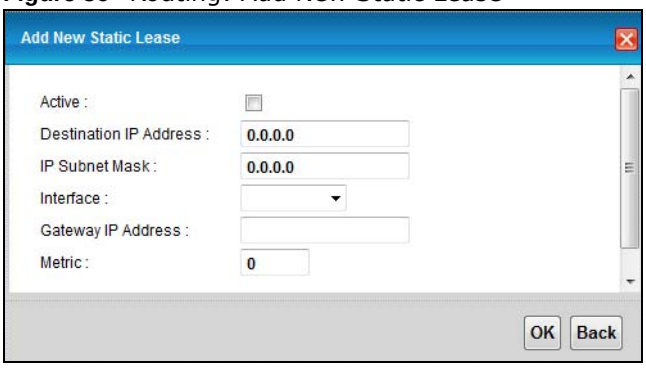
Table 11 Network Setting > Routing > Static Route

LABEL	DESCRIPTION
Add New Static Lease	Click this to set up a new static route on the LTE Device.
#	This is the number of an individual static route.
Active	This specifies whether the static route is on or off.
Destination IP	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Subnet Mask	This parameter specifies the IP network subnet mask of the final destination.
Interface	This is the WAN interface through which the traffic is routed.
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.
Metric	This is the "cost" of transmission for routing purposes.
Modify	Click the **Edit** icon to go to the screen where you can set up a static route on the LTE Device. Click the **Delete** icon to remove a static route from the LTE Device.

6.2.1 Add/Edit Static Lease

Click **Add New Static Lease** in the **Static Routing** screen, the following screen appears. Use this screen to configure the required information for a static route.

Figure 36 Routing: Add New Static Lease



The following table describes the labels in this screen.

Table 12 Routing: Add/Edit

LABEL	DESCRIPTION
Active	Select or clear this field to turn the static route on or off.
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.
Interface	You can decide if you want to forward packets to a gateway IP address or a bound interface. If you want to configure bound interface, choose an interface through which the traffic is sent. You must have the WAN interfaces already configured in the **Broadband** screen.
Gateway IP Address	You can decide if you want to forward packets to a gateway IP address or a bound interface. 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.
Metric	This is the "cost" of transmission for routing purposes.
OK	Click this to save your changes.
Back	Click this to exit this screen without saving.

7

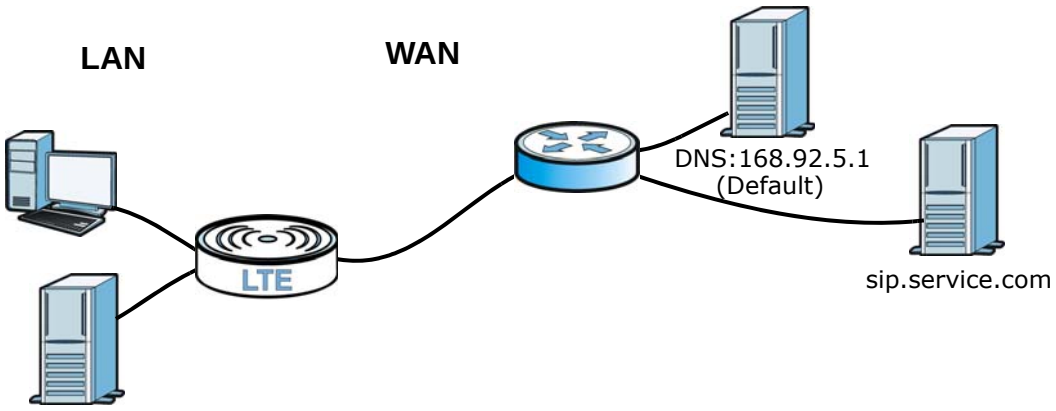
DNS Route

7.1 Overview

DNS (Domain Name System) is for mapping 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 machine before you can access it.

In addition to the system DNS servers, each WAN interface (service) is set to have its own static or dynamic DNS server list. You can configure a DNS static route to forward DNS queries for certain domain names through a specific WAN interface to its DNS servers. The LTE Device uses a system DNS server (in the order you specify in the **Broadband** screen) to resolve domain names that do not match any DNS routing entry. After the LTE Device receives a DNS reply from a DNS server, it creates a new entry for the resolved IP address in the routing table.

Figure 37 Example of DNS Routing Topology



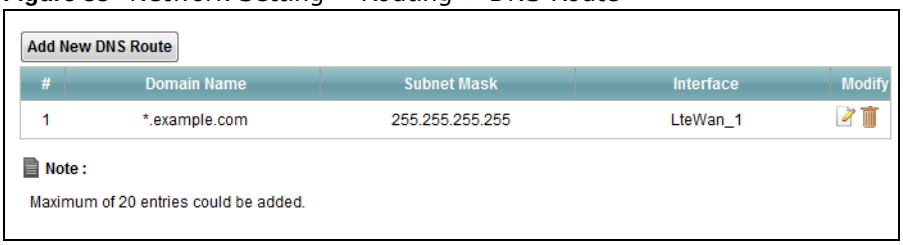
7.1.1 What You Can Do in this Chapter

The **DNS Route** screens let you view and configure DNS routes on the LTE Device (Section 7.2 on page 54).

7.2 The DNS Route Screen

The **DNS Route** screens let you view and configure DNS routes on the LTE Device. Click **Network Setting > Routing > DNS Route** to open the **DNS Route** screen. A DNS route forwards DNS queries for a specific domain name through a specific WAN interface to its DNS server.

Figure 38 Network Setting > Routing > DNS Route



The following table describes the labels in this screen.

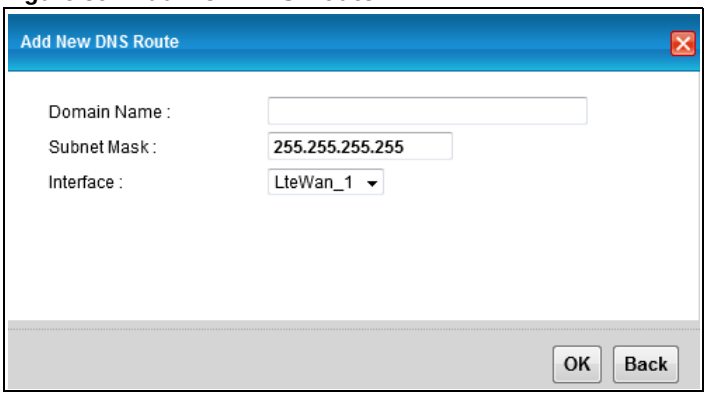
Table 13 Network Setting > Routing > DNS Route

LABEL	DESCRIPTION
Add new DNS route	Click this to create a new entry.
#	This is the number of an individual DNS route.
Domain Name	This is the domain name to which the DNS route applies.
Subnet Mask	This parameter specifies the IP network subnet mask.
Interface	This is the WAN interface through which the matched DNS request is routed.
Modify	Click the **Edit** icon to configure a DNS route on the LTE Device. Click the **Delete** icon to remove a DNS route from the LTE Device.

7.2.1 Add/Edit DNS Route

Click **Add new DNS route** in the **DNS Route** screen, use this screen to configure the required information for a DNS route.

Figure 39 Add New DNS Route



The following table describes the labels in this screen.

Table 14 DNS Route: Add/Edit

LABEL	DESCRIPTION
Domain Name	Enter the domain name you want to resolve. You can use the wildcard character, an "*" (asterisk) as the left most part of a domain name, such as *.example.com. The LTE Device forwards DNS queries for any domain name ending in example.com to the WAN interface specified in this route.
Subnet Mask	Type the subnet mask of the network for which to use the DNS route in dotted decimal notation, for example 255.255.255.255.
Interface	Select a WAN interface through which the matched DNS query is sent. You must have the WAN interface(s) already configured in the **Broadband** screen.
OK	Click this to save your changes.
Back	Click this to exit this screen without saving.

8

Network Address Translation (NAT)

8.1 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.

8.1.1 What You Can Do in this Chapter

- Use the **General** screen to limit the number of concurrent NAT sessions each client can use (Section 8.2 on page 57).
- Use the **Port Forwarding** screen to configure forward incoming service requests to the servers on your local network (Section 8.3 on page 57).
- Use the **DMZ** screen to configure a default server (Section 8.4 on page 60).
- Use the **ALG** screen to enable or disable the SIP ALG (Section 8.5 on page 61).

8.1.2 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

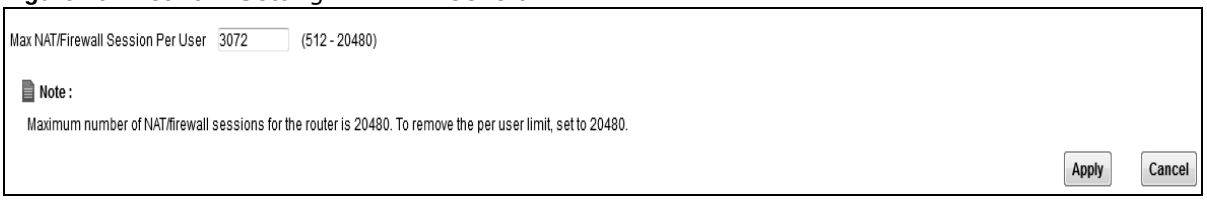
See Section 8.6 on page 61 for advanced technical information on NAT.

8.2 The General Screen

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

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

Figure 40 Network Setting > NAT > General



The following table describes the fields in this screen.

Table 15 Network Setting > NAT > General

LABEL	DESCRIPTION
Max NAT/ Firewall Session Per User	Use this field to set a common limit to the number of concurrent NAT sessions each client computer can have. 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.

8.3 The Port Forwarding Screen

Use the **Port Forwarding** screen to forward incoming service requests to the servers on your local network.

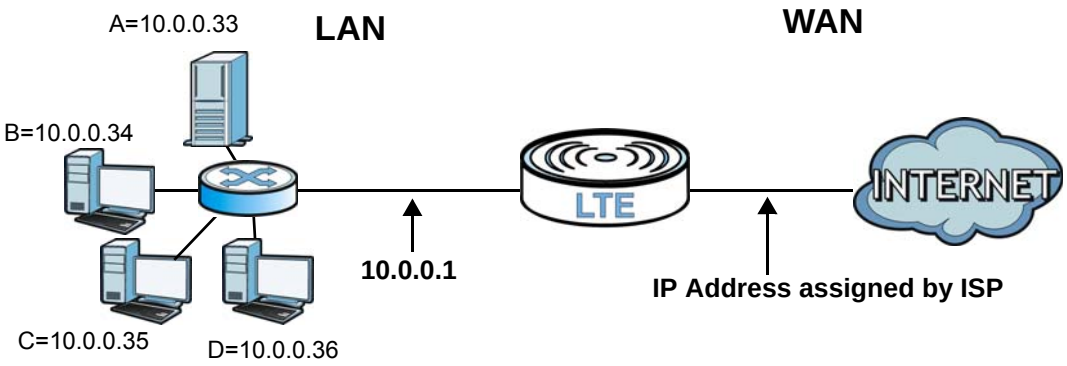
You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more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

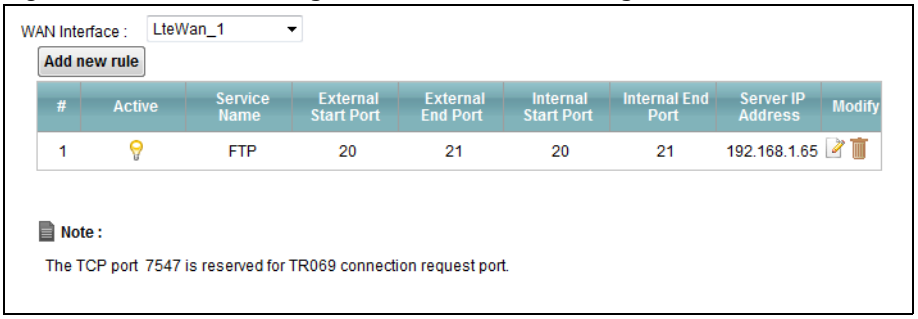
Figure 41 Multiple Servers Behind NAT Example



8.3.1 The Port Forwarding Screen

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

Figure 42 Network Setting > NAT > Port Forwarding



The following table describes the fields in this screen.

Table 16 Network Setting > NAT > Port Forwarding

LABEL	DESCRIPTION
WAN Interface	Select the WAN interface for which to configure NAT port forwarding rules.
Add new rule	Click this to add a new port forwarding rule.
#	This is the index number of the entry.
Active	This field indicates whether the rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.

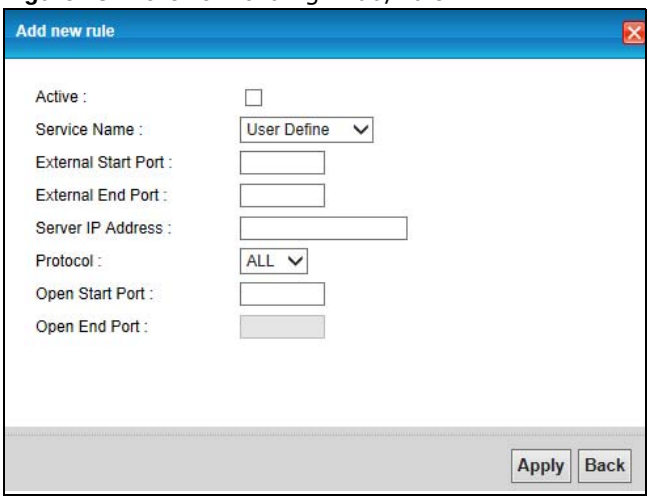
Table 16 Network Setting > NAT > Port Forwarding (continued)

LABEL	DESCRIPTION
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.
External Start Port	This is the first external port number that identifies a service.
External End Port	This is the last external port number that identifies a service.
Internal Start Port	This is the first internal port number that identifies a service.
Internal End Port	This is the last internal port number that identifies a service.
Server IP Address	This is the server's IP address.
Modify	Click the **Edit** icon to edit the port forwarding rule. 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.

8.3.2 The Port Forwarding Add/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 43 Port Forwarding: Add/Edit



The following table describes the labels in this screen.

Table 17 Port Forwarding: Add/Edit

LABEL	DESCRIPTION
Active	Select or clear this field to turn the port forwarding rule on or off.
Service Name	Select a service to forward or select **User Defined** and enter a name in the field to the right.
External Start Port	Configure this for a user-defined entry. Enter the original destination port for the packets. To forward only one port, enter the port number again in the **External End Port** field. To forward a series of ports, enter the start port number here and the end port number in the **External End Port** field.

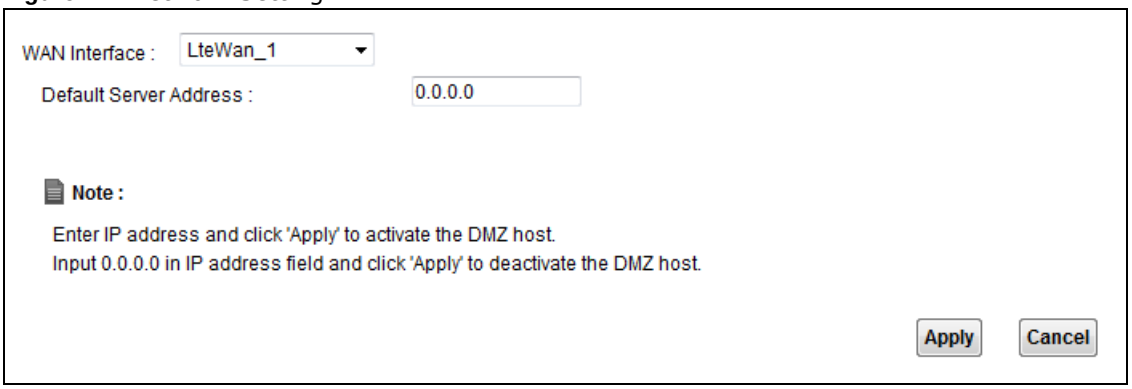
Table 17 Port Forwarding: Add/Edit (continued)

LABEL	DESCRIPTION
External End Port	Configure this for a user-defined entry. Enter the last port of the original destination port range. To forward only one port, enter the port number in the **External Start Port** field above and then enter it again in this field. 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.
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**.
Open Start Port	Configure this for a user-defined entry. 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.
Open End Port	Configure this for a user-defined entry. This shows the last port of the translated port range.
Apply	Click this to save your changes.
Back	Click this to exit this screen without saving.

8.4 The DMZ Screen

Click **Network Setting > NAT > DMZ** to open the **DMZ** screen. Use this screen to specify the IP address of a default server to receive packets from ports not specified in the **Port Forwarding** screen.

Figure 44 Network Setting > NAT > DMZ



The following table describes the fields in this screen.

Table 18 Network Setting > NAT > DMZ

LABEL	DESCRIPTION
WAN Interface	Select the WAN interface for which to configure a default server.
Default Server Address	Enter the IP address of the default server which receives packets from ports that are not specified in the **Port Forwarding** screen. Note: If you do not assign a default server, the LTE Device discards all packets received for ports not specified in the virtual server configuration.

Table 18 Network Setting > NAT > DMZ

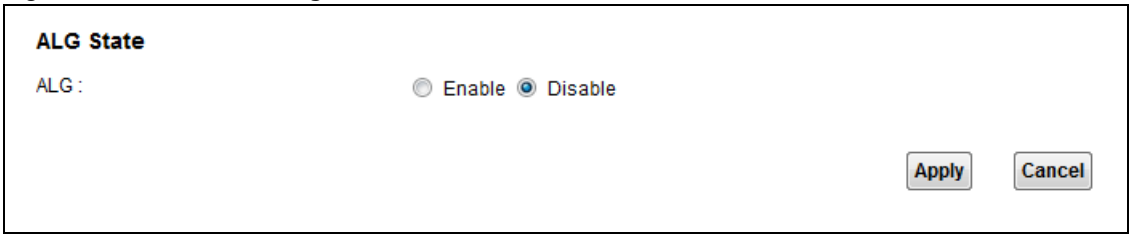
LABEL	DESCRIPTION
Apply	Click this to save your changes back to the LTE Device.
Cancel	Click **Cancel** to restore your previously saved settings.

8.5 The ALG Screen

Click **Network Setting > NAT > ALG** to open the **ALG** screen. Use this screen to enable and disable the NAT Application Layer Gateway (ALG) in the LTE Device.

The SIP ALG allows SIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream. When the LTE Device registers with the SIP register server, the SIP ALG translates the LTE Device's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if you enable the SIP ALG.

Figure 45 Network Setting > NAT > ALG



The following table describes the fields in this screen.

Table 19 Network Setting > NAT > ALG

LABEL	DESCRIPTION
ALG	Enable this to make sure SIP (VoIP) works correctly with port-forwarding.
Apply	Click this to save your changes back to the LTE Device.
Cancel	Click **Cancel** to restore your previously saved settings.

8.6 Technical Reference

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

8.6.1 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 20 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.

8.6.2 What NAT Does

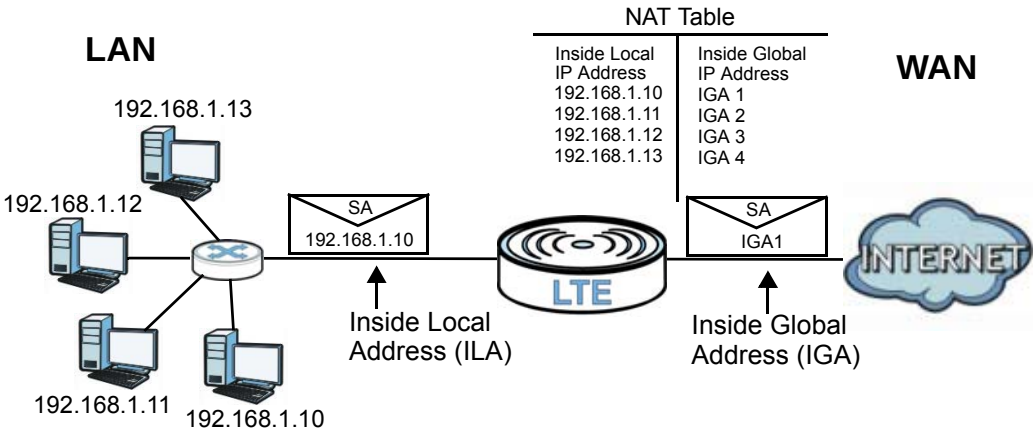
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address)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

8.6.3 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 46 How NAT Works



9

Dynamic DNS

9.1 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.

9.1.1 What You Need To Know

DYNDNS Wildcard

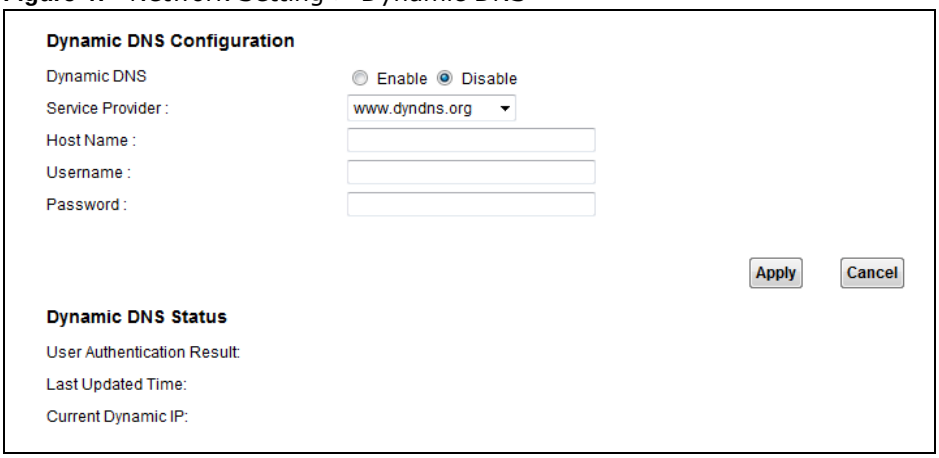
Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

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

9.2 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 47 Network Setting > Dynamic DNS



The following table describes the fields in this screen.

Table 21 Network Setting > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Configuration	
Dynamic DNS	Select **Enable** to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
Host Name	Type the domain name assigned to your LTE Device by your Dynamic DNS provider.
Username	Type your user name for the Dynamic DNS service provider.
Password	Type your password for the Dynamic DNS service provider.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.
Dynamic DNS Status	
User Authentication Result	This field displays the results of the LTE Device's attempt to authenticate with the Dynamic DNS service provider.
Last Updated Time	This field displays when the LTE Device last updated its WAN IP address to the Dynamic DNS service provider.
Current Dynamic IP	This field displays the LTE Device's current WAN IP address.

