

User's Guide

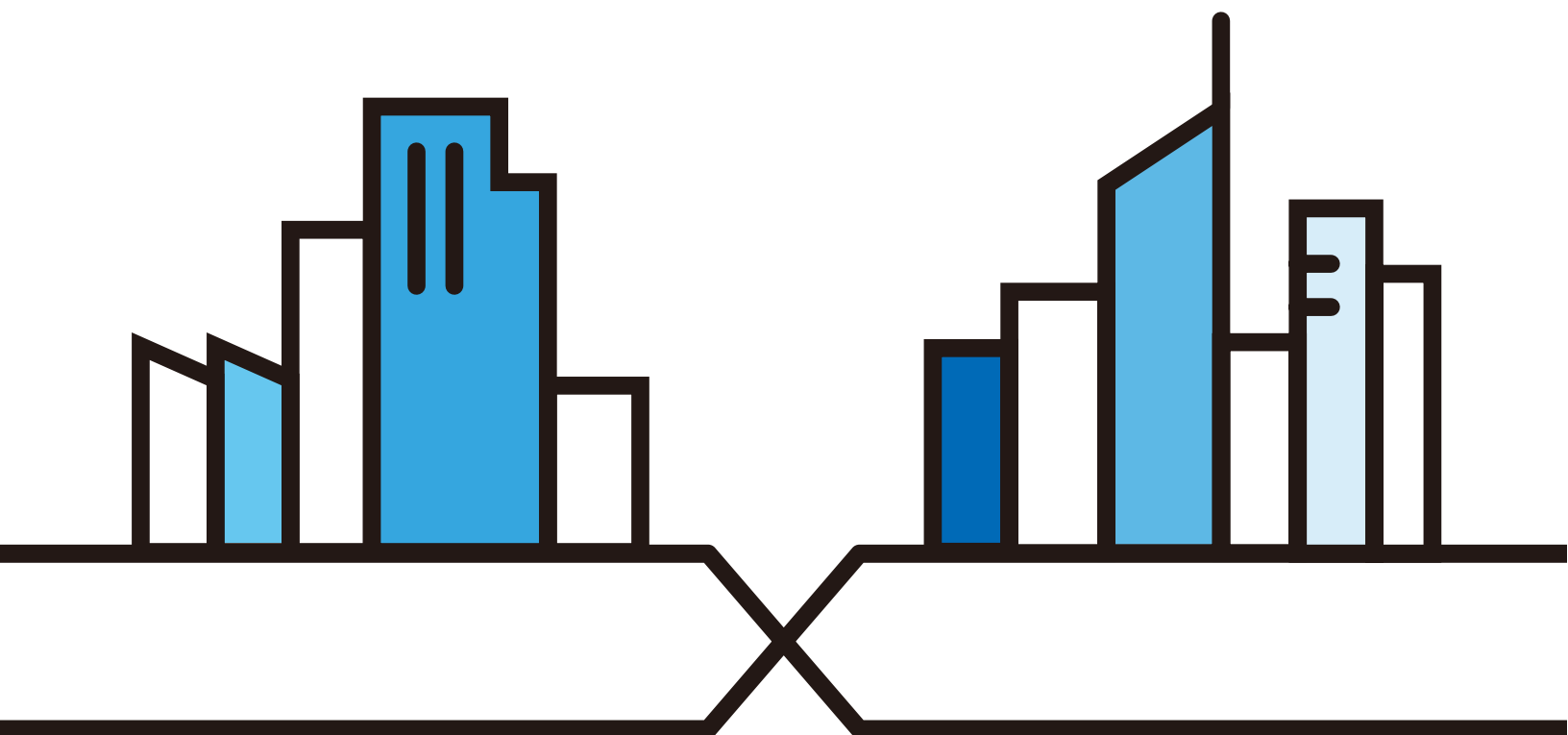
LTE7240-M403

LTE Outdoor CPE

Default Login Details

LAN IP Address	http://192.168.1.1
Login	admin
Password	See the device label

Version 1.00 Edition 1, 1/2019



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

This is a User's Guide for the LTE7240-M403. Screenshots and graphics in this book may differ slightly from what you see 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 managed device.

- More Information

Go to **support.zyxel.com** to find other information on the LTE7240.



Document Conventions

Warnings and Notes

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

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








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

Syntax Conventions

- The LTE7240-M403 in this user's guide may be referred to as the "Zyxel Device" in this guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Network Setting** > **Broadband** > **SIM** means you first click **Network Setting** in the navigation panel, then the **Broadband** sub menu and finally the **SIM** tab to get to that screen.