10 Firewall

10.1 Overview

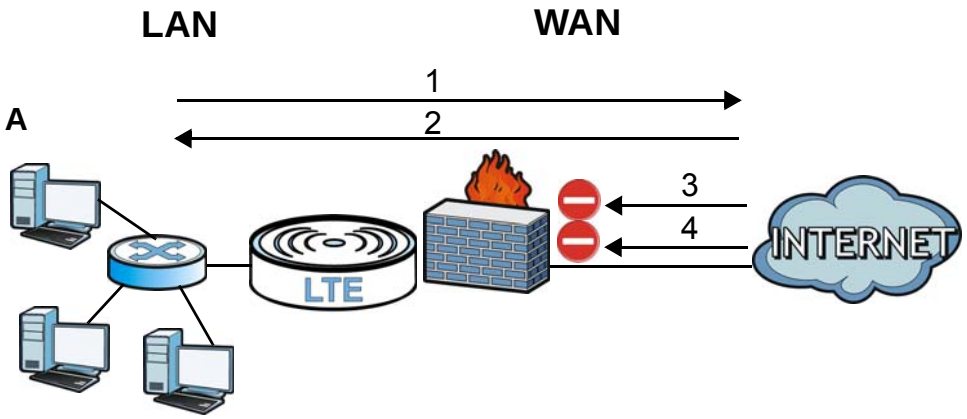
This chapter shows you how to enable the LTE Device firewall. Use the firewall to protect your LTE Device and network from attacks by hackers on the Internet and control access to it. The firewall:

- 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.
- blocks SYN and port scanner attacks.

By default, the LTE Device blocks DDOS, LAND and Ping of Death attacks whether the firewall is enabled or disabled.

The following figure illustrates the 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 48 Default Firewall Action



10.1.1 What You Can Do in the Firewall Screens

- Use the **General** screen (Section 10.2 on page 68) to select the firewall protection level on the LTE Device.
- Use the **Default Action** screen (Section 10.3 on page 69) to set the default action that the firewall takes on packets that do not match any of the firewall rules.
- Use the **Rules** screen (Section 10.4 on page 70) to view the configured firewall rules and add, edit or remove a firewall rule.

- Use the **DoS** screen (Section 10.5 on page 74) to set the thresholds that the LTE Device uses to determine when to start dropping sessions that do not become fully established (half-open sessions).

Note: The settings and rules configured in the **Default Action** and **Rules** screens can be apply only when the firewall protection level is set to **Custom** in the **General** screen.

10.1.2 What You Need to Know About Firewall

SYN Attack

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

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.

DDoS

A Distributed DoS (DDoS) attack is one in which multiple compromised systems attack a single target, thereby causing denial of service for users of the targeted system.

LAND Attack

In a Local Area Network Denial (LAND) attack, hackers flood SYN packets into the network with a spoofed source IP address of the target system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

Ping of Death

Ping of Death uses a "ping" utility to create and send an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. This may cause systems to crash, hang or reboot.

SPI

Stateful Packet Inspection (SPI) tracks each connection crossing the firewall and makes sure it is valid. Filtering decisions are based not only on rules but also context. For example, traffic from the WAN may only be allowed to cross the firewall in response to a request from the LAN.

RFC 4890 SPEC Traffic

RFC 4890 specifies the filtering policies for ICMPv6 messages. This is important for protecting against security threats including DoS, probing, redirection attacks and renumbering attacks that can be carried out through ICMPv6. Since ICMPv6 error messages are critical for establishing and maintaining communications, filtering policy focuses on ICMPv6 informational messages.

Anti-Probing

If an outside user attempts to probe an unsupported port on your LTE Device, an ICMP response packet is automatically returned. This allows the outside user to know the LTE Device exists. The LTE Device supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your LTE Device when unsupported ports are probed.

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.

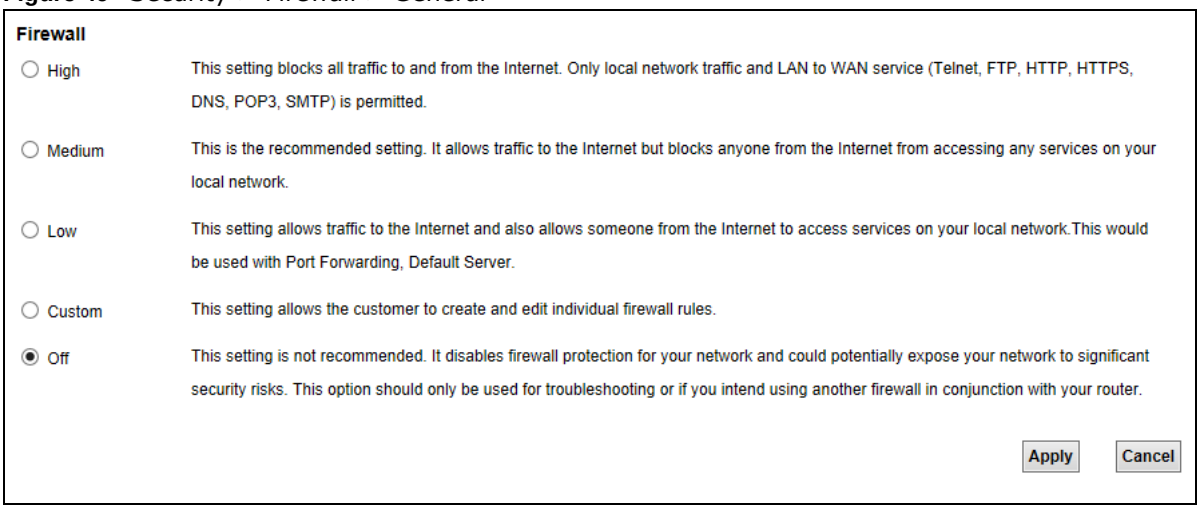
DoS Thresholds

For DoS attacks, the LTE Device uses thresholds to determine when to drop sessions that do not become fully established. These thresholds apply globally to all sessions. You can use the default threshold values, or you can change them to values more suitable to your security requirements.

10.2 Firewall General Screen

Use this screen to select the firewall protection level on the LTE Device. Click **Security > Firewall > General** to display the following screen.

Figure 49 Security > Firewall > General



The following table describes the labels in this screen.

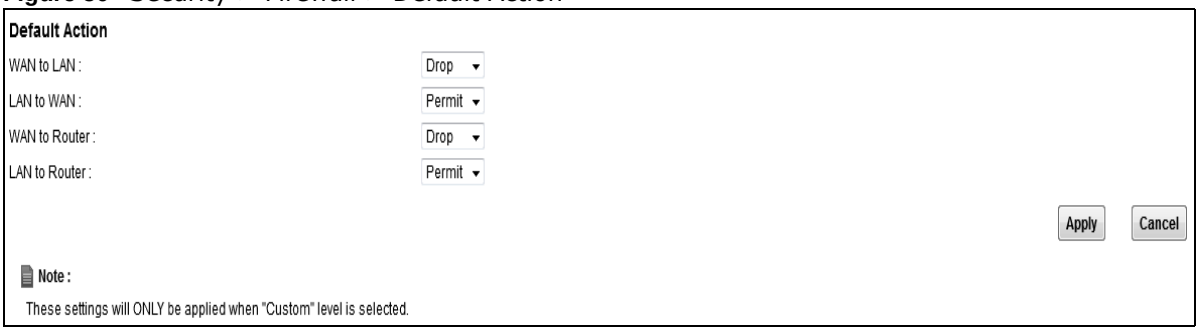
Table 22 Security > Firewall > General

LABEL	DESCRIPTION
High	This setting blocks all traffic to and from the Internet. Only local network traffic and LAN to WAN service (Telnet, FTP, HTTP, HTTPS, DNS, POP3, SMTP) is permitted.
Medium	This is the recommended setting. It allows traffic to the Internet but blocks anyone from the Internet from accessing any services on your local network.
Low	This setting allows traffic to the Internet and also allows someone from the Internet to access services on your local network. This would be used with Port Forwarding, Default Server.
Custom	Use this setting to be able to create and edit individual firewall rules. Firewall rules can be created in the Default Action screen (Section 10.3 on page 69) and Rules screen (Section 10.4 on page 70).
Off	This setting is not recommended. It disables firewall protection for your network and could potentially expose your network to significant security risks. This option should only be used for troubleshooting or if you intend to use another firewall in conjunction with your router.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

10.3 Default Action Screen

Use this screen to set the default action that the firewall takes on packets that do not match any of the firewall rules. Click **Security > Firewall > Default Action** to display the following screen.

Figure 50 Security > Firewall > Default Action



The following table describes the labels in this screen.

Table 23 Security > Firewall > Default Action

LABEL	DESCRIPTION
Default Action	Use the drop-down list boxes to select the default action that the firewall is to take on packets that are traveling in the selected direction and do not match any of the firewall rules. Select **Drop** to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender. Select **Reject** to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender. Select **Permit** to allow the passage of the packets.

Table 23 Security > Firewall > Default Action (continued)

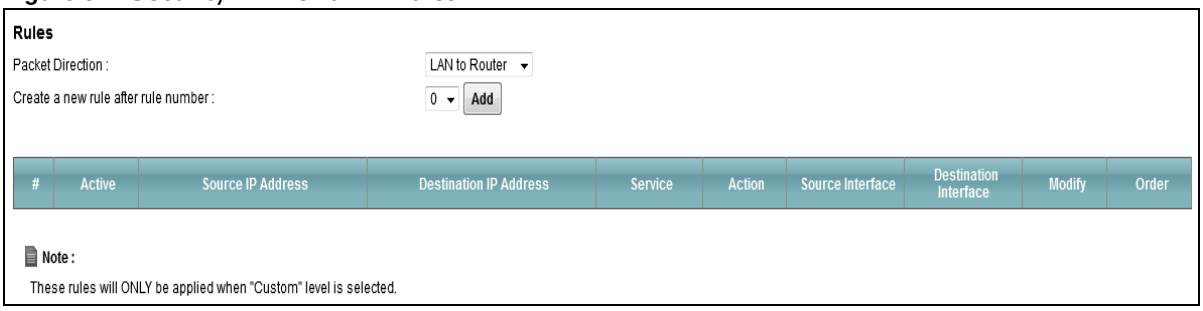
LABEL	DESCRIPTION
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

10.4 Rules Screen

Click **Security > Firewall > Rules** to display the following screen. This screen displays a list of the configured firewall rules. Note the order in which the rules are listed.

The ordering of your rules is very important as rules are applied in turn.

Figure 51 Security > Firewall > Rules



The following table describes the labels in this screen.

Table 24 Security > Firewall > Rules

LABEL	DESCRIPTION
Packet Direction	Use the drop-down list box to select a direction of travel of packets (**WAN to LAN**, **LAN to WAN**, **WAN to Router**, **LAN to Router**) for which you want to configure firewall rules.
Create a new rule after rule number	Select an index number and click **Add** to add a new firewall rule after the selected index number. For example, if you select "6", your new rule becomes number 7 and the previous rule 7 (if there is one) becomes rule 8.
#	This is the index number of the entry.
Active	Displays whether the firewall rule is enabled or disabled.
Source IP Address	Displays the source IP address or ranges of addresses to which the firewall rule applies. Please note that a blank source address is equivalent to **Any**.
Destination IP Address	Displays the destination IP address or ranges of addresses to which the firewall rule applies. Please note that a blank destination address is equivalent to **Any**.
Service	Displays the service to which this firewall rule applies.
Action	Displays whether the firewall 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**).
Source Interface	Displays the source interface to which the firewall rule applies. This is the interface through which the traffic entered the Device. Please note that a blank source interface is equivalent to **Any.**
Destination Interface	Displays the destination interface to which the firewall rule applies. This is the interface through which the traffic is destined to leave the Device. Please note that a blank source interface is equivalent to **Any**.

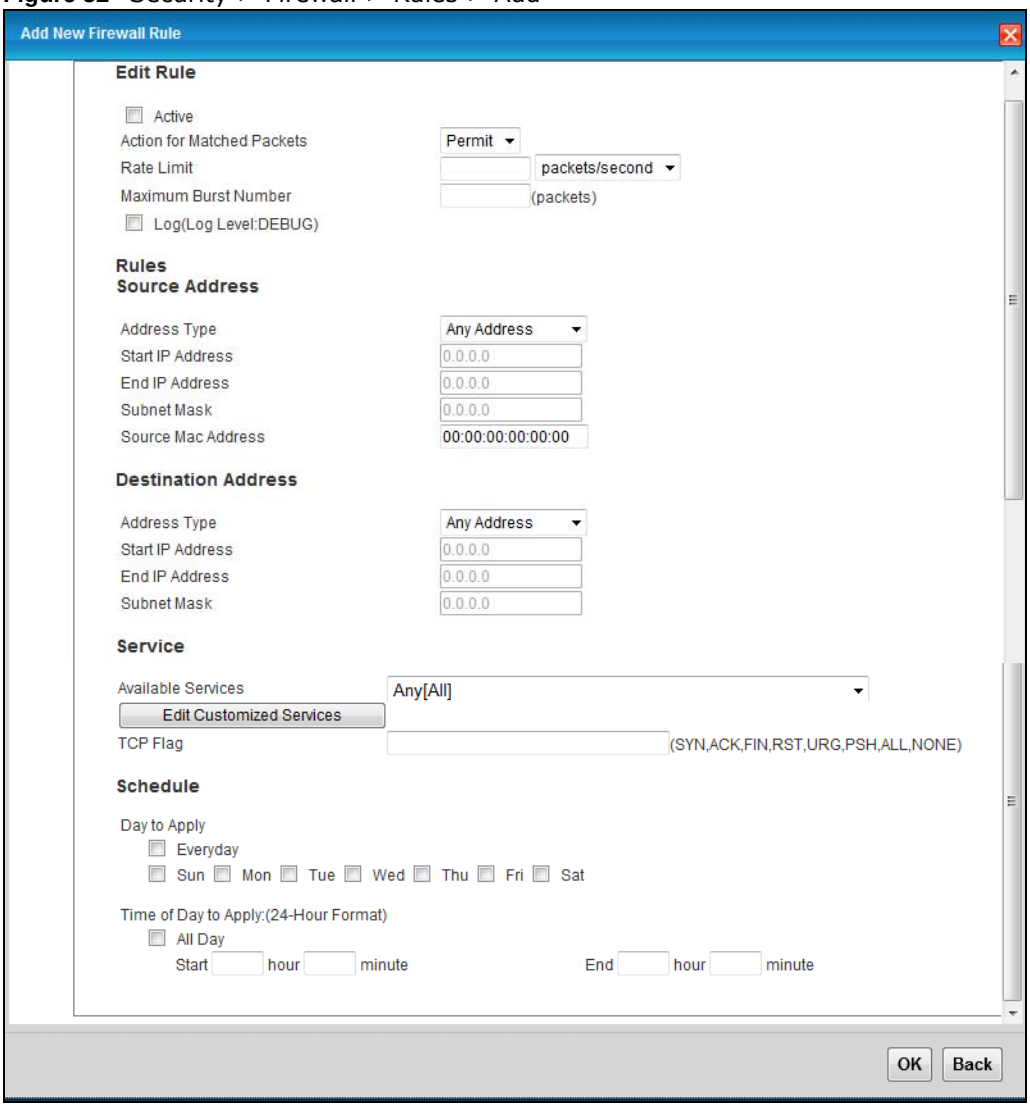
Table 24 Security > Firewall > Rules (continued)

LABEL	DESCRIPTION
Modify	Click the **Edit** icon to edit the firewall rule. Click the **Delete** icon to delete an existing firewall rule.
Order	Click **N** to change the sequence of the firewall rule.

10.4.1 Rules Add Screen

Use this screen to configure firewall rules. In the **Rules** screen, select an index number and click **Add** or click a rule's **Edit** icon to display this screen and refer to the following table for information on the labels.

Figure 52 Security > Firewall > Rules > Add



The following table describes the labels in this screen.

Table 25 Security > Firewall > Rules > Add

LABEL	DESCRIPTION
Edit Rule	
Active	Select this option to enable this firewall rule.
Action for Matched Packets	Use the drop-down list box to select whether to 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.
Rate Limit	Set a maximum number of packets per second, minute, or hour to limit the throughput of traffic that matches this rule.
Maximum Burst Number	Set the maximum number of packets that can be sent at the peak rate.
Log	This field determines if a log for packets that match the rule is created or not.
Rules/Source Address	
Address Type	Do you want your rule to apply to packets with a particular (single) IP, a range of IP addresses (for instance, 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop-down list box that includes: **Single Address**, **Range Address**, **Subnet Address** and **Any Address**.
Start IP Address	Enter the single IP address or the starting IP address in a range here.
End IP Address	Enter the ending IP address in a range here.
Subnet Mask	Enter the subnet mask here, if applicable.
Source Mac Address	Specify a source MAC address of traffic to which to apply this firewall rule applies. Please note that a blank source MAC address is equivalent to any.
Source Interface	Specify a source interface (**Blank**, **LteWAN1**, **LteWAN2**, or **LteWAN3**) to which the firewall rule applies. This is the interface through which the traffic entered the Device. Please note that a blank source interface is equivalent to any. Note: To show this option, go to **Network Setting > Broadband** to activate LteWAN2 and LteWAN3 first. Then go to **Security > Firewall > Rules** and configure **Packet Direction** as **WAN to LAN** or **WAN to Router**.
Destination Address	
Address Type	Do you want your rule to apply to packets with a particular (single) IP, a range of IP addresses (for instance, 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop-down list box that includes: **Single Address**, **Range Address**, **Subnet Address** and **Any Address**.
Start IP Address	Enter the single IP address or the starting IP address in a range here.
End IP Address	Enter the ending IP address in a range here.
Subnet Mask	Enter the subnet mask here, if applicable.
Destination Interface	Specify a destination interface (**Blank**, **LteWAN1**, **LteWAN2**, or **LteWAN3**) to which the firewall rule applies. This is the interface through which the traffic is destined to leave the Device. Please note that a blank destination interface is equivalent to any. Note: To show this option, go to **Network Setting > Broadband** to activate LteWAN2 and LteWAN3 first. Then go to **Security > Firewall > Rules** and configure **Packet Direction** as **LAN to WAN**.
Service	
Available Services	Select a service from the **Available Services** box.
Edit Customized Services	Click the **Edit Customized Service** button to bring up the screen that you use to configure a new custom service that is not in the predefined list of services.

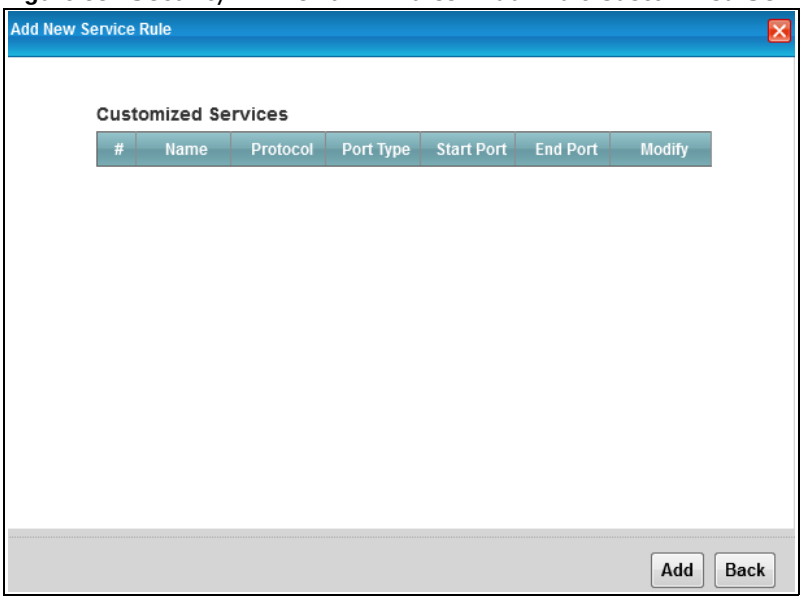
Table 25 Security > Firewall > Rules > Add (continued)

LABEL	DESCRIPTION
TCP Flag	Specify any TCP flag bits the firewall rule is to check for.
Schedule	Select the days and time during which to apply the rule. Select **Everyday** and **All Day** to always apply the rule.
OK	Click this to save your changes.
Back	Click this to exit this screen without saving.

10.4.2 Customized Services

Configure customized services and port numbers not predefined by the LTE Device. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. Click the **Edit Customized Services** button while editing a firewall rule to configure a custom service port. This displays the following screen.

Figure 53 Security > Firewall > Rules: Add: Edit Customized Services



The following table describes the labels in this screen.

Table 26 Security > Firewall > Rules: Add: Edit Customized Services

LABEL	DESCRIPTION
#	This is the number of your customized port.
Name	This is the name of your customized service.
Protocol	This shows the IP protocol (**TCP** or **UDP**) that defines your customized service.
Port Type	This is the port number or range that defines your customized service.
Start Port	This is a single port number or the starting port number of a range that defines your customized service.
End Port	This is a single port number or the ending port number of a range that defines your customized service.
Modify	Click this to edit a customized service.

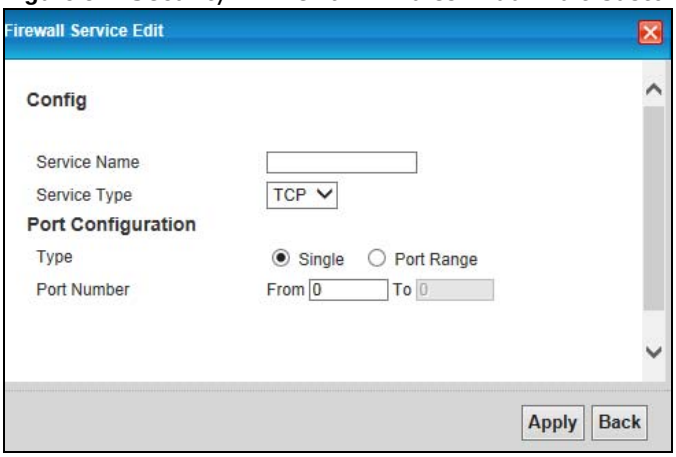
Table 26 Security > Firewall > Rules: Add: Edit Customized Services (continued)

LABEL	DESCRIPTION
Add	Click this to configure a customized service.
Back	Click this to return to the **Firewall Edit Rule** screen.

10.4.3 Customized Service Add

Use this screen to add a customized rule or edit an existing rule. Click **Add** icon in the **Customized Services** screen to display the following screen.

Figure 54 Security > Firewall > Rules: Add: Edit Customized Services: Add



The following table describes the labels in this screen.

Table 27 Security > Firewall > Rules: Edit: Edit Customized Services: Add/Edit

LABEL	DESCRIPTION
Config	
Service Name	Type a unique name for your custom port.
Service Type	Choose the IP port (**TCP** or **UDP**) that defines your customized port from the drop down list box.
Port Configuration	
Type	Click **Single** to specify one port only or **Port Range** to specify a span of ports that define your customized service.
Port Number	Type a single port number or the range of port numbers that define your customized service.
Apply	Click this to save your changes.
Back	Click this to exit this screen without saving.

10.5 DoS Screen

Use this screen to enable DoS protection. Click **Security > Firewall > Dos** to display the following screen.

Figure 55 Security > Firewall > Dos

The following table describes the labels in this screen.

Table 28 Security > Firewall > Dos

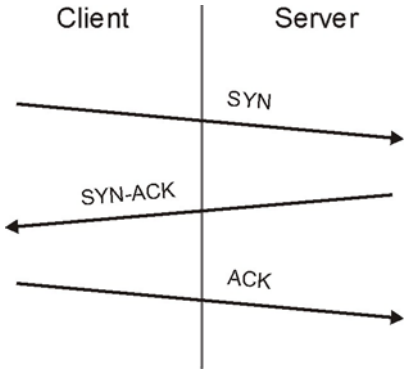
LABEL	DESCRIPTION
Denial of Services	Enable this to protect against DoS attacks. The LTE Device will drop sessions that surpass maximum thresholds.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.
Advanced	Click this to go to a screen to specify maximum thresholds at which the LTE Device will start dropping sessions.

10.5.1 The DoS Advanced Screen

For DoS attacks, the LTE Device uses thresholds to determine when to start dropping sessions that do not become fully established (half-open sessions). These thresholds apply globally to all sessions.

For TCP, half-open means that the session has not reached the established state-the TCP three-way handshake has not yet been completed. Under normal circumstances, the application that initiates a session sends a SYN (synchronize) packet to the receiving server. The receiver sends back an ACK (acknowledgment) packet and its own SYN, and then the initiator responds with an ACK (acknowledgment). After this handshake, a connection is established.

Figure 56 Three-Way Handshake



For UDP, half-open means that the firewall has detected no return traffic. An unusually high number (or arrival rate) of half-open sessions could indicate a DOS attack.

10.5.1.1 Threshold Values

If everything is working properly, you probably do not need to change the threshold settings as the default threshold values should work for most small offices. Tune these parameters when you

believe the LTE Device has been receiving DoS attacks that are not recorded in the logs or the logs show that the LTE Device is classifying normal traffic as DoS attacks. Factors influencing choices for threshold values are:

1 The maximum number of opened sessions.

2 The minimum capacity of server backlog in your LAN network.

3 The CPU power of servers in your LAN network.

4 Network bandwidth.

5 Type of traffic for certain servers.

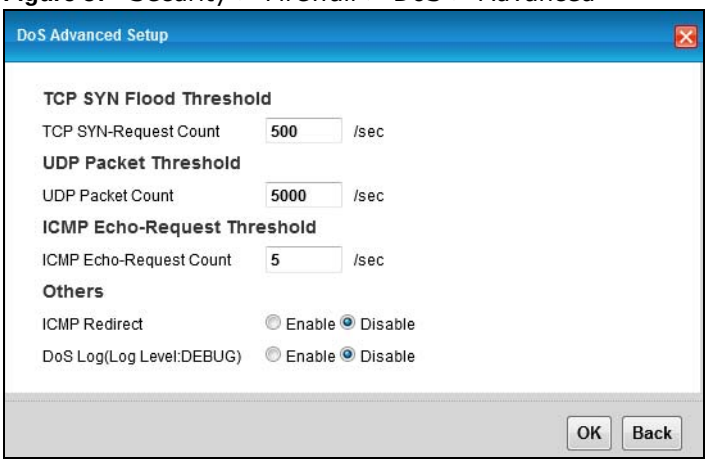
Reduce the threshold values if your network is slower than average for any of these factors (especially if you have servers that are slow or handle many tasks and are often busy).

- If you often use P2P applications such as file sharing with eMule or eDonkey, it's recommended that you increase the threshold values since lots of sessions will be established during a small period of time and the LTE Device may classify them as DoS attacks.

10.5.2 Configuring Firewall Thresholds

Click **Security > Firewall > DoS > Advanced** to display the following screen.

Figure 57 Security > Firewall > DoS > Advanced



The following table describes the labels in this screen.

Table 29 Security > Firewall > DoS > Advanced

LABEL	DESCRIPTION
TCP SYN Flood Threshold	
TCP SYN-Request Count	This is the rate of new TCP half-open sessions per second that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the LTE Device deletes half-open sessions as required to accommodate new connection attempts.
UDP Packet Threshold	

Table 29 Security > Firewall > DoS > Advanced (continued)

LABEL	DESCRIPTION
UDP Packet Count	This is the rate of new UDP half-open sessions per second that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the LTE Device deletes half-open sessions as required to accommodate new connection attempts.
ICMP Echo-Request Threshold	
ICMP Echo-Request Count	This is the rate of new ICMP Echo-Request half-open sessions per second that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the LTE Device deletes half-open sessions as required to accommodate new connection attempts.
Others	
ICMP Redirect	Select **Enable** to monitor for and block ICMP redirect attacks. An ICMP redirect attack is one where forged ICMP redirect messages can force the client device to route packets for certain connections through an attacker's host.
DoS Log(Log Level: DEBUG)	Select **Enable** to log DoS attacks. See LTE7410 User's Guide for information on viewing logs.
OK	Click this to save your changes.
Back	Click this to exit this screen without saving.

10.6 Firewall Technical Reference

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

10.6.1 Firewall Rules Overview

Your customized rules take precedence and override the LTE Device's default settings. The LTE Device checks the source IP address, destination IP address and IP protocol type of network traffic against the firewall rules (in the order you list them). When the traffic matches a rule, the LTE Device takes the action specified in the rule.

Firewall rules are grouped based on the direction of travel of packets to which they apply:

- LAN to Router
- LAN to WAN
- WAN to LAN
- WAN to Router

By default, the LTE Device's stateful packet inspection allows packets traveling in the following directions:

- LAN to Router

  These rules specify which computers on the LAN can manage the LTE Device (remote management).

Note: You can also configure the remote management settings to allow only a specific computer to manage the LTE Device.

- LAN to WAN

  These rules specify which computers on the LAN can access which computers or services on the WAN.

By default, the LTE Device's stateful packet inspection drops packets traveling in the following directions:

- WAN to LAN

  These rules specify which computers on the WAN can access which computers or services on the LAN.

Note: You also need to configure NAT port forwarding (or full featured NAT address mapping rules) to allow computers on the WAN to access devices on the LAN.

- WAN to Router

  By default the LTE Device stops computers on the WAN from managing the LTE Device. You could configure one of these rules to allow a WAN computer to manage the LTE Device.

Note: You also need to configure the remote management settings to allow a WAN computer to manage the LTE Device.

You may define additional rules and sets or modify existing ones but please exercise extreme caution in doing so.

For example, you may create rules to:

- Block certain types of traffic, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
- Allow everyone except your competitors to access a web server.
- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by comparing the source IP address, destination IP address and IP protocol type of network traffic to rules set by the administrator. Your customized rules take precedence and override the LTE Device's default rules.

10.6.2 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 router.
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 Protect against IP spoofing by making sure the firewall is active.

7 Keep the firewall in a secured (locked) room.

10.6.3 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.

11

Certificates

11.1 Overview

The LTE Device can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

11.1.1 What You Can Do in this Chapter

- Use the **Local Certificates** screen to view and import the LTE Device's CA-signed certificates (Section 11.2 on page 82).
- Use the **Trusted CA** screen to save the certificates of trusted CAs to the LTE Device. You can also export the certificates to a computer (Section 11.3 on page 84).

11.1.2 What You Need to Know

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

Certification Authorities

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities.

Public and Private Keys

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available; the other key is private and must be kept secure. Public-key encryption in general works as follows.

1. Tim wants to send a private message to Jenny. Tim generates a public-private key pair. What is encrypted with one key can only be decrypted using the other.
2. Tim keeps the private key and makes the public key openly available.
3. Tim uses his private key to encrypt the message and sends it to Jenny.
4. Jenny receives the message and uses Tim's public key to decrypt it.
5. Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

The LTE Device uses certificates based on public-key cryptology to authenticate users attempting to establish a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

Certification Path

A certification path is the hierarchy of certification authority certificates that validate a certificate. The LTE Device does not trust a certificate if any certificate on its path has expired or been revoked.

Certificate Directory Servers

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The LTE Device can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

Advantages of Certificates

Certificates offer the following benefits.

- The LTE Device only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

Certificate File Format

The certification authority certificate that you want to import has to be in PEM (Base-64) encoded X.509 file format. This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.

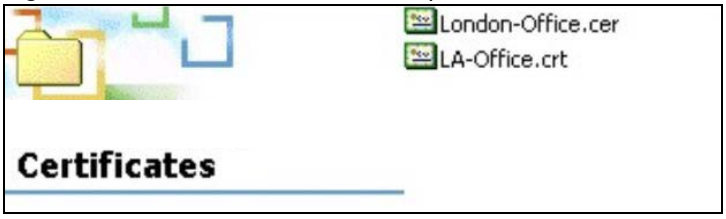
11.1.3 Verifying a Certificate

Before you import a trusted CA or trusted remote host certificate into the LTE Device, you should verify that you have the actual certificate. This is especially true of trusted CA certificates since the LTE Device also trusts any valid certificate signed by any of the imported trusted CA certificates.

You can use a certificate's fingerprint to verify it. A certificate's fingerprint is a message digest calculated using the MD5 or SHA1 algorithms. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

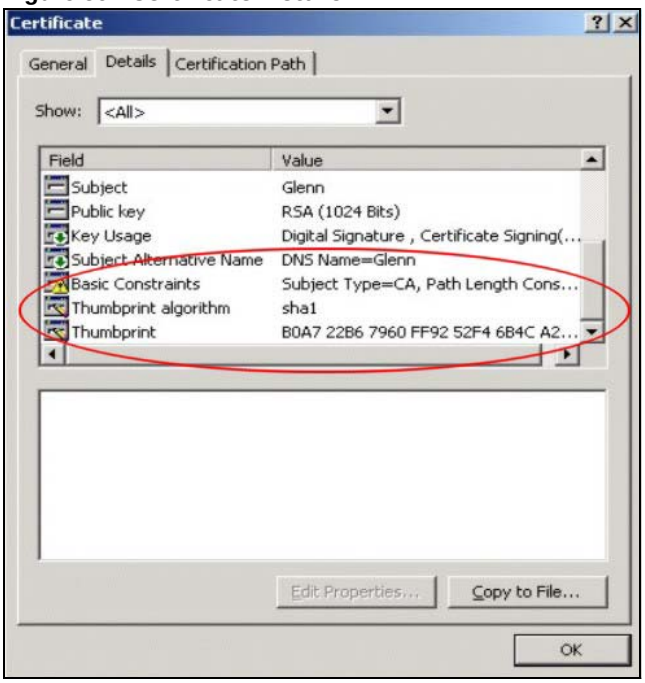
1. Browse to where you have the certificate saved on your computer.
2. Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 58 Certificates on Your Computer



3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

Figure 59 Certificate Details



4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may very based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

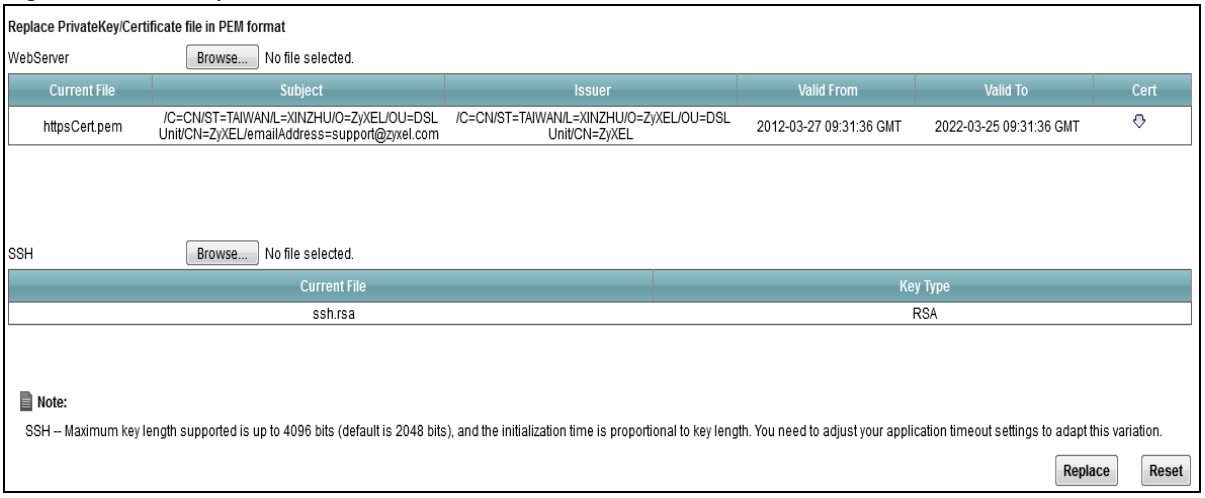
11.2 Local Certificates

Use this screen to view the LTE Device's summary list of certificates and certification requests. You can import the following certificates to your LTE Device:

- Web Server - This certificate secures HTTP connections.
- SSH- This certificate secures remote connections.

Click **Security > Certificates** to open the **Local Certificates** screen.

Figure 60 Security > Certificates > Local Certificates



The following table describes the labels in this screen.

Table 30 Security > Certificates > Local Certificates

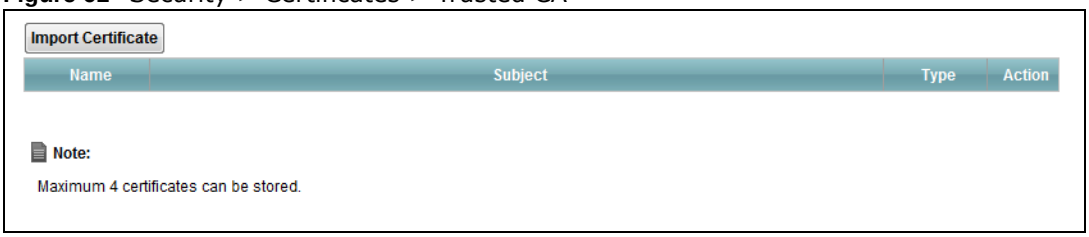
LABEL	DESCRIPTION
WebServer	Click **Browse...** to find the certificate file you want to upload.
Current File	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Subject	This field displays identifying information about the certificate's owner, such as **CN** (Common Name), **OU** (Organizational Unit or department), **O** (Organization or company) and **C** (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a **Not Yet Valid!** message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an **Expiring!** or **Expired!** message if the certificate is about to expire or has already expired.
Cert	Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
SSH	Type in the location of the **SSH** certificate file you want to upload in this field or click **Browse** to find it.
Current File	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Key Type	This field applies to the **SSH / SCP / SFTP** certificate. This shows the file format of the current certificate.
Replace	Click this to replace the certificates and save your changes back to the LTE Device.
Reset	Click this to clear your settings.

11.3 Trusted CA

Use this screen to view a summary list of certificates of the certification authorities that you have set the LTE Device to accept as trusted. The LTE Device accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

Click **Security > Certificates > Trusted CA** to open the **Trusted CA** screen.

Figure 61 Security > Certificates > Trusted CA



The following table describes the labels in this screen.

Table 31 Security > Certificates > Trusted CA

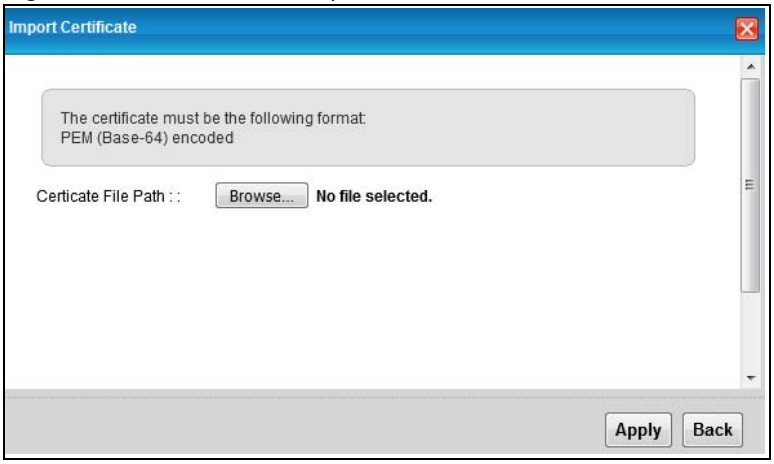
LABEL	DESCRIPTION
Import Certificate	Click this button to open a screen where you can save the certificate of a certification authority that you trust to the LTE Device.
Name	This field displays the name used to identify this certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), OU (Organizational Unit or department), Organization (O), State (ST) and Country (C). It is recommended that each certificate have unique subject information.
Type	This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate.
Action	Click the **View** icon to open a screen with an in-depth list of information about the certificate (or certification request). Click the **Delete** icon to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

11.4 Trusted CA Import

Click **Import Certificate** in the **Trusted CA** screen to open the **Import Certificate** screen. You can save a trusted certification authority's certificate to the LTE Device.

Note: You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 62 Trusted CA > Import



The following table describes the labels in this screen.

Table 32 Security > Certificates > Trusted CA > Import

LABEL	DESCRIPTION
Certificate File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click **Browse** to find the certificate file you want to upload.
Apply	Click this to save the certificate on the LTE Device.
Back	Click this to exit this screen without saving.

11.5 View Certificate

Use this screen to view in-depth information about the certification authority's certificate, change the certificate's name and set whether or not you want the LTE Device to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

Click **Security** > **Certificates** > **Trusted CA** to open the **Trusted CA** screen. Click the **View** icon to open the **View Certificate** screen.

Figure 63 Trusted CA: View

The following table describes the labels in this screen.

Table 33 Trusted CA: View

LABEL	DESCRIPTION
Certificate Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Certificate Detail	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Back	Click this to return to the previous screen.

12

L2TP VPN

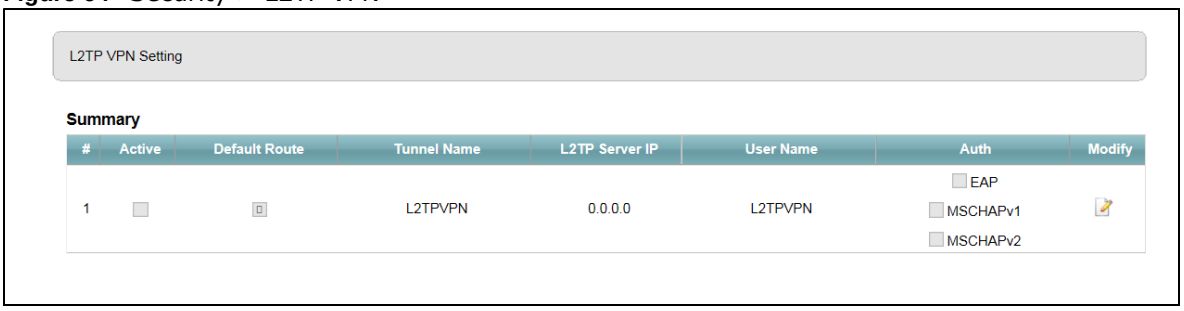
12.1 Overview

L2TP VPN tunnels network traffic between the LTE Device and a peer device or server over the Internet.

12.2 The Setup Screen

Use this screen to view and manage L2TP VPN tunnels. Click **Security > L2TP VPN** to open the following screen.

Figure 64 Security > L2TP VPN



The following table describes the labels in this screen.

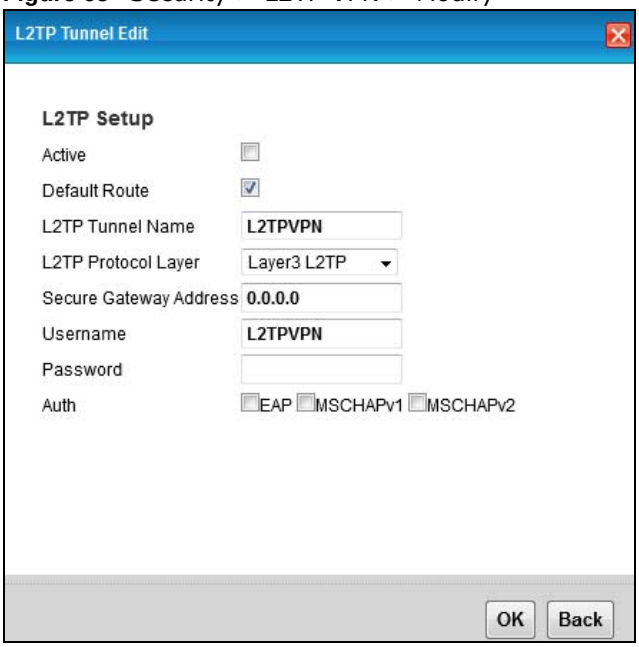
Table 34 Security > L2TP VPN

LABEL	DESCRIPTION
#	This shows the index number of an L2TP tunnel.
Active	This shows whether the L2TP VPN is on or not.
Default Route	This shows the default route is on or not.
Tunnel Name	This shows the name of this tunnel.
L2TP Server IP	This shows the IP address of the remote gateway with which the LTE Device establishes the L2TP tunnel.
User Name	The remote user must log into the LTE Device to use the L2TP VPN tunnel. This shows a user or user group that can use the L2TP VPN tunnel.
Auth	Select the protocol (EAP, MSCHAPv1 or MSCHAPv2) the LTE Device uses for user authentication.
Modify	Click the **Edit** icon to go to the screen where you can edit the L2TP VPN tunnel.

12.3 The Edit L2TP Tunnel Screen

Use this screen to modify a L2TP VPN tunnel. Click **Security > L2TP VPN** and then the **Edit** icon to open the following screen.

Figure 65 Security > L2TP VPN > Modify



The following table describes the labels in this screen.

Table 35 Security > L2TP VPN > Modify

LABEL	DESCRIPTION
Active	Click this to activate the L2TP VPN.
Default Route	Click this to activate the default route.
L2TP Tunnel Name	This shows the IP address that the LTE Device assigned for the remote user's computer to use within the L2TP VPN tunnel.
L2TP Protocol Layer	Select which OSI layer (Layer2 or Layer3) protocol the L2TP tunnels over a network. Use **Layer3 L2TP** to have the LTE Device tunnel OSI layer 3 protocol over a network and **Layer2 L2TP** for OSI layer 2 protocol (BCP tunnel).
Secure Gateway Address	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).
Username	The remote user must log into the LTE Device to use the L2TP VPN tunnel. This shows a user or user group that can use the L2TP VPN tunnel.
Password	Enter the password for the user.
Auth	Select the protocol (EAP, MSCHAPv1 or MSCHAPv2) the LTE Device uses for user authentication.
OK	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.

13

GRE VPN

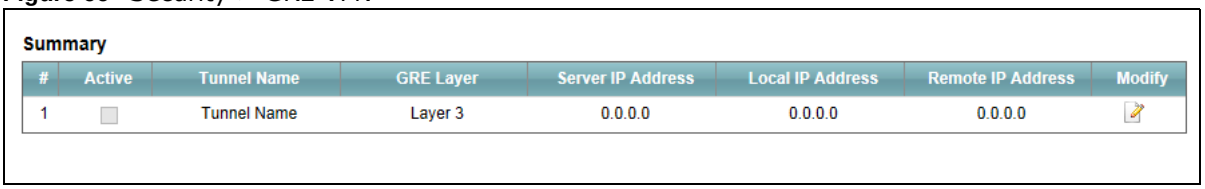
13.1 Overview

GRE (Generic Routing Encapsulation) tunnels encapsulate a wide variety of network layer protocol packet types inside IP tunnels. A GRE tunnel serves as a virtual point-to-point link between the LTE Device and another router over an IPv4 network.

13.2 The Setup Screen

Use this screen to view and manage GRE VPN tunnels. Click **Security** > **GRE VPN** to open the following screen.

Figure 66 Security > GRE VPN



The following table describes the labels in this screen.

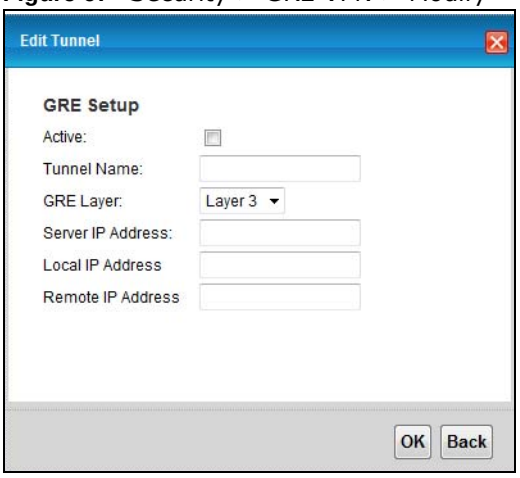
Table 36 Security > L2TP VPN

LABEL	DESCRIPTION
#	This shows the index number of a GRE tunnel.
Active	The check box is selected if the GRE VPN tunnel is enabled.
Tunnel Name	This shows the name of this tunnel.
GRE Layer	This shows whether the GRE VPN tunnels **Layer 2** or **Layer 3** protocol traffic.
Server IP Address	This is the IP address or domain name of the remote gateway to which the LTE Device's WAN interface tunnels traffic.
Local IP Address	This is the local hosts' IP addresses for which the LTE Device tunnels traffic sent to the remote gateway.
Remote IP Address	This is the remote hosts' IP addresses behind the remote gateway to which the LTE Device tunnels traffic.
Modify	Click the **Edit** icon to go to the screen where you can edit the GRE VPN tunnel.

13.3 The Edit GRE Tunnel Screen

Use this screen to modify a GRE VPN tunnel. Click **Edit** icon in **Security > GRE VPN > Modify** to open the following screen.

Figure 67 Security > GRE VPN > Modify



The following table describes the labels in this screen.

Table 37 Security > GRE VPN > Modify

LABEL	DESCRIPTION
Active	Click this to activate the GRE VPN.
Tunnel Name	Enter a descriptive name for the GRE tunnel.
GRE Layer	Select which OSI layer (**Layer 2** or **Layer 3**) protocol the GRE tunnels over a network. Use layer 2 when 1 local LAN PC and 1 LAN PC behind the remote gateway IPs are in the same subnet domain. Use layer 3 when the LAN PC IPs are in different subnet domains.
Server IP Address	Enter the IP address or domain name of the remote gateway to which the LTE Device's WAN interface tunnels traffic.
Local IP Address	This field displays when you select the layer 3 GRE layer. Enter the IP address of the local LAN computer that can use the GRE tunnel.
Remote IP Address	This field displays when you select the layer 3 GRE layer. Enter the IP address of the computer behind the remote gateway to which the LTE Device's WAN interface tunnels traffic.
OK	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

VoIP

14.1 Overview

Use this chapter to:

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

14.1.1 What You Can Do in this Chapter

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

- Use the **SIP Service Provider** screens to configure the SIP server information, and the numbers for certain phone functions (Section 14.2 on page 93).
- Use the **SIP Account** screens to set up information about your SIP account, control which SIP accounts the phones connected to the LTE Device use and configure audio settings such as volume levels for the phones connected to the ZyXEL Device (Section 14.3 on page 100).
- Use the **Phone** screen to change settings that depend on the country you are in (Section 14.4 on page 103).
- Use the **Call Rule** screen to set up shortcuts for dialing frequently-used (VoIP) phone numbers (Section 14.5 on page 104).

You don't necessarily need to use all these screens to set up your account. In fact, if your service provider did not supply information on a particular field in a screen, it is usually best to leave it at its default setting.

14.1.2 What You Need to Know

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

VoIP

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

SIP

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

SIP Accounts

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

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

Voice Activity Detection/Silence Suppression

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

Comfort Noise Generation

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

Echo Cancellation

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

Use this screen to maintain basic information about each SIP account. You can also enable and disable each SIP account, configure the volume, echo cancellation and VAD (Voice Activity Detection) settings for each individual phone port on the LTE Device.

How to Find Out More

See page 104 for advanced technical information on SIP.

14.1.3 Before You Begin

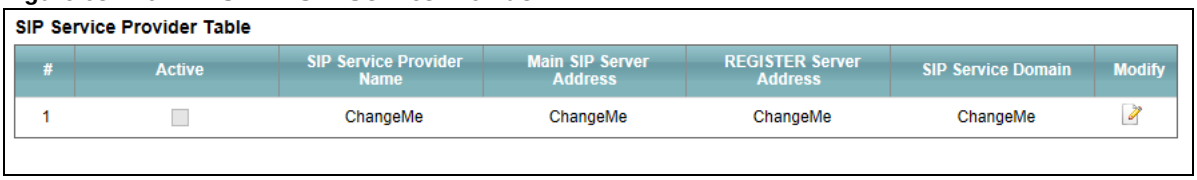
- Before you can use these screens, you need to have a VoIP account already set up. If you don't have one yet, you can sign up with a VoIP service provider over the Internet.

- You should have the information your VoIP service provider gave you ready, before you start to configure the LTE Device.

14.2 The SIP Service Provider Screen

Use this screen to manage profiles of SIP service provider settings. Click **VoIP > SIP** to open the **SIP Service Provider** screen.

Figure 68 VoIP > SIP > SIP Service Provider



The following table describes the labels in this screen.

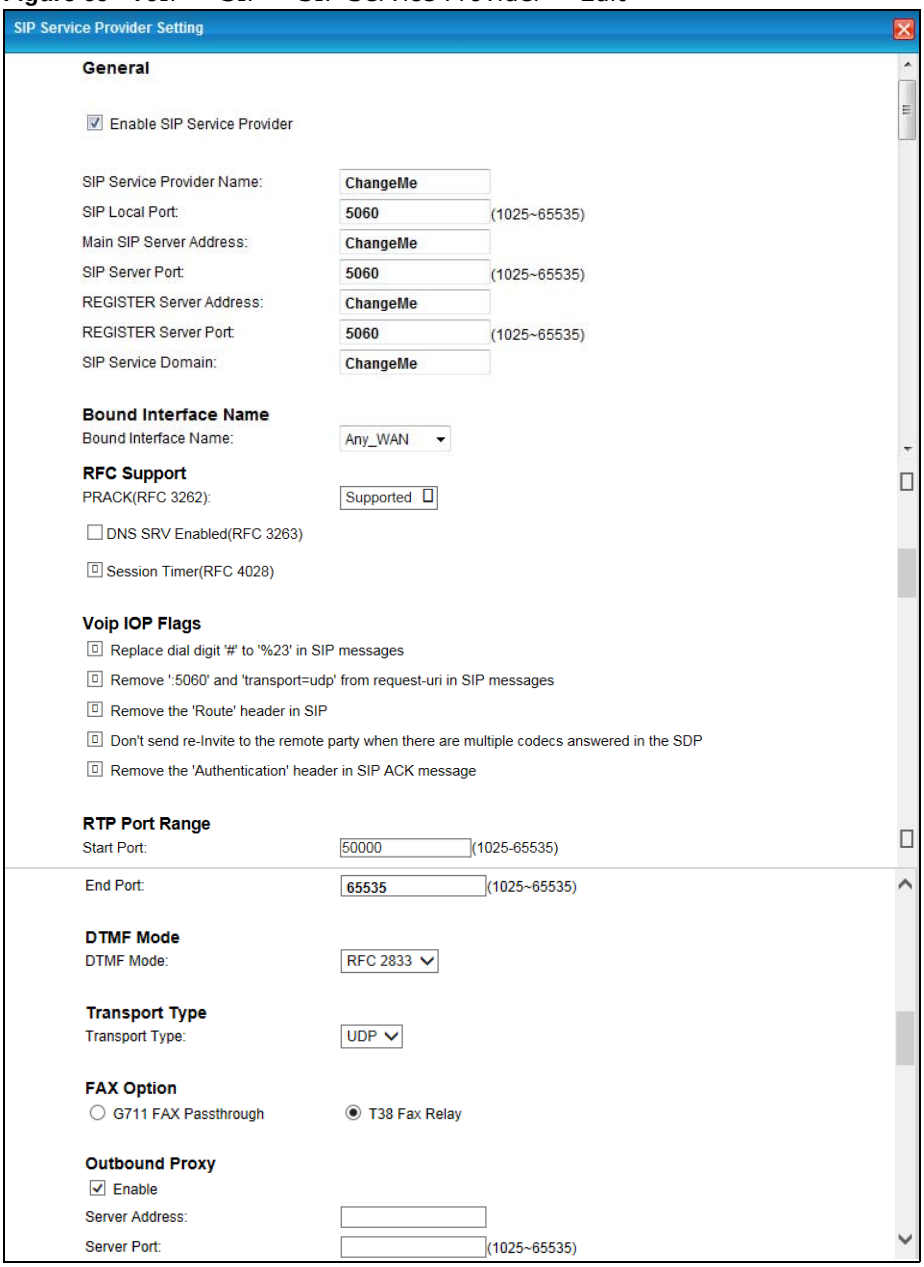
Table 38 VoIP > SIP > SIP Service Provider

LABEL	DESCRIPTION
#	This is the index number of the entry.
Active	The check box is selected if this SIP service provider is enabled.
SIP Service Provider Name	This shows the name of the SIP service provider.
Main SIP Server Address	This shows the IP address or domain name of the SIP server.
REGISTER Server Address	This shows the IP address or domain name of the SIP register server.
SIP Service Domain	This shows the SIP service domain name. In the full SIP URI, this is the part after the @ symbol.
Modify	Click the **Edit** icon to configure the profile of SIP service provider settings.

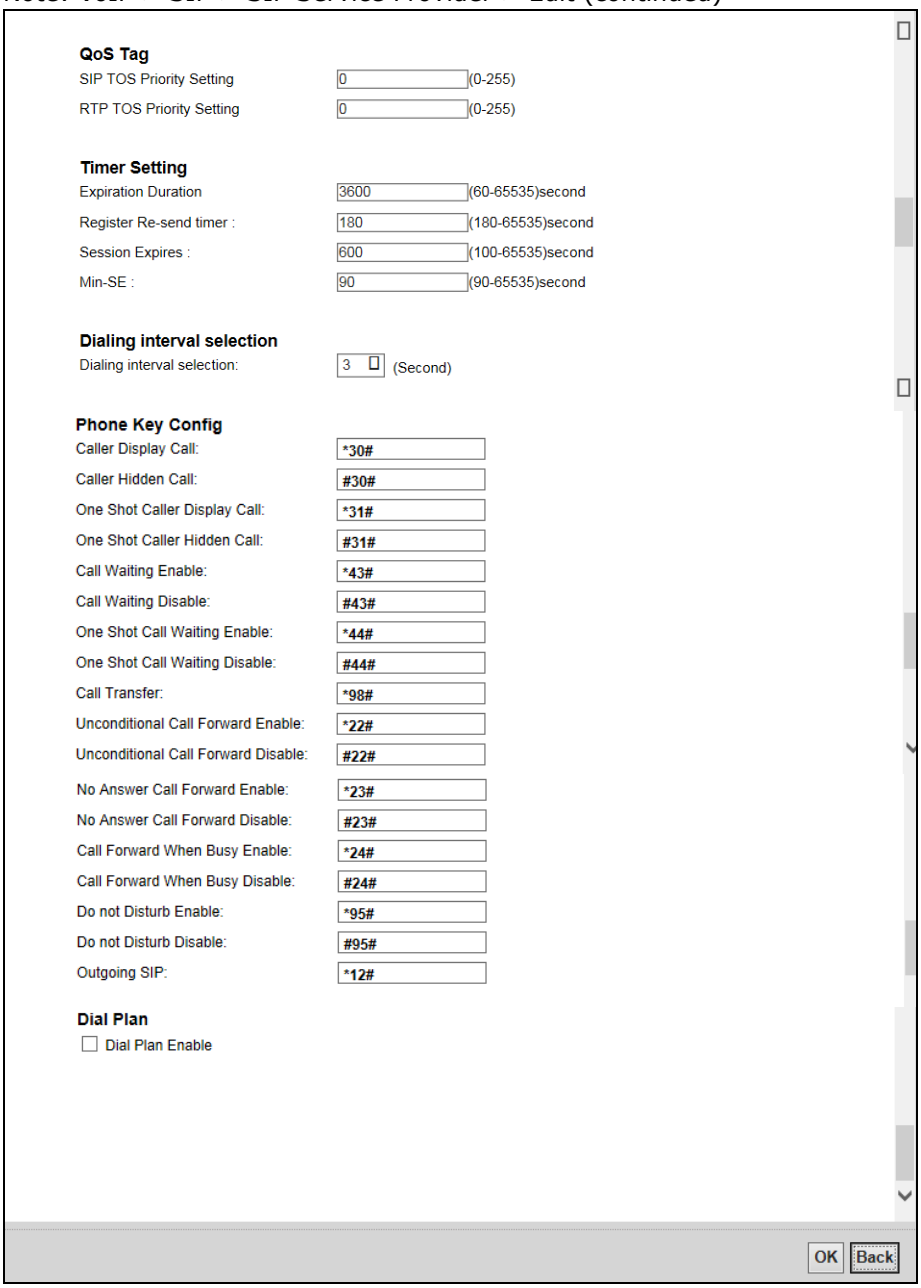
14.2.1 Edit SIP Service Provider

Use this screen to configure the SIP server information, the numbers for certain phone functions and dialing plan for a SIP service provider. Click **VoIP > SIP > SIP Service Provider** and then click the **Edit** icon next to a profile of SIP service provider settings to open the following screen.

Figure 69 VoIP > SIP > SIP Service Provider > Edit



Note: VoIP > SIP > SIP Service Provider > Edit (continued)



The following table describes the labels in this screen.

Table 39 VoIP > SIP > SIP Service Provider > Edit

LABEL	DESCRIPTION
General	
Enable SIP Service Provider	Select this if you want the LTE Device to use this SIP provider. Clear it if you do not want the LTE Device to use this SIP provider.
SIP Service Provider Name	Enter the name of your SIP service provider.
SIP Local Port	Enter the LTE Device's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.

Table 39 VoIP > SIP > SIP Service Provider > Edit (continued)

LABEL	DESCRIPTION
Main SIP Server Address	Enter the IP address or domain name of the SIP server provided by your VoIP service provider. You can use up to 256 printable ASCII characters. It does not matter whether the SIP server is a proxy, redirect or register server.
SIP Server Port	Enter the SIP server's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
REGISTER Server Address	Enter the IP address or domain name of the SIP register server, if your VoIP service provider gave you one. Otherwise, enter the same address you entered in the **SIP Server Address** field. You can use up to 256 printable ASCII characters.
REGISTER Server Port	Enter the SIP register server's listening port number, if your VoIP service provider gave you one. Otherwise, enter the same port number you entered in the **SIP Server Port** field.
SIP Service Domain	Enter the SIP service domain name. In the full SIP URI, this is the part after the @ symbol. You can use up to 127 printable ASCII Extended set characters.
Bound Interface Name	
Bound Interface Name	If you select **Any_WAN**, the LTE Device automatically activates the VoIP service when any WAN connection is up. If you select **Multi_WAN**, you also need to select the pre-configured WAN connections. The VoIP service is activated only when one of the selected WAN connections is up.
RFC Support	
PRACK (RFC 3262)	RFC 3262 defines a mechanism to provide reliable transmission of SIP provisional response messages, which convey information on the processing progress of the request. This uses the option tag 100rel and the Provisional Response ACKnowledgement (PRACK) method. Select **Supported** or **Required** to have the LTE Device include a SIP Require/Supported header field with the option tag 100rel in all INVITE requests. When the LTE Device receives a SIP response message indicating that the phone it called is ringing, the LTE Device sends a PRACK message to have both sides confirm the message is received. If you select **Supported**, the peer device supports the option tag 100rel to send provisional responses reliably. If you select **Required**, the peer device requires the option tag 100rel to send provisional responses reliably. Select **Disabled** to turn off this function.
DNS SRV Enabled (RFC 3263)	Select this to have the LTE Device query your ISP's DNS server for a list of any available SIP servers that it maintains. This is useful if your static SIP server experiences difficulties, making it hard for your IP phone users to make SIP calls.
Session Timer (RFC 4028)	Select this to have the LTE Device support RFC 4028. This makes sure that SIP sessions do not hang and the SIP line can always be available for use.
VoIP IOP Flags - Select VoIP inter-operability settings.	
	Replace dial digit '#' to '%23' in SIP messages.
	Remove ':5060' and 'transport=udp' from request-uri in SIP messages.
	Remove the 'Route' header in SIP messages.
	Don't send re-Invite to the remote party when there are multiple codecs answered in the Session Description Protocol (SDP).
	Remove the 'Authentication' header in SIP ACK messages.
RTP Port Range	

Table 39 VoIP > SIP > SIP Service Provider > Edit (continued)

LABEL	DESCRIPTION
Start Port End Port	Enter the listening port number(s) for RTP traffic, if your VoIP service provider gave you this information. Otherwise, keep the default values. To enter one port number, enter the port number in the **Start Port** and **End Port** fields. To enter a range of ports, • enter the port number at the beginning of the range in the **Start Port** field. • enter the port number at the end of the range in the **End Port** field.
DTMF Mode	Control how the LTE Device handles the tones that your telephone makes when you push its buttons. You should use the same mode your VoIP service provider uses. **RFC2833** - send the DTMF tones in RTP packets. **Inband** - send the DTMF tones in the voice data stream. This method works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.726) can distort the tones. **SIPInfo** - send the DTMF tones in SIP messages.
Transport Type	
Transport Type	Select the transport layer protocol **UDP** or **TCP** (usually UDP) used for SIP.
FAX Option	This field controls how the LTE Device handles fax messages.
G711 Fax Passthrough	Select this if the LTE Device should use G.711 to send fax messages. The peer devices must also use G.711.
T38 Fax Relay	Select this if the LTE Device should send fax messages as UDP or TCP/IP packets through IP networks. This provides better quality, but it may have inter-operability problems. The peer devices must also use T.38.
Outbound Proxy	
Enable	Select this if your VoIP service provider has a SIP outbound server to handle voice calls. This allows the LTE Device to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off any SIP ALG on a NAT router in front of the LTE Device to keep it from re-translating the IP address (since this is already handled by the outbound proxy server).
Server Address	Enter the IP address or domain name of the SIP outbound proxy server.
Server Port	Enter the SIP outbound proxy server's listening port, if your VoIP service provider gave you one. Otherwise, keep the default value.
QoS Tag	
SIP TOS Priority Setting	Enter the DSCP (DiffServ Code Point) number for SIP message transmissions. The LTE Device creates Class of Service (CoS) priority tags with this number to SIP traffic that it transmits.
RTP TOS Priority Setting	Enter the DSCP (DiffServ Code Point) number for RTP voice transmissions. The LTE Device creates Class of Service (CoS) priority tags with this number to RTP traffic that it transmits.
Timer Setting	
Expiration Duration	Enter the number of seconds your SIP account is registered with the SIP register server before it is deleted. The LTE Device automatically tries to re-register your SIP account when one-half of this time has passed. (The SIP register server might have a different expiration.)
Register Re-send timer	Enter the number of seconds the LTE Device waits before it tries again to register the SIP account, if the first try failed or if there is no response.
Session Expires	Enter the number of seconds the LTE Device lets a SIP session remain idle (without traffic) before it automatically disconnects the session.

Table 39 VoIP > SIP > SIP Service Provider > Edit (continued)

LABEL	DESCRIPTION
Min-SE	Enter the minimum number of seconds the LTE Device lets a SIP session remain idle (without traffic) before it automatically disconnects the session. When two SIP devices start a SIP session, they must agree on an expiration time for idle sessions. This field is the shortest expiration time that the LTE Device accepts.
Dialing interval selection	
Dialing interval selection	Enter the number of seconds the LTE Device should wait after you stop dialing numbers before it makes the phone call. The value depends on how quickly you dial phone numbers.
Phone Key Config Use this section to customize the phone keypad combinations you use to access certain features on the LTE Device.	
Caller Display Call	This code is used to display the caller ID for outgoing calls.
Caller Hidden Call	This code is used to hide the caller ID for outgoing calls.
One Shot Caller Display Call	This code is used to display the caller ID only for the phone call your are going to make.
One Shot Caller Hidden Call	This code is used to hide the caller ID only for the phone call your are going to make.
Call Waiting Enable	This code is used to turn the call waiting feature on. With call waiting, you hear a special beep notifying you of another incoming call while you have a call. It allows you to place the first incoming call on hold and answer the second call so that you won't miss any important calls.
Call Waiting Disable	This code is used to turn the call waiting feature off.
One Shot Call Waiting Enable	This code is used to enable call waiting only for the phone call your are going to make. See the description for the **Call Waiting Enable** field for more information.
One Shot Call Waiting Disable	This code is used to disable one shot call waiting.
Call Transfer	This code is used to enable call transfer that allows you to transfer an incoming call (that you have answered) to another phone.
Unconditional Call Forward Enable	This code is used to enable unconditional call forwarding. Incoming calls are always forwarded to a specified number without any condition.
Unconditional Call Forward Disable	This code is used to disable unconditional call forwarding.
No Answer Call Forward Enable	This code is used to enable call forwarding when there is no answer at a SIP number (no one picked up the connected phone that uses the SIP number).
No Answer Call Forward Disable	This code is used to disable call forwarding when there is no answer at a SIP number (no one picked up the connected phone that uses the SIP number).
Call Forward When Busy Enable	This code is used to enable call forwarding when the phone is busy.
Call Forward When Busy Disable	This code is used to disable call forwarding when the phone is busy.
Do Not Disturb Enable	This code is used to turn the do not disturb feature on. This has the LTE Device reject all calls destined to the phone line.
Do Not Disturb Disable	This code is used to turn the Do Not Disturb feature off.

Table 39 VoIP > SIP > SIP Service Provider > Edit (continued)

LABEL	DESCRIPTION
Outgoing SIP	Enter the key combinations that you can enter to select the SIP account that you use to make outgoing calls. If you enter #12(by default)<SIP account index number>#<the phone number you want to call>, #1201#12345678 for example, the LTE Device uses the first SIP account to call 12345678.
Dial Plan	
Dial Plan Enable	Select this to activate the dial plan rules you specify in the text box provided. See Section 14.2.2 on page 99 for how to set up a rule.
OK	Click this to save your changes.
Back	Click this to exit this screen without saving.

14.2.2 Dial Plan Rules

A dial plan defines the dialing patterns, such as the length and range of the digits for a telephone number. It also includes country codes, access codes, area codes, local numbers, long distance numbers or international call prefixes. For example, the dial plan ([2-9]xxxxxx) does not allow a local number which begins with 1 or 0.

Without a dial plan, users have to manually enter the whole callee's number and wait for the specified dialing interval to time out or press a terminator key (usually the pound key on the phone keypad) before the LTE Device makes the call.

The LTE Device initializes a call when the dialed number matches any one of the rules in the dial plan. Dial plan rules follow these conventions:

- The collection of rules is in parentheses ().
- Rules are separated by the | (bar) symbol.
- "x" stands for a wildcard and can be any digit from 0 to 9.
- A subset of keys is in a square bracket []. Ranges are allowed.

  For example, [359] means a number matching this rule can be 3, 5 or 9. [26-8*] means a number matching this rule can be 2, 6, 7, 8 or *.
- The dot "." appended to a digit allows the digit to be ignored or repeated multiple times. Any digit (0~9, *, #) after the dot will be ignored.

  For example, (01.) means a number matching this rule can be 0, 01, 0111, 01111, and so on.
- <dialed-number:translated-number> indicates the number after the colon replaces the number before the colon in an angle bracket <>. For example,

  (<:1212> xxxxxxx) means the LTE Device automatically prefixes the translated-number "1212" to the number you dialed before making the call. This can be used for local calls in the US.

  (<9:> xxx xxxxxxx) means the LTE Device automatically removes the specified prefix "9" from the number you dialed before making the call. This is always used for making outside calls from an office.

  (xx<123:456>xxxx) means the LTE Device automatically translates "123" to "456" in the number you dialed before making the call.
- Calls with a number followed by the exclamation mark "!" will be dropped.
- Calls with a number followed by the termination character "@" will be made immediately. Any digit (0~9, *, #) after the @ character will be ignored.

In this example dial plan (0 | [49]11 | 1 [2-9]xx xxxxxxx | 1 947 xxxxxxx !), you can dial "0" to call the local operator, call 411 or 911, or make a long distance call with an area code starting from 2 to 9 in the US. The calls with the area code 947 will be dropped.

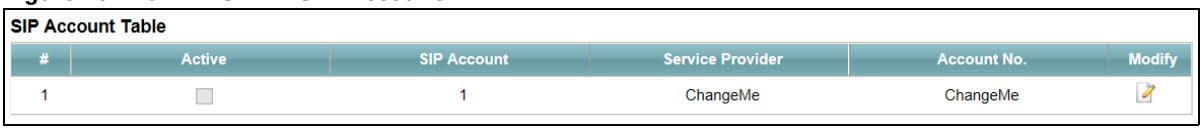
14.3 The SIP Account Screen

The LTE Device uses a SIP account to make outgoing VoIP calls and check if an incoming call's destination number matches your SIP account's SIP number. In order to make or receive a VoIP call, you need to enable and configure a SIP account, and map it to a phone port. The SIP account contains information that allows your LTE Device to connect to your VoIP service provider.

See Section 14.4 on page 103 for how to map a SIP account to a phone port.

To access the following screen, click **VoIP > SIP > SIP Account**.

Figure 70 VoIP > SIP > SIP Account



The following table describes the labels in this screen.

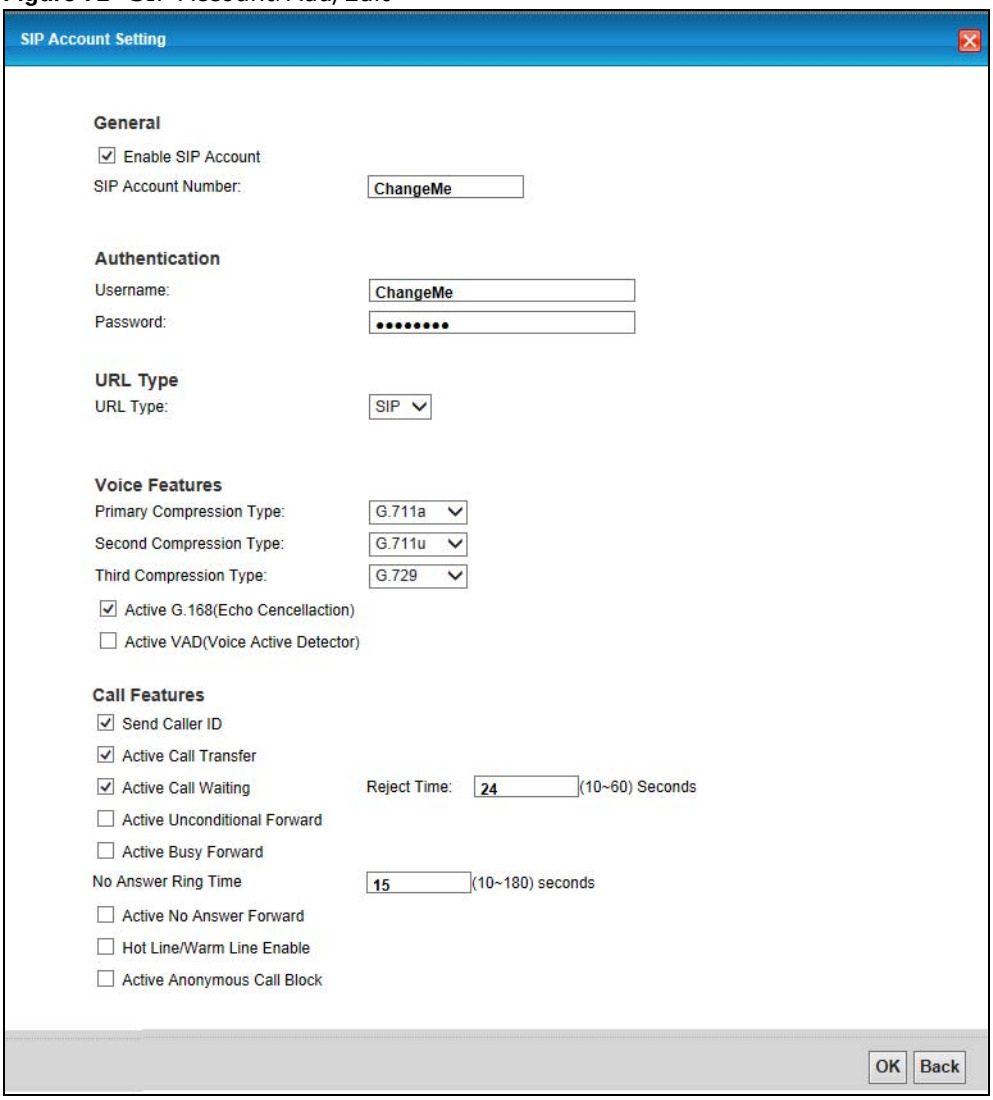
Table 40 VoIP > SIP > SIP Account

LABEL	DESCRIPTION
#	This is the index number of the entry.
Active	This shows whether the SIP account is activated or not. A yellow bulb signifies that this SIP account is activated. A gray bulb signifies that this SIP account is activated.
SIP Account	This shows the name of the SIP account.
Service Provider	This shows the name of the SIP service provider.
Account No.	This shows the SIP number.
Modify	Click the **Edit** icon to configure the SIP account.

14.3.1 Edit SIP Account

You can configure a SIP account. To access this screen, click the **Edit** icon next to an account.

Figure 71 SIP Account: Add/Edit



Each field is described in the following table.

Table 41 SIP Account: Edit

LABEL	DESCRIPTION
General	
Enable SIP Account	Select the check box to use this account. Clear it to not use this account.
SIP Account Number	Enter your SIP number. In the full SIP URI, this is the part before the @ symbol. You can use up to 64 printable ASCII characters.
Authentication	
Username	Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 128 printable ASCII characters.
Password	Enter the password for registering this SIP account, exactly as it was given to you. You can use up to 128 printable ASCII characters.
URL Type	

Table 41 SIP Account: Edit (continued)

LABEL	DESCRIPTION
URL Type	Select whether or not to include the SIP service domain name when the LTE Device sends the SIP number. **SIP** - include the SIP service domain name. **TEL** - do not include the SIP service domain name.
Voice Features	
Primary Compression Type Secondary Compression Type Third Compression Type	Select the type of voice coder/decoder (codec) that you want the LTE Device to use. G.711 provides higher voice quality but requires more bandwidth (64 kbps). • **G.729** provides good sound quality and reduces the required bandwidth to 8 kbps. • **G.711a** is typically used in Europe. • **G.711u** is typically used in North America and Japan. • **G.726-32** operates at 16, 24, 32 or 40 kbps. • **G.722** operates at 6.3 kbps or 5.3 kbps. When two SIP devices start a SIP session, they must agree on a codec. Select the LTE Device's first choice for voice coder/decoder. Select the LTE Device's second choice for voice coder/decoder. Select **None** if you only want the LTE Device to accept the first choice. Select the LTE Device's third choice for voice coder/decoder. Select **None** if you only want the LTE Device to accept the first or second choice.
Active G.168 (Echo Cancellation)	Select this if you want to eliminate the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
Active VAD (Voice Active Detector)	Select this if the LTE Device should stop transmitting when you are not speaking. This reduces the bandwidth the LTE Device uses.
Call Features	
Send Caller ID	Select this if you want to send identification when you make VoIP phone calls. Clear this if you do not want to send identification.
Active Call Transfer	Select this to enable call transfer on the LTE Device. This allows you to transfer an incoming call (that you have answered) to another phone.
Active Call Waiting	Select this to enable call waiting on the LTE Device. This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.
Reject Time	Specify a time of seconds that the LTE Device waits before rejecting the second call if you do not answer it.
Active Unconditional Forward	Select this if you want the LTE Device to forward all incoming calls to the specified phone number. Specify the phone number in the **To Number** field on the right.
Active Busy Forward	Select this if you want the LTE Device to forward incoming calls to the specified phone number if the phone port is busy. Specify the phone number in the **To Number** field on the right. If you have call waiting, the incoming call is forwarded to the specified phone number if you reject or ignore the second incoming call.
No Answer Ring Time	This field is used by the **Active No Answer Forward** feature. Enter the number of seconds the LTE Device should wait for you to answer an incoming call before it considers the call is unanswered.

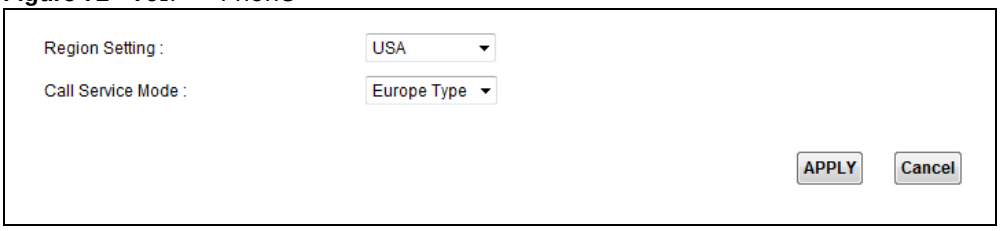
Table 41 SIP Account: Edit (continued)

LABEL	DESCRIPTION
Active No Answer Forward	Select this if you want the LTE Device to forward incoming calls to the specified phone number if the call is unanswered. (See **No Answer Time**.) Specify the phone number in the **To Number** field on the right.
Hot Line / Warm Line Enable	Select this to enable the hot line or warm line feature on the LTE Device.
Warm Line	Select this to have the LTE Device dial the specified warm line number after you pick up the telephone and do not press any keys on the keypad for a period of time.
Hot Line	Select this to have the LTE Device dial the specified hot line number immediately when you pick up the telephone.
Hot Line / Warm Line number	Enter the number of the hot line or warm line that you want the LTE Device to dial.
Warm Line number	Enter a number of seconds that the LTE Device waits before dialing the warm line number if you pick up the telephone and do not press any keys on the keypad.
Active Anonymous Call Block	Select this to have the phone not ring for incoming calls with caller ID deactivated.
OK	Click this to save your changes.
Back	Click this to exit this screen without saving.

14.4 Phone Screen

Use this screen to maintain settings that depend on which region of the world the LTE Device is in. To access this screen, click **VoIP > Phone**.

Figure 72 VoIP > Phone



Each field is described in the following table.

Table 42 VoIP > Phone

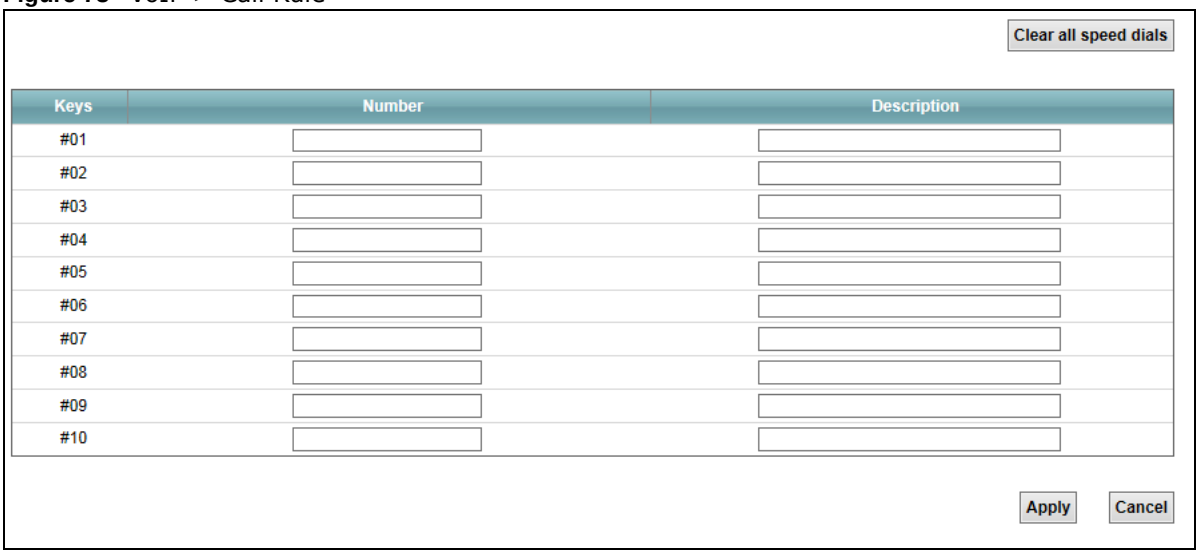
LABEL	DESCRIPTION
Region Setting	Select the place in which the LTE Device is located.
Call Service Mode	Select the mode for supplementary phone services (call hold, call waiting, call transfer and three-way conference calls) that your VoIP service provider supports. • **Europe Type** - use supplementary phone services in European mode. • **USA Type** - use supplementary phone services American mode. You might have to subscribe to these services to use them. Contact your VoIP service provider.
Apply	Click this to save your changes and to apply them to the LTE Device.
Cancel	Click this to set every field in this screen to its last-saved value.

14.5 Call Rule Screen

Use this screen to add, edit, or remove speed-dial numbers for outgoing calls. Speed dial provides shortcuts for dialing frequently-used (VoIP) phone numbers. You also have to create speed-dial entries if you want to call SIP numbers that contain letters. Once you have configured a speed dial rule, you can use a shortcut (the speed dial number, #01 for example) on your phone's keypad to call the phone number.

To access this screen, click **VoIP > Call Rule**.

Figure 73 VoIP > Call Rule



Each field is described in the following table.

Table 43 VoIP > Call Rule

LABEL	DESCRIPTION
Clear all speed dials	Click this to erase all the speed-dial entries.
Keys	This field displays the speed-dial number you should dial to use this entry.
Number	Enter the SIP number you want the LTE Device to call when you dial the speed-dial number.
Description	Enter a short description to identify the party you call when you dial the speed-dial number. You can use up to 127 printable ASCII characters.
Apply	Click this to save your changes and to apply them to the LTE Device.
Cancel	Click this to set every field in this screen to its last-saved value.

14.6 Technical Reference

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

14.6.1 VoIP

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

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

14.6.2 SIP

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

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

SIP Identities

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

SIP Number

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

SIP Service Domain

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

SIP Registration

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

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

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

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

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

Authorization Requirements

SIP registrations (and subsequent SIP requests) require a username and password for authorization. These credentials are validated via a challenge / response system using the HTTP digest mechanism (as detailed in RFC 3261, "SIP: Session Initiation Protocol").

SIP Servers

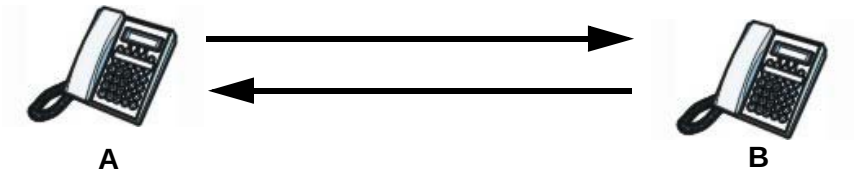
SIP is a client-server protocol. A SIP client is an application program or device that sends SIP requests. A SIP server responds to the SIP requests.

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

SIP User Agent

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

Figure 74 SIP User Agent



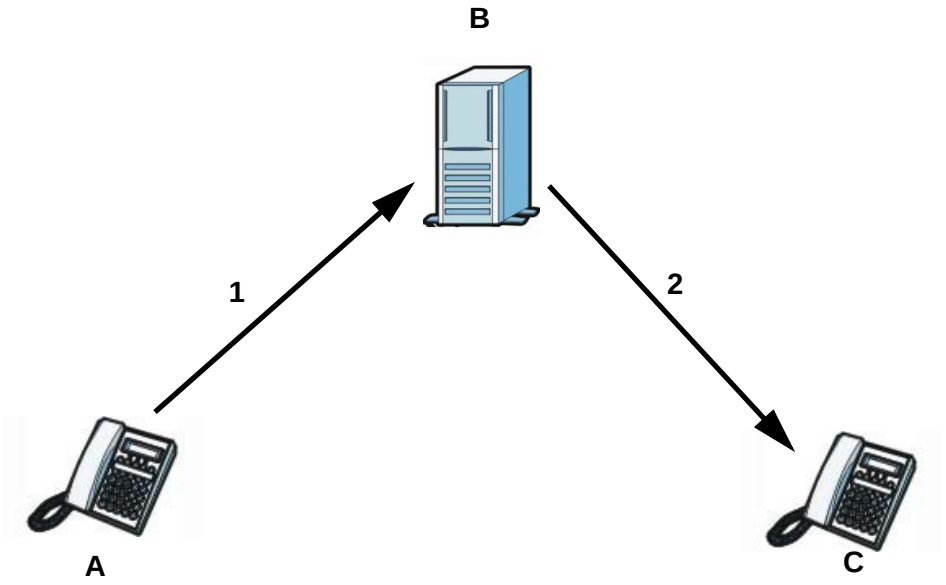
SIP Proxy Server

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

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

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

Figure 75 SIP Proxy Server



SIP Redirect Server

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

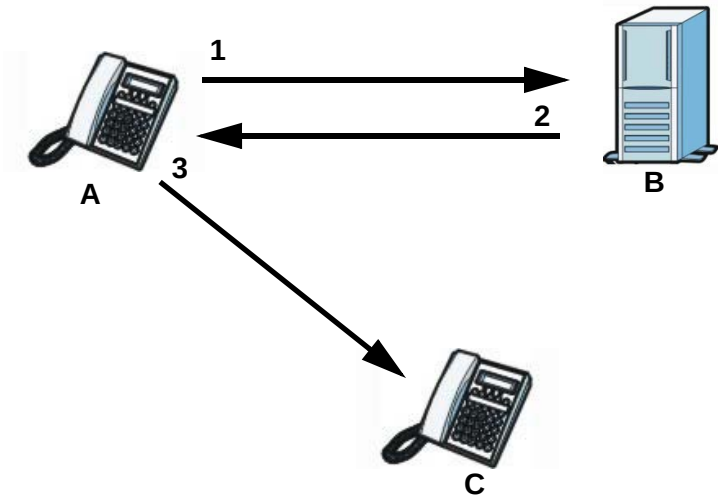
In the following example, you want to use client device **A** to call someone who is using client device **C**.

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

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

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

Figure 76 SIP Redirect Server



SIP Register Server

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

RTP

When you make a VoIP call using SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 3550 for details on RTP.

Pulse Code Modulation

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

SIP Call Progression

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

Table 44 SIP Call Progression

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

1. **A** sends a SIP INVITE request to **B**. This message is an invitation for **B** to participate in a SIP telephone call.
2. **B** sends a response indicating that the telephone is ringing.
3. **B** sends an OK response after the call is answered.
4. **A** then sends an ACK message to acknowledge that **B** has answered the call.
5. Now **A** and **B** exchange voice media (talk).
6. After talking, **A** hangs up and sends a BYE request.
7. **B** replies with an OK response confirming receipt of the BYE request and the call is terminated.

Voice Coding

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

- G.711 is a Pulse Code Modulation (PCM) waveform codec. PCM measures analog signal amplitudes at regular time intervals and converts them into digital samples. G.711 provides very good sound quality but requires 64 kbps of bandwidth.
- G.723.1 uses Low-Delay Code-Excited Linear Prediction (LD-CELP) to code audio in 30-millisecond frames. The standard supports two bitrates, 6.3 kbps and 5.3 kbps. G.723.1 provides toll-quality sound and requires very little bandwidth.
- G.726 is an Adaptive Differential PCM (ADPCM) waveform codec that uses a lower bitrate than standard PCM conversion. ADPCM converts analog audio into digital signals based on the difference between each audio sample and a prediction based on previous samples. The more similar the audio sample is to the prediction, the less space needed to describe it. G.726 operates at 16, 24, 32 or 40 kbps.
- G.729 is an Analysis-by-Synthesis (AbS) hybrid waveform codec that uses a filter based on information about how the human vocal tract produces sounds. G.729 provides good sound quality and reduces the required bandwidth to 8 kbps.

PSTN Call Setup Signaling

Dual-Tone MultiFrequency (DTMF) signaling uses pairs of frequencies (one lower frequency and one higher frequency) to set up calls. It is also known as Touch Tone®. Each of the keys on a DTMF telephone corresponds to a different pair of frequencies.

Pulse dialing sends a series of clicks to the local phone office in order to dial numbers.[1]

MWI (Message Waiting Indication)

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

1. The LTE Device does not support pulse dialing at the time of writing.

14.6.3 Phone Services Overview

Supplementary services such as call hold, call waiting, and call transfer. are generally available from your VoIP service provider. The LTE Device supports the following services:

- Call Hold
- Call Waiting
- Making a Second Call
- Call Transfer
- Three-Way Conference
- Internal Calls
- Do not Disturb

Note: To take full advantage of the supplementary phone services available through the LTE Device's phone ports, you may need to subscribe to the services from your VoIP service provider.

The Flash Key

Flashing means to press the hook for a short period of time (a few hundred milliseconds) before releasing it. On newer telephones, there should be a "flash" key (button) that generates the signal electronically. If the flash key is not available, you can tap (press and immediately release) the hook by hand to achieve the same effect. However, using the flash key is preferred since the timing is much more precise. With manual tapping, if the duration is too long, it may be interpreted as hanging up by the LTE Device.

You can invoke all the supplementary services by using the flash key.

Europe Type Supplementary Phone Services

This section describes how to use supplementary phone services with the **Europe Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command time-out (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

Table 45 European Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash		Put a current call on hold to place a second call. Switch back to the call (if there is no second call).
Flash	0	Drop the call presently on hold or reject an incoming call which is waiting for answer.
Flash	1	Disconnect the current phone connection and answer the incoming call or resume with caller presently on hold.
Flash	2	1. Switch back and forth between two calls. 2. Put a current call on hold to answer an incoming call. 3. Separate the current three-way conference call into two individual calls (one is on-line, the other is on hold).

Table 45 European Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash	3	Create three-way conference connection.
Flash	*98#	Transfer the call to another phone.

European Call Hold

Call hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key and then "2" to switch back and forth between caller **A** and **B** by putting either one on hold.

Press the flash key and then "0" to disconnect the call presently on hold and keep the current call on line.

Press the flash key and then "1" to disconnect the current call and resume the call on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

European Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to a telephone number, you will hear a call waiting tone. Take one of the following actions.

- Reject the second call.

  Press the flash key and then press "0".
- Disconnect the first call and answer the second call.

  Either press the flash key and press "1", or just hang up the phone and then answer the phone after it rings.
- Put the first call on hold and answer the second call.

  Press the flash key and then "2".

European Call Transfer

Do the following to transfer a call (that you have answered) to another phone number.

1. Press the flash key to put the caller on hold.
2. When you hear the dial tone, dial "*98#" followed by the number to which you want to transfer the call. to operate the Intercom.
3. After you hear the ring signal or the second party answers it, hang up the phone.

European Three-Way Conference

Use the following steps to make three-way conference calls.

1. When you are on the phone talking to someone, press the flash key to put the call on hold and get a dial tone.
2. Dial a phone number directly to make another call.
3. When the second call is answered, press the flash key and press “3” to create a three-way conversation.
4. Hang up the phone to drop the connection.
5. If you want to separate the activated three-way conference into two individual connections (one is on-line, the other is on hold), press the flash key and press “2”.

15

System Monitor

15.1 Overview

Use the **Traffic Status** screens to view status and log information.

15.1.1 What You Can Do in this Chapter

- Use the **LTE Status** screen to see the present LTE Status in detail (Section 15.2 on page 114).
- Use the **Log** screen to see the system logs for the categories that you select (Section 15.3 on page 115).
- Use the **WAN Traffic Status** screen to view the WAN traffic statistics (Section 15.4 on page 116).
- Use the **LAN Traffic Status** screen to view the LAN traffic statistics (Section 15.5 on page 117).
- Use the **NAT Traffic Status** screen to view the NAT status of the LTE Device's clients (Section 15.6 on page 117).
- Use the **VoIP Status** screen to view the VoIP traffic statistics (Section 15.7 on page 118).

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.

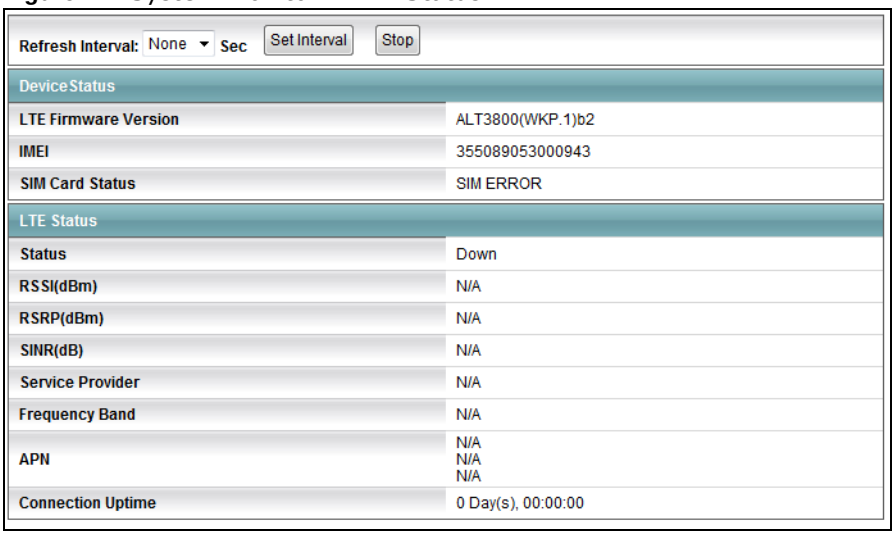
Table 46 Syslog Severity Levels

CODE	SEVERITY
0	Emergency: The system is unusable.
1	Alert: Action must be taken immediately.
2	Critical: The system condition is critical.
3	Error: There is an error condition on the system.
4	Warning: There is a warning condition on the system.
5	Notice: There is a normal but significant condition on the system.
6	Informational: The syslog contains an informational message.
7	Debug: The message is intended for debug-level purposes.

15.2 The LTE Status Screen

Click **System Monitor > LTE Status** to open the **LTE Status** screen. Use the **LTE Status** screen to see the present LTE Status in detail.

Figure 77 System Monitor > LTE Status



The following table describes the fields in this screen.

Table 47 System Monitor > LTE Status

LABEL	DESCRIPTION
Refresh Interval	Specify how often you want the LTE Device to update this screen and click **Set Interval** to apply the change. Click **Stop** to halt updating of the screen.
Device Status	
LTE Firmware Version	This is the firmware version of the LTE Device.

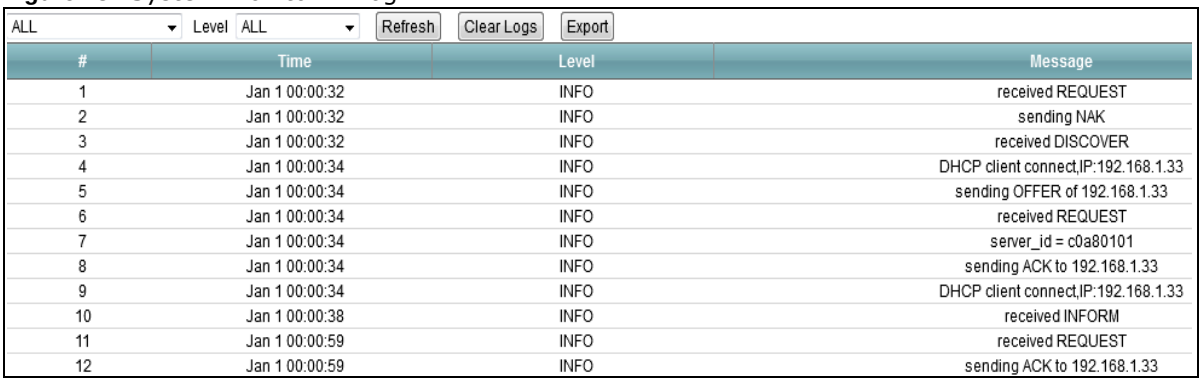
Table 47 System Monitor > LTE Status (continued)

LABEL	DESCRIPTION
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.
SIM Card Status	This displays the SIM card status.
LTE Status	
Status	This displays **Up** if there is an LTE connection, otherwise, it displays **Down**.
RSSI(dBm)	This displays the Received Signal Strength Indication (RSSI) of the LTE connection.
RSRP(dBm)	This displays the Reference Signal Received Power (RSRP) of the LTE connection.
SINR(dB)	This displays the signal-to-interference-plus-noise (SINR) ratio.
Service Provider	This displays the service provider's name of the connected LTE network.
Frequency Band	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.
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.
Connection Uptime	This displays how long the LTE connection has been available since it was last established successfully.

15.3 The Log Screen

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

Figure 78 System Monitor > Log



The following table describes the fields in this screen.

Table 48 System Monitor > Log

LABEL	DESCRIPTION
Level	Select a severity level from the 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.
Refresh	Click this to renew the log screen.

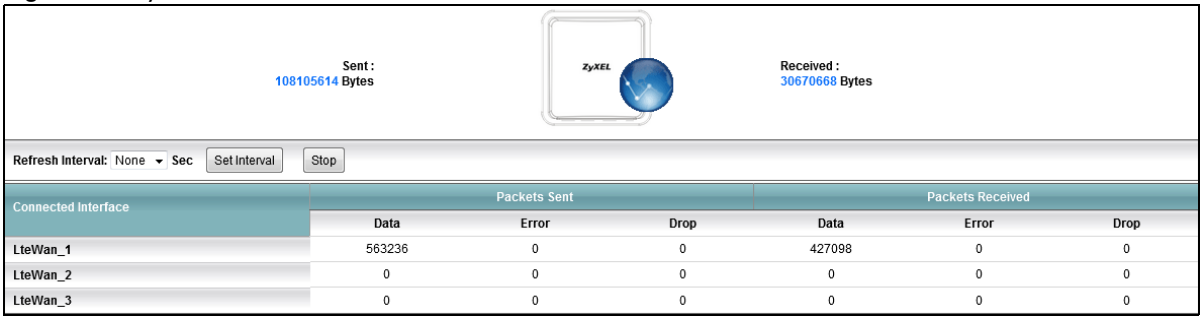
Table 48 System Monitor > Log (continued)

LABEL	DESCRIPTION
Clear Logs	Click this to delete all the logs.
Export	Click this to save a copy of the logs to your computer.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the 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.
Messages	This field states the reason for the log.

15.4 The WAN Traffic Status Screen

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

Figure 79 System Monitor > Traffic Status > WAN



The following table describes the fields in this screen.

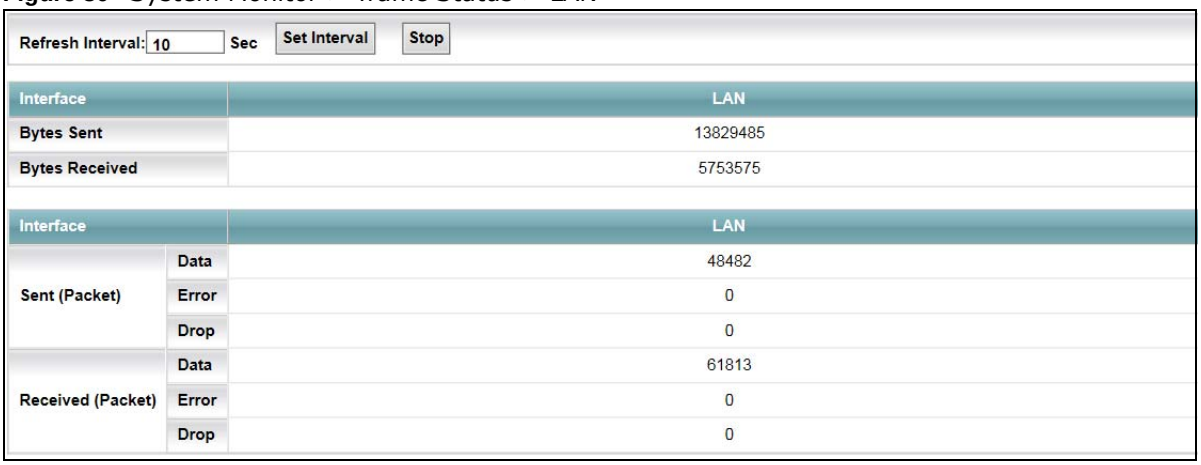
Table 49 System Monitor > Traffic Status > WAN

LABEL	DESCRIPTION
Status	This shows the number of bytes sent and received through the WAN interface of the LTE Device.
Refresh Interval	Specify how often you want the LTE Device to update this screen and click **Set Interval** to apply the change. Click **Stop** to halt updating of the screen.
Connected Interface	This shows the name of all the WAN interfaces.
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.

15.5 The LAN Traffic Status Screen

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

Figure 80 System Monitor > Traffic Status > LAN



The following table describes the fields in this screen.

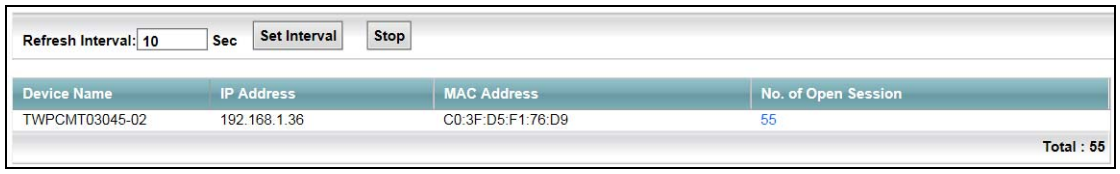
Table 50 System Monitor > Traffic Status > LAN

LABEL	DESCRIPTION
Refresh Interval	Specify how often you want the LTE Device to update this screen and click **Set Interval** to apply the change. Click **Stop** to halt updating of the screen.
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.
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.

15.6 The NAT Traffic Status Screen

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

Figure 81 System Monitor > Traffic Status > NAT



The following table describes the fields in this screen.

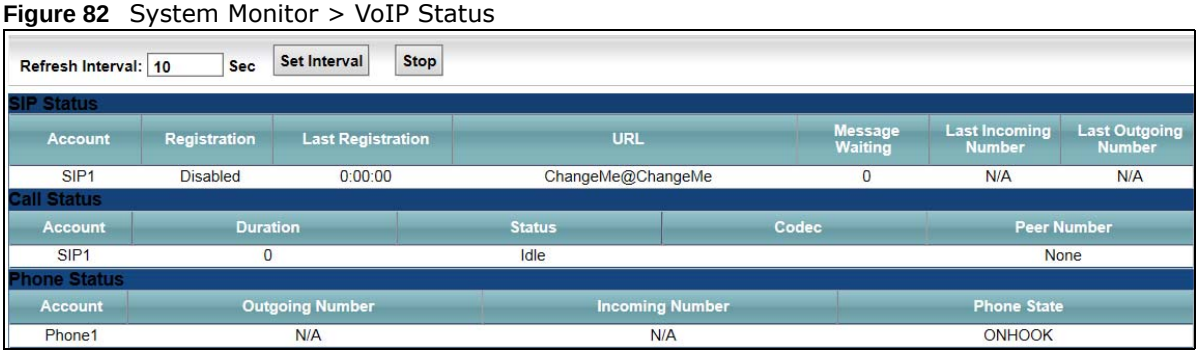
Table 51 System Monitor > Traffic Status > NAT

LABEL	DESCRIPTION
Refresh Interval	Specify how often you want the LTE Device to update this screen and click **Set Interval** to apply the change. Click **Stop** to halt updating of the screen.
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.
Total	This shows the total number of NAT sessions currently open on the LTE Device.

15.7 The VoIP Status Screen

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

Figure 82 System Monitor > VoIP Status



The following table describes the fields in this screen.

Table 52 System Monitor > VoIP Status

LABEL	DESCRIPTION
Refresh Interval	Specify how often you want the LTE Device to update this screen and click **Set Interval** to apply the change.
SIP Status	
Account	This column displays each SIP account in the LTE Device.

Table 52 System Monitor > VoIP Status (continued)

LABEL	DESCRIPTION
Registration	This field displays the current registration status of the SIP account. You can change this in the **Status** screen. **Registered** - The SIP account is registered with a SIP server. **Not Registered** - The last time the LTE Device tried to register the SIP account with the SIP server, the attempt failed. The LTE Device automatically tries to register the SIP account when you turn on the LTE Device or when you activate it. **Inactive** - The SIP account is not active. You can activate it in **VoIP > SIP > SIP Account**.
Last Registration	This field displays the last time you successfully registered the SIP account. The field is blank if you never successfully registered this account.
URL	This field displays the account number and service domain of the SIP account. You can change these in the **VoIP > SIP** screens.
Message Waiting	This field indicates whether or not there are any messages waiting for the SIP account.
Last Incoming Number	This field displays the last number that called the SIP account. The field is blank if no number has ever dialed the SIP account.
Last Outgoing Number	This field displays the last number the SIP account called. The field is blank if the SIP account has never dialed a number.
Call Status	
Account	This column displays each SIP account in the LTE Device.
Duration	This field displays how long the current call has lasted.
Status	This field displays the current state of the phone call. **Idle** - There are no current VoIP calls, incoming calls or outgoing calls being made. **Calling** - The callee's phone is ringing. **Ringing** - The phone is ringing for an incoming VoIP call. **Connecting** - The status after dialing and before the dialing tone starts. **InCall** - There is a VoIP call in progress. **Hold** - The call is reserved. **Disconnecting** - The callee's line is busy, the callee hung up or your phone was left off the hook.
Codec	This field displays what voice codec is being used for a current VoIP call through a phone port.
Peer Number	This field displays the SIP number of the party that is currently engaged in a VoIP call through a phone port.
Phone Status	
Account	This field displays the phone accounts of the LTE Device.
Outgoing Number	This field displays the SIP number that you use to make calls on this phone port.
Incoming Number	This field displays the SIP number that you use to receive calls on this phone port.
Phone State	This field shows whether or the phone connected to the subscriber port is on-hook **ONHOOK**) or off-hook **(OFFHOOK**).

16

User Account

16.1 Overview

You can configure the system password in the **User Account** screen.

16.2 The User Account Screen

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

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

Figure 83 Maintenance > User Account

The following table describes the labels in this screen.

Table 53 Maintenance > User Account

LABEL	DESCRIPTION
User Name	You can configure the password for the admin account.
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.

17

TR-069 Client

17.1 Overview

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

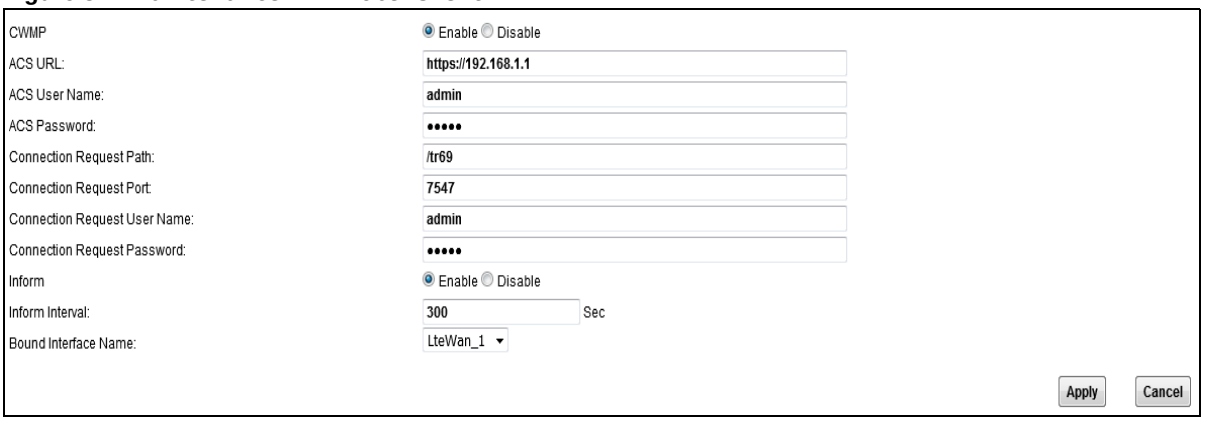
17.2 The TR-069 Client Screen

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

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

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

Figure 84 Maintenance > TR-069 Client



The following table describes the fields in this screen.

Table 54 Maintenance > TR-069 Client

LABEL	DESCRIPTION
CWMP	Select **Enable** to allow the LTE Device to be managed by a management server. Otherwise, select **Disable** to not allow the LTE Device to be managed by a management server.
ACS URL	Enter the URL or IP address of the auto-configuration server. Check with your ISP/network administrator if you are not sure of this information.
ACS User Name	Enter the TR-069 user name for authentication with the auto-configuration server.
ACS Password	Enter the TR-069 password for authentication with the auto-configuration server.
Connection Request Path	Type the IP address or domain name of the LTE Device. The management server uses this path to verify the LTE Device.
Connection Request Port	The default port for access to the LTE Device from the management server is the HTTP port, port 80. If you change it, make sure it does not conflict with another port on your network and it is recommended to use a port number above 1024 (not a commonly used port). The management server should use this port to connect to the LTE Device. You may need to alter your NAT port forwarding rules if they were already configured.
Connection Request User Name	Enter the connection request user name. When the ACS makes a connection request to the LTE Device, this user name is used to authenticate the ACS.
Connection Request Password	Enter the connection request password. When the ACS makes a connection request to the LTE Device, this password is used to authenticate the ACS.
Inform	Select **Enable** for the LTE Device to send periodic inform via TR-069 on the WAN. Otherwise, select **Disable**.
Inform Interval	Enter the time interval (in seconds) at which the LTE Device sends information to the auto-configuration server.
Bound Interface Name	Select the WAN interface the ACS is bound to.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore the screen's last saved settings.

18

System

18.1 Overview

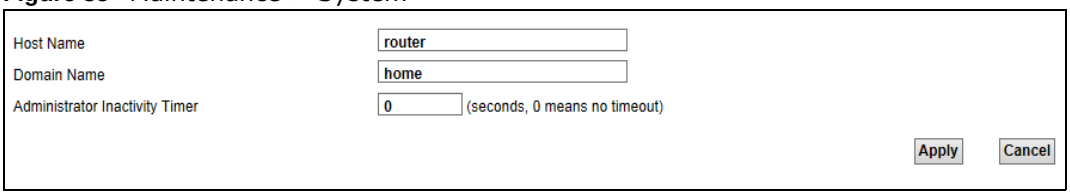
You can configure system settings, including the host name, domain name and the inactivity time-out interval in the **System** screen.

18.2 The System Screen

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

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

Figure 85 Maintenance > System



The following table describes the labels in this screen.

Table 55 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	The ISP may assign a domain name via DHCP. 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 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.

19

Time Setting

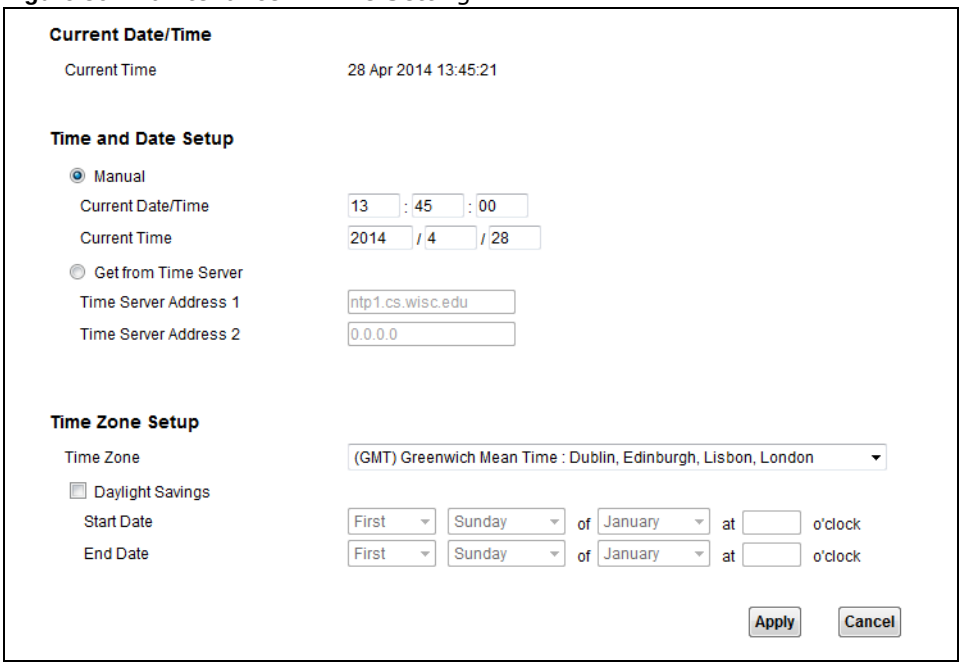
19.1 Overview

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

19.2 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 86 Maintenance > Time Setting



The following table describes the fields in this screen.

Table 56 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Current Date/Time	
Current Time	This field displays the date and time of your LTE Device.
Time and Date Setup	
Manual	Select this to enter the time and date manually in hh:mm:ss and yyyy/mm/dd format.

Table 56 Maintenance > System > Time Setting (continued)

LABEL	DESCRIPTION
Get from Time Server	Select this to have the LTE Device get the time automatically from a time server.
Time Server Address 1, 2	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).
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: 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. 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: 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. 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.
Cancel	Click **Cancel** to restore the screen’s last saved settings.

20

Log Setting

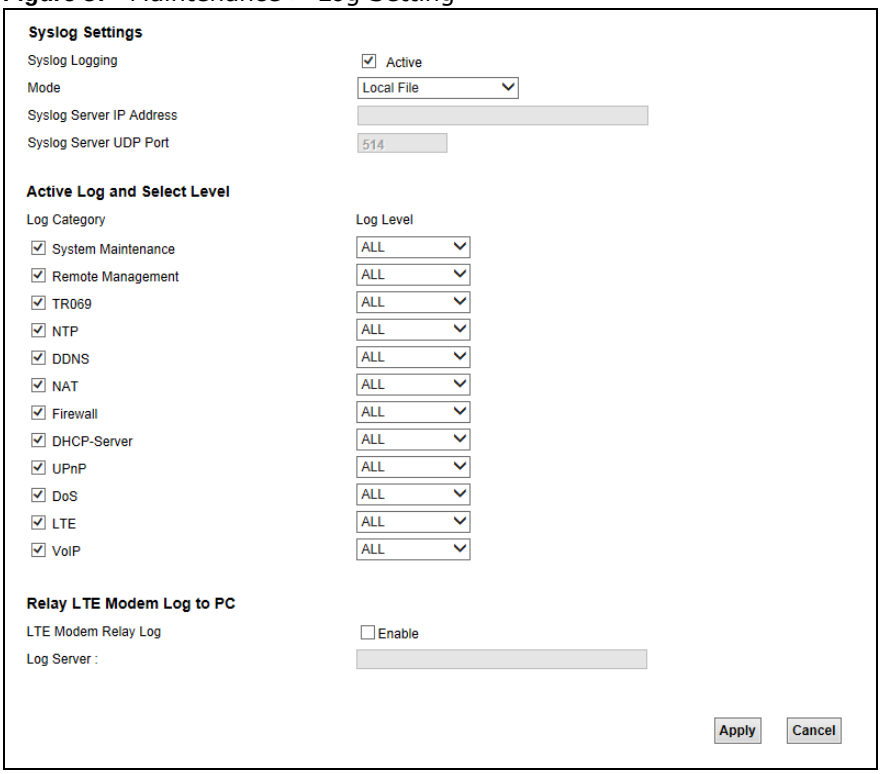
20.1 Overview

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.

20.2 The Log Setting Screen

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

Figure 87 Maintenance > Log Setting



The following table describes the fields in this screen.

Table 57 Maintenance > Log Setting

LABEL	DESCRIPTION
Syslog Settings	
Syslog Logging	Select the **Active** check box to enable syslog logging.
Mode	Select **Local File** to have the LTE Device save the log file locally. Select **Local File and Remote** to have the LTE Device save the log file locally and send it to an external syslog server.
Syslog Server IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Syslog Server 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**.
Relay LTE Modem Log to PC	
LTE Modem Relay Log	Select **Enable** to redirect LTE modem logs to the LAN computer that you specify below.
Log Server	Enter the IP address of the LAN computer that you want to use for collecting LTE modem logs.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

21

Firmware Upgrade

21.1 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.

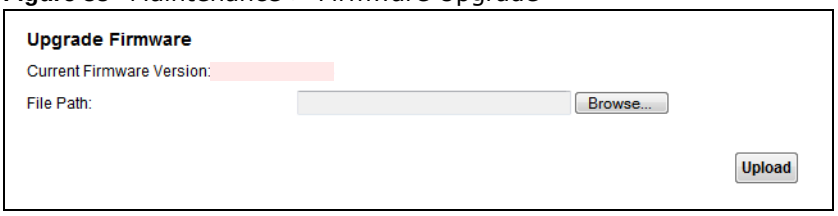
Only use firmware for your device's specific model. Refer to the label on the bottom of your LTE Device.

21.2 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 88 Maintenance > Firmware Upgrade



The following table describes the labels in this screen.

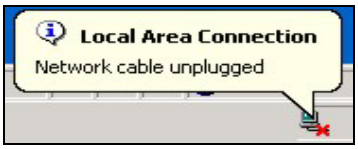
Table 58 Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Upgrade Firmware	Use these fields to upload firmware to the LTE Device.
Current Firmware Version	This is the present firmware version.
File Path	Click **Browse ...** to find the .bin file.
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.

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 89 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.

22

Backup/Restore

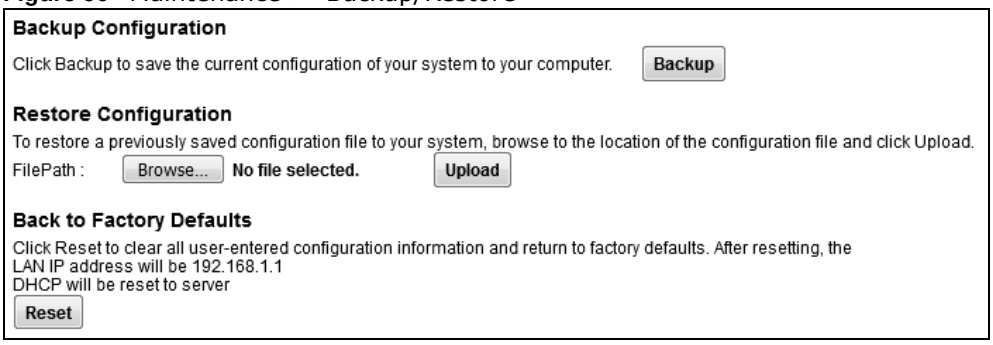
22.1 Overview

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

22.2 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 90 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 59 Restore Configuration

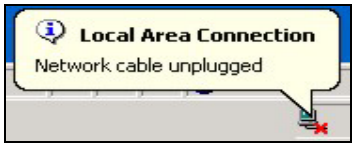
LABEL	DESCRIPTION
File Path	Click **Browse ...** to find the file.
Browse...	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click this to begin the upload process.
Reset	Click this to reset your device settings 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 91 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).

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

22.3 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.

23

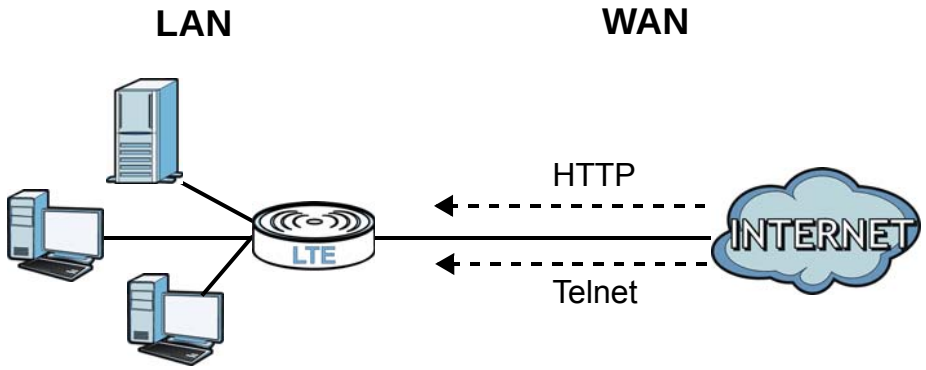
Remote Management

23.1 Overview

Remote management allows you to determine which services/protocols can access which LTE Device interface (if any) from which computers.

The following figure shows remote management of the LTE Device coming in from the WAN.

Figure 92 Remote Management From the WAN



Note: When you configure remote management to allow management from the WAN, you still need to configure a IP filter rule to allow access.

You may manage your LTE Device from a remote location via:

- Internet (WAN only)
- LAN only
- LAN and WAN
- None (Disable)

To disable remote management of a service, select **Disable** in the corresponding **Service Access** field.

23.1.1 What You Can Do in the Remote Management Screens

- Use the **WWW** screen (Section 23.2 on page 133) to configure through which interfaces and from which IP addresses users can use HTTP to manage the LTE Device.
- Use the **Telnet** screen (Section 23.3 on page 135) to configure through which interfaces and from which IP addresses users can use Telnet to manage the LTE Device.
- Use the **ICMP** screen (Section 23.4 on page 135) to set whether or not your LTE Device will respond to pings and probes for services that you have not made available.

- Use the **SSH** screen (Section 23.5 on page 136) to configure through which interfaces and from which IP addresses users can use SSH to manage the LTE Device.

23.1.2 What You Need to Know About Remote Management

Remote Management Limitations

- Remote management does not work when:
- You have not enabled that service on the interface in the corresponding remote management screen.
- You have disabled that service in one of the remote management screens.
- The IP address in the **Secured Client IP Address** field does not match the client IP address. If it does not match, the LTE Device will disconnect the session immediately.
- There is a firewall rule that blocks it.

Remote Management and NAT

When NAT is enabled:

- Use the LTE Device's WAN IP address when configuring from the WAN.
- Use the LTE Device's LAN IP address when configuring from the LAN.

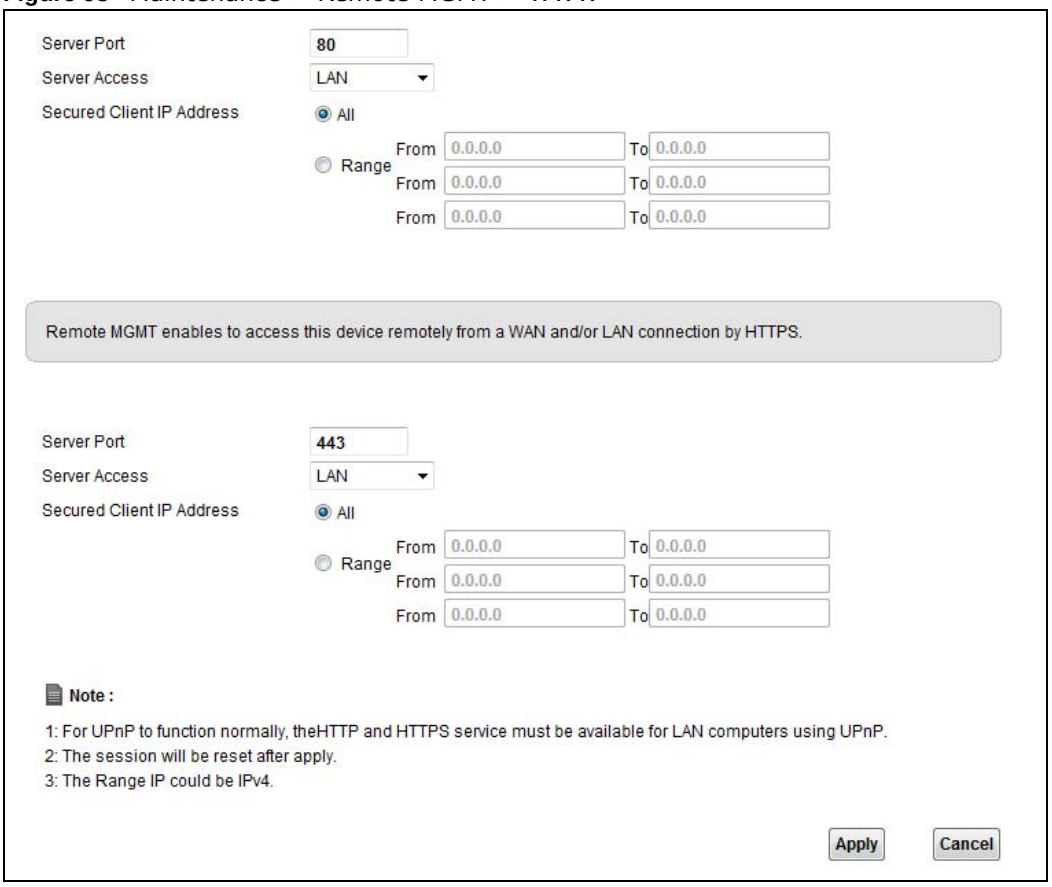
23.2 The WWW Screen

Use this screen to specify how to connect to the LTE Device from a web browser, such as Internet Explorer.

23.2.1 Configuring the WWW Screen

Click **Maintenance > Remote MGMT** to display the **WWW** screen.

Figure 93 Maintenance > Remote MGMT > WWW



The following table describes the labels in this screen.

Table 60 Maintenance > Remote MGMT > WWW

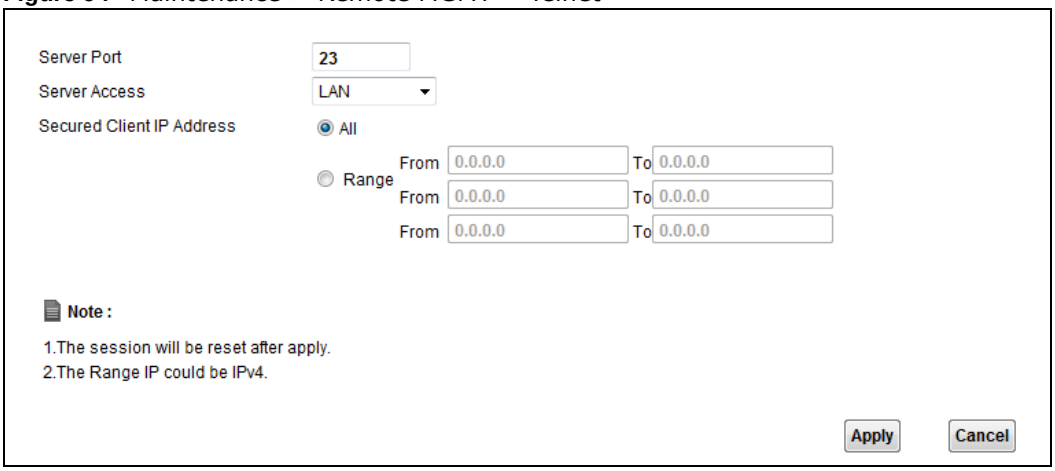
LABEL	DESCRIPTION
Server Port	This displays the service port number for accessing the LTE Device using HTTP or HTTPS. If the number is grayed out, it is not editable.
Server Access	Select the interfaces through which a computer may access the LTE Device using this service. Note: It is recommended if you are allowing WAN access even temporarily to change the default password (in **Maintenance** > **User Account**). To allow access from the WAN, you will need to configure a WAN to Router firewall rule.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the LTE Device using this service. Select **All** to allow any computer to access the LTE Device using this service. Choose **Range** to just allow the computers with an IP address in the range that you specify to access the LTE Device using this service.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

23.3 Telnet Screen

You can use Telnet to access the Device's command line interface. Specify which interfaces allow Telnet access and from which IP address the access can come.

Click **Maintenance > Remote MGMT** > **Telnet** tab to display the screen as shown.

Figure 94 Maintenance > Remote MGMT > Telnet



The following table describes the labels in this screen.

Table 61 Maintenance > Remote MGMT > Telnet

LABEL	DESCRIPTION
Server Port	This displays the service port number for accessing the LTE Device. If the number is grayed out, it is not editable.
Server Access	Select the interfaces through which a computer may access the LTE Device using this service. Note: It is recommended if you are allowing WAN access even temporarily to change the default password (in **Maintenance** > **User Account**). To allow access from the WAN, you will need to configure a WAN to Router firewall rule.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the LTE Device using this service. Select **All** to allow any computer to access the LTE Device using this service. Choose **Range** to just allow the computers with an IP address in the range that you specify to access the LTE Device using this service.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

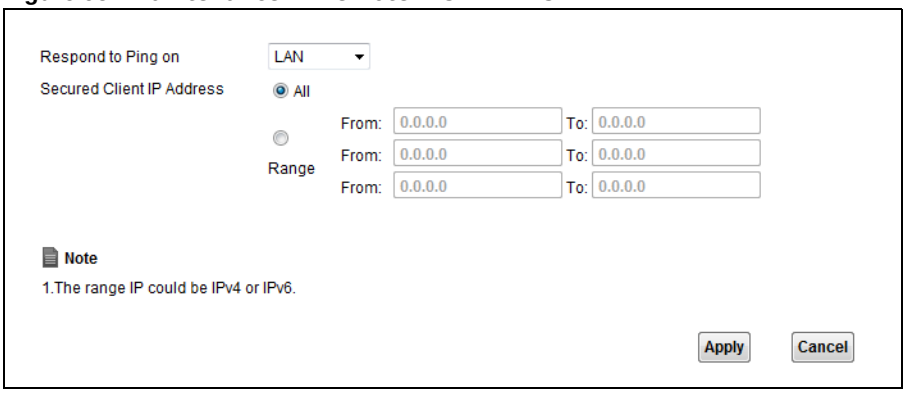
23.4 ICMP Screen

To change your LTE Device's security settings, click **Maintenance > Remote MGMT** > **ICMP**. The screen appears as shown.

If an outside user attempts to probe an unsupported port on your LTE Device, an ICMP response packet is automatically returned. This allows the outside user to know the LTE Device exists. Your LTE Device supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your LTE Device when unsupported ports are probed.

Note: If you want your device to respond to pings and requests for unauthorized services, you will also need to configure the firewall accordingly by disabling SPI.

Figure 95 Maintenance > Remote MGMT > ICMP



The following table describes the labels in this screen.

Table 62 Maintenance > Remote MGMT > ICMP

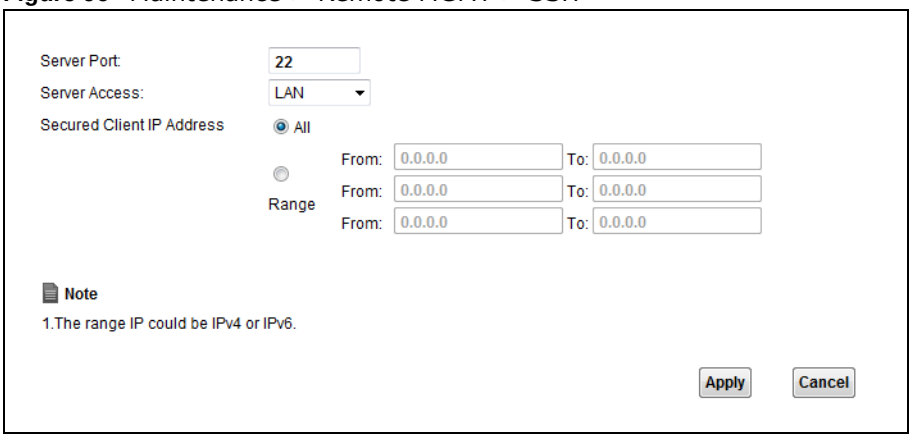
LABEL	DESCRIPTION
Respond to Ping on	The LTE Device will not respond to any incoming Ping requests when **Disable** is selected. Select **LAN** to reply to incoming LAN Ping requests. Select **WAN** to reply to incoming WAN Ping requests. Otherwise select **LAN & WAN** to reply to both incoming LAN and WAN Ping requests.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to send Ping requests to the LTE Device. Select **All** to allow any computer to send Ping requests to the LTE Device. Choose **Range** to just allow the computers with an IP address in the range that you specify to send Ping requests to the LTE Device.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

23.5 SSH Screen

You can use Secure SHell (SSH) to securely access the Device's command line interface. Specify which interfaces allow SSH access and from which IP address the access can come. SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

Click **Maintenance > Remote MGMT** > **SSH** tab to display the screen as shown.

Figure 96 Maintenance > Remote MGMT > SSH



The following table describes the labels in this screen.

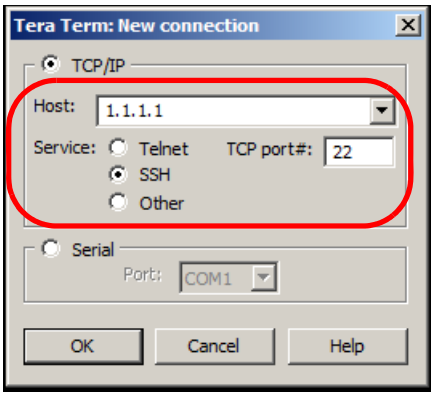
Table 63 Maintenance > Remote MGMT > SSH

LABEL	DESCRIPTION
Server Port	This displays the service port number for accessing the LTE Device. If the number is grayed out, it is not editable.
Server Access	Select the interfaces through which a computer may access the LTE Device using this service. Note: It is recommended if you are allowing WAN access even temporarily to change the default password (in **Maintenance** > **User Account**). To allow access from the WAN, you will need to configure a WAN to Router firewall rule.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the LTE Device using this service. Select **All** to allow any computer to access the LTE Device using this service. Choose **Range** to just allow the computers with an IP address in the range that you specify to access the LTE Device using this service.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

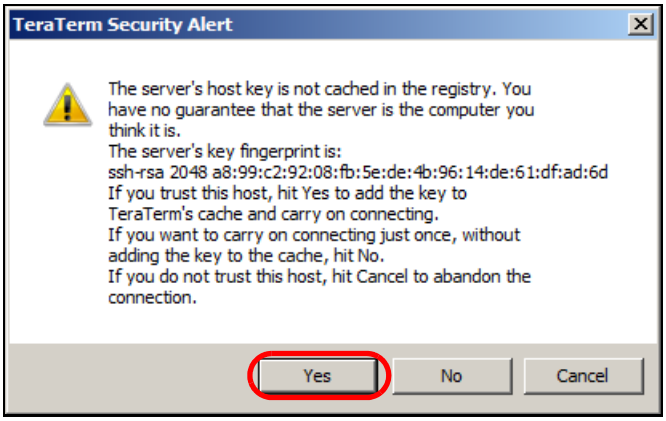
23.5.1 SSH Example

This section shows an example using a graphical interface SSH client program to remotely access the ZyXEL device. The configuration and connection steps are similar for most SSH client programs. Refer to your SSH client program user's guide.

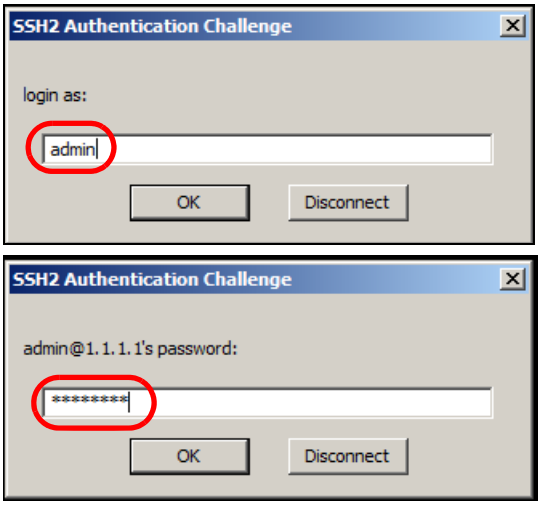
1 Enter the IP address and port number. Select **SSH**.



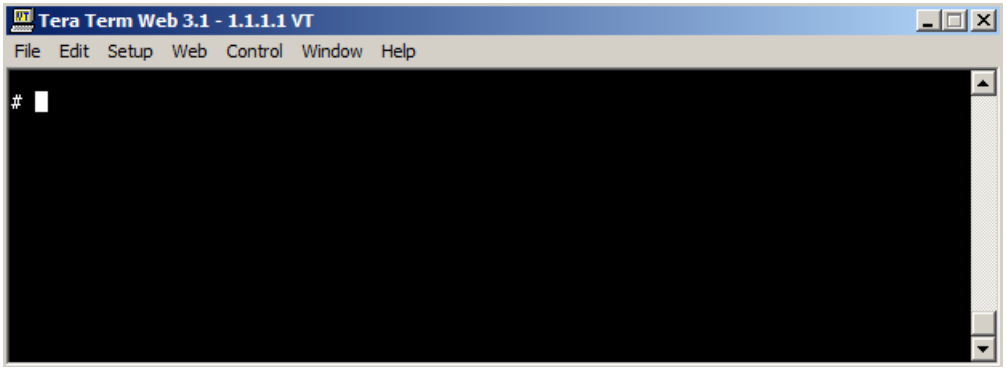
2 A window displays prompting you to store the host key in your computer. Click **Yes** to continue.



3 Enter your user name and password.



4 The command line interface displays.


Tera Term Web 3.1 - 1.1.1.1 VT
File Edit Setup Web Control Window Help
#

24

Diagnostic

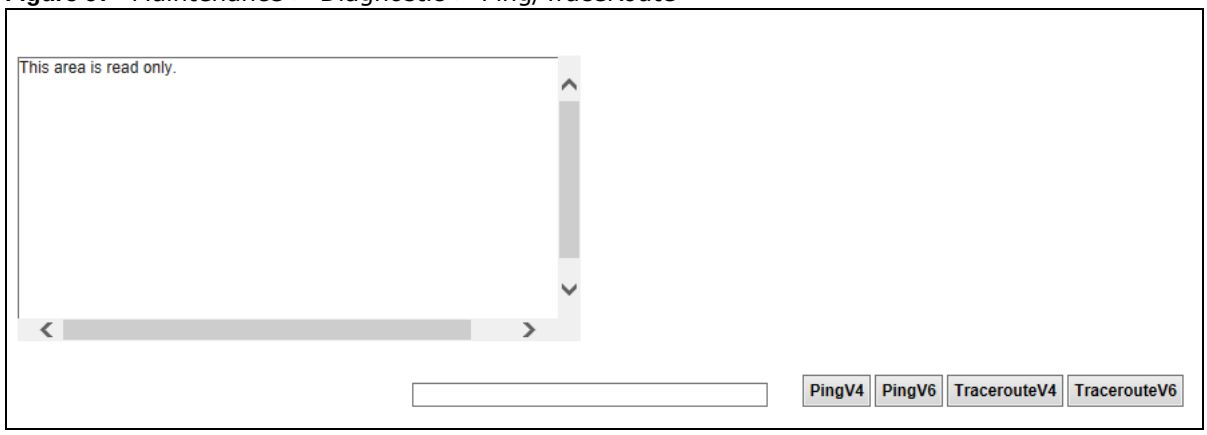
24.1 Overview

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 97 Maintenance > Diagnostic > Ping/TraceRoute



The following table describes the fields in this screen.

Table 64 Maintenance > Diagnostic > Ping/TraceRoute

LABEL	DESCRIPTION
PingV4	Type the IPv4 address of a computer that you want to ping in order to test a connection. Click **PingV4** and the ping statistics will show in the diagnostic .
PingV6	Type the IPv6 address of a computer that you want to ping in order to test a connection. Click **PingV6** and the ping statistics will show in the diagnostic .
TraceRouteV4	Click this button to perform the IPv4 traceroute function. This determines the path a packet takes to the specified host.
TraceRouteV6	Click this button to perform the IPv6 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 and Hardware Connections
- LTE Device Access and Login
- Internet Access
- Phone Calls and VoIP
- UPnP

25.2 Power and Hardware Connections

The LTE Device does not 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.

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.

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.

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

1 Make sure you are using the correct IP address.

- The default protocol is https, and the default IP address is 192.168.1.1.
- If you changed the IP address (page 40), 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, see the Quick Start Guide.

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

4 Reset the device to its factory defaults, and try to access the LTE Device with the default IP address.

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 HTTPS.

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 141.

I cannot Telnet to the LTE Device.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

25.4 Internet Access

I cannot access the Internet.

1 Check the hardware.

2 Make sure you entered your ISP account information correctly. These fields are case-sensitive, so make sure [Caps Lock] is not on.

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.

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. 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.

25.5 Phone Calls and VoIP

The telephone port won't work or the telephone lacks a dial tone.

1 Check the telephone connections and telephone wire.

I can access the Internet, but cannot make VoIP calls.

1 You can also check the VoIP status in the **System Info** screen.

2 If the VoIP settings are correct, use speed dial to make peer-to-peer calls. If you can make a call using speed dial, there may be something wrong with the SIP server, contact your VoIP service provider.

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

Customer Support

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

See *http://www.zyxel.com/homepage.shtml* and also

http://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml for the latest information.

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

Required Information

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

Corporate Headquarters (Worldwide)

Taiwan

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

Asia

China

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

India

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

Kazakhstan

- ZyXEL Kazakhstan

- http://www.zyxel.kz

Korea

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

Malaysia

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

Pakistan

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

Philippines

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

Singapore

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

Taiwan

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

Thailand

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

Vietnam

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

Europe

Austria

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

Belarus

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

Belgium

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

Bulgaria

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

Czech Republic

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

Denmark

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

Estonia

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

Finland

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

France

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

Germany

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

Hungary

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

Italy

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

Latvia

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

Lithuania

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

Netherlands

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

Norway

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

Poland

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

Romania

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

Russia

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

Slovakia

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

Spain

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

Sweden

- ZyXEL Communications

- http://www.zyxel.se

Switzerland

- Studerus AG
- http://www.zyxel.ch/

Turkey

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

UK

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

Ukraine

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

Latin America

Argentina

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

Brazil

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

Ecuador

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

Middle East

Israel

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

Middle East

- ZyXEL Communication Corporation

- http://www.zyxel.com/me/en/

North America

USA

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

Oceania

Australia

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

Africa

South Africa

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

B

Legal Information

Copyright

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Regulatory Notice and Statement

EUROPEAN UNION

The following information applies if you use the product within the European Union.

Declaration of Conformity with Regard to EU Directive 1999/5/EC (R&TTE Directive)

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

Български (Bulgarian)	С настоящото ZyXEL декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 1999/5/ЕС.
Español (Spanish)	Por medio de la presente ZyXEL declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Čeština (Czech)	ZyXEL tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/EC.
Dansk (Danish)	Undertegnede ZyXEL erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch (German)	Hiermit erklärt ZyXEL, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EU befindet.
Eesti keel (Estonian)	Käesolevaga kinnitab ZyXEL seadme seadmed vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ ZyXEL ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕC.
English	Hereby, ZyXEL declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Français (French)	Par la présente ZyXEL déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/EC.
Hrvatski (Croatian)	ZyXEL ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 1999/5/EC.
Íslenska (Icelandic)	Hér með lýsir, ZyXEL því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 1999/5/EC.
Italiano (Italian)	Con la presente ZyXEL dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.

Latviešu valoda (Latvian)	Ar šo ZyXEL deklarē, ka iekārtas atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių kalba (Lithuanian)	Šiuo ZyXEL deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, ZyXEL nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EK irányelv egyéb elõírásainak.
Malti (Maltese)	Hawnhekk, ZyXEL, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Nederlands (Dutch)	Hierbij verklaart ZyXEL dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EC.
Polski (Polish)	Niniejszym ZyXEL oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português (Portuguese)	ZyXEL declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/EC.
Română (Romanian)	Prin prezenta, ZyXEL declară că acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 1999/5/EC.
Slovenčina (Slovak)	ZyXEL týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/EC.
Slovenščina (Slovene)	ZyXEL izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/EC.
Suomi (Finnish)	ZyXEL vakuuttaa täten että laitteet tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska (Swedish)	Härmed intygar ZyXEL att denna utrustning står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EC.
Norsk (Norwegian)	Erklærer herved ZyXEL at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 1999/5/EF.

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

National Restrictions

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

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

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

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

In the majority of the EU and other European countries, the 2.4GHz and 5GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable.

The requirements for any country may evolve. ZyXEL recommends that you check with the local authorities for the latest status of their national regulations for both the 2.4GHz and 5GHz wireless LANs.

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

Belgium

The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details.

Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens.

Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails.

Denmark

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

I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.

Italy

This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check http://www.sviluppoeconomico.gov.it/ for more details.

Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all 'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare http://www.sviluppoeconomico.gov.it/ per maggiori dettagli.

Latvia

The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details.

2.4 GHz frekvenèu joslas izmantoðanai ârpus telpâm nepiecieðama atïauja no Elektronisko sakaru direkcijas. Vairâk informâcijas: http://www.esd.lv.

Notes:

1. Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 1999/5/EC has also been implemented in those countries.

2. The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used(specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CZ	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Switzerland	CH
Ireland	IE	Sweden	SE
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Safety Warnings

- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Do not expose your device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do not open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do not allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Please use the provided or designated connection cables/power cables/ adaptors. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adapter or cord is prohibited. Contact your local vendor to order a new one.
- CAUTION: Risk of explosion if battery is replaced by an incorrect type, dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- Do not obstruct the device ventilation slots, as insufficient airflow may harm your device.

The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,

- For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;
- For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.

Environment Statement

ErP (Energy-related Products)

ZyXEL products put on the EU market in compliance with the requirement of the European Parliament and the Council published Directive 2009/125/EC establishing a framework for the setting of ecodesign requirements for energy-related products (recast), so called

as "ErP Directive (Energy-related Products directive) as well as ecodesign requirement laid down in applicable implementing measures, power consumption has satisfied regulation requirements which are:

Network standby power consumption < 12W, and/or

Off mode power consumption < 0.5W, and/or

Standby mode power consumption < 0.5W.

Wireless setting, please refer to "Wireless" chapter for more detail.

European Union - Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

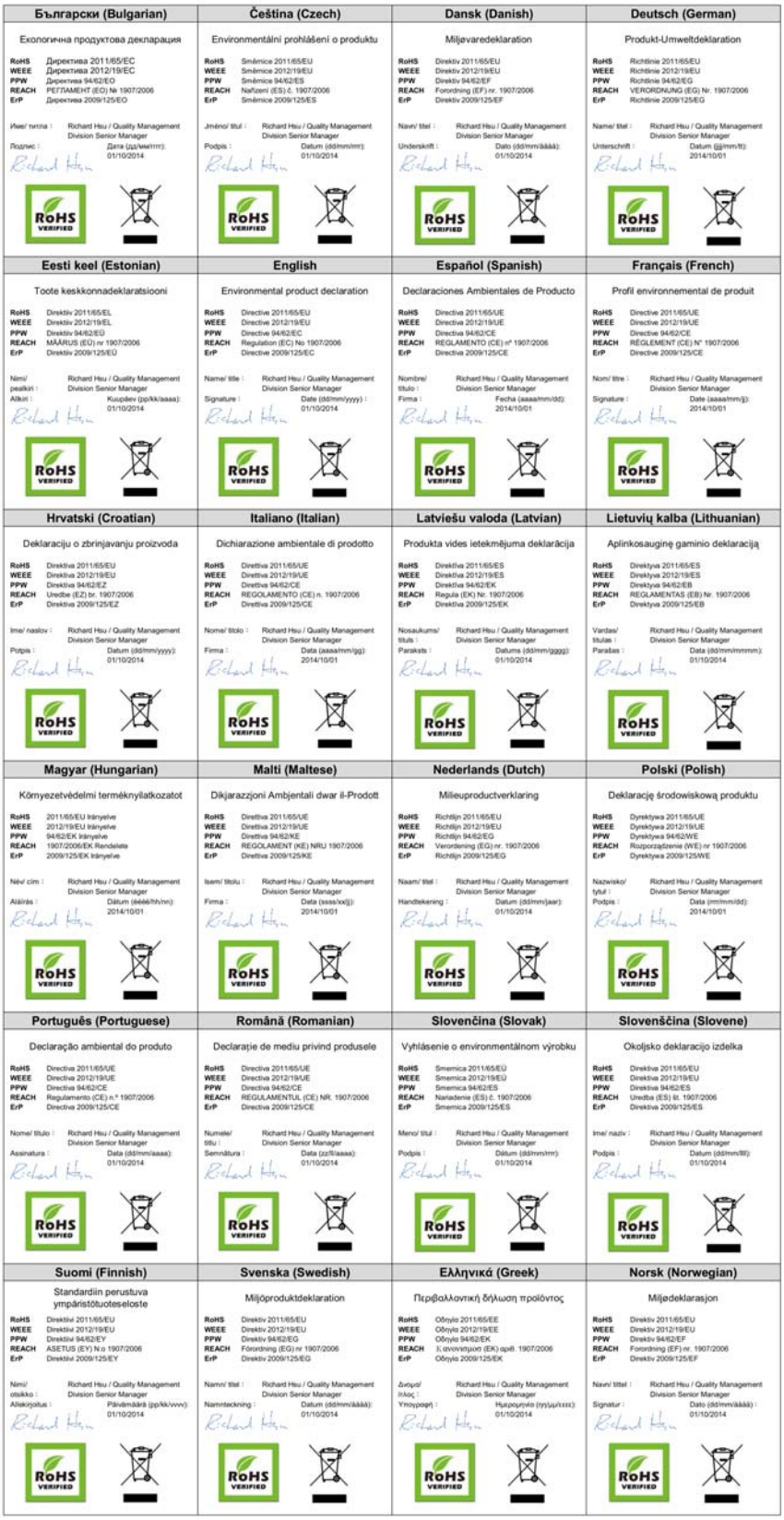
El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado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

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.

Environmental Product Declaration



Български (Bulgarian)

Екологична продуктова декларация

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

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

Čeština (Czech)

Environmentální prohlášení o produktu

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

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

Dansk (Danish)

Miljøvaredeklaration

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

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

Deutsch (German)

Produkt-Umweltdeklaration

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

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

Eesti keel (Estonian)

Toote keskkonnadeklaratsiooni

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

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

English

Environmental product declaration

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

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

Español (Spanish)

Declaraciones Ambientales de Producto

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

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

Français (French)

Profil environnemental de produit

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

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

Hrvatski (Croatian)

Deklaraciju o zbrinjavanju proizvoda

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

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

Italiano (Italian)

Dichiarazione ambientale di prodotto

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

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

Latviešu valoda (Latvian)

Produkta vides ietekmējuma deklarācija

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

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

Lietuvių kalba (Lithuanian)

Aplinkosauginę gaminio deklaraciją

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

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

Magyar (Hungarian)

Környezetvédelmi terméknyilatkozatot

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

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

Malti (Maltese)

Dikjarazzjoni Ambjentali dwar il-Prodott

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

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

Nederlands (Dutch)

Milieuproductverklaring

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

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

Polski (Polish)

Deklarację środowiskową produktu

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

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

Português (Portuguese)

Declaração ambiental do produto

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

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

Română (Romanian)

Declarație de mediu privind produsele

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

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

Slovenčina (Slovak)

Vyhlásenie o environmentálnom výrobku

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

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

Slovenščina (Slovene)

Okoljsko deklaracijo izdelka

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

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

Suomi (Finnish)

Standardiin perustuva ympäristötuoteseloste

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

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

Svenska (Swedish)

Miljöproduktdeklaration

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

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

Ελληνικά (Greek)

Περιβαλλοντική δήλωση προϊόντος

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

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

Norsk (Norwegian)

Miljødeklarasjon

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

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

台灣

以下訊息僅適用於產品具有無線功能且銷售至台灣地區

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司，商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信法規定作業之無線電通信。 低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

用 20cm 計算 MPE 能符合 1 mW/cm2

電磁波曝露量 MPE 標準值 1mW/cm2，送測產品實測值為： _XX_mW/cm2

無線資訊傳輸設備忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用， 俟無干擾之虞，始得繼續使用。

無線資訊傳設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作， 發射的信號應維持於操作頻帶中

以下訊息僅適用於產品操作於 5.25-5.35 秭赫頻帶內並銷售至台灣地區

- 在 5.25-5.35 秭赫頻帶內操作之無線資訊傳輸設備，限於室內使用。

以下訊息僅適用於產品屬於專業安裝並銷售至台灣地區

- 本器材須經專業工程人員安裝及設定，始得 設置使用，且不得直接販售給一般消費者

安全警告

為了您的安全，請先閱讀以下警告及指示：

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
- 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝，使用或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請插在正確的電壓供給插座 (如：北美 / 台灣電壓 110V AC，歐洲是 230V AC)。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
  - 對永久連接之設備， 在設備外部須安裝可觸及之斷電裝置；
  - 對插接式之設備， 插座必須接近安裝之地點而且是易於觸及的。

Viewing Certifications

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

ZyXEL Limited Warranty

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

Note

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

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

Registration

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

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W