Icons Used in Figures

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

Zyxel Device 	Generic Router 	Switch 
Server 	Firewall 	USB Storage Device 
Printer 		

Contents Overview

User's Guide	11
Introduction	12
Introducing the Web Configurator	15
Technical Reference	22
Connection Status and System Info	23
Broadband	28
Wireless	39
Home Networking	63
Routing	77
Network Address Translation (NAT)	85
DNS Setup	96
Firewall	100
Certificates	112
System Monitor	122
ARP Table	127
Routing Table	129
System	131
User Account	132
Remote Management	134
TR-069 Client	137
Time Setting	139
E-mail Notification	141
Log Setting	143
Firmware Upgrade	145
Backup/Restore	147
Diagnostic	150
Troubleshooting	152

Table of Contents

Document Conventions	3
Contents Overview	4
Table of Contents	5
Part I: User's Guide.....	11
Chapter 1	
Introduction	12
1.1 Overview	12
1.2 Application for the Zyxel Device	12
1.3 Managing the Zyxel Device	12
1.4 Good Habits for Managing the LTE Device	13
1.5 LEDs (Lights)	13
1.6 The RESET Button	14
Chapter 2	
Introducing the Web Configurator	15
2.1 Overview	15
2.1.1 Accessing the Web Configurator	15
2.2 Quick Start Wizard	16
2.2.1 Time Zone	16
2.2.2 Wireless Setup	17
2.3 The Web Configurator Layout	19
2.3.1 Title Bar	20
2.3.2 Main Window	21
Part II: Technical Reference.....	22
Chapter 3	
Connection Status and System Info	23
3.1 Overview	23
3.2 The Connection Status Screen	23
3.3 The Status Screen	25

Chapter 4	
Broadband.....	28
4.1 Overview	28
4.1.1 What You Can Do in this Chapter	28
4.1.2 What You Need to Know	28
4.1.3 Before You Begin	29
4.2 Cellular WAN Screen	29
4.3 SIM Configuration Screen	30
4.4 The Band Configuration Screen	32
4.5 PLMN Configuration Screen	33
4.6 IP Passthrough Screen	34
4.7 Detail Statistics Screen	35
 Chapter 5	
Wireless	39
5.1 Overview	39
5.1.1 What You Can Do in this Chapter	39
5.1.2 What You Need to Know	39
5.2 The General Screen	40
5.2.1 No Security	42
5.2.2 More Secure (WPA2-PSK)	42
5.3 MAC Authentication	44
5.4 The WPS Screen	45
5.5 The WMM Screen	47
5.6 The Others Screen	48
5.7 Technical Reference	50
5.7.1 WiFi Network Overview	50
5.7.2 Additional Wireless Terms	52
5.7.3 WiFi Security Overview	52
5.7.4 Signal Problems	54
5.7.5 BSS	54
5.7.6 Preamble Type	55
5.7.7 WiFi Protected Setup (WPS)	55
 Chapter 6	
Home Networking.....	63
6.1 Overview	63
6.1.1 What You Can Do in this Chapter	63
6.1.2 What You Need To Know	63
6.2 The LAN Setup Screen	64
6.3 The Static DHCP Screen	66
6.3.1 Before You Begin	66
6.4 The UPnP Screen	68

6.5 Technical Reference	69
6.6 Turning on UPnP in Windows 7 Example	70
6.6.1 Auto-discover Your UPnP-enabled Network Device	71
6.7 Web Configurator Easy Access	74
Chapter 7	
Routing	77
7.1 Overview	77
7.2 Configuring Static Route	77
7.2.1 Add/Edit Static Route	78
7.3 The DNS Route Screen	80
7.3.1 Add/Edit DNS Route	80
7.4 The Policy Route Screen	81
7.4.1 Add/Edit Policy Route	83
7.5 RIP	84
7.5.1 The RIP Screen	84
Chapter 8	
Network Address Translation (NAT)	85
8.1 Overview	85
8.1.1 What You Can Do in this Chapter	85
8.1.2 What You Need To Know	85
8.2 The Port Forwarding Screen	86
8.2.1 The Port Forwarding Screen	87
8.2.2 Add/Edit Port Forwarding	88
8.3 The Applications Screen	89
8.3.1 The Applications Add/Edit Screen	90
8.4 The Port Triggering Screen	91
8.4.1 Add/Edit Port Triggering Rule	93
8.5 The DMZ Screen	94
8.6 The ALG Screen	95
Chapter 9	
DNS Setup	96
9.1 Overview	96
9.1.1 What You Can Do in this Chapter	96
9.1.2 What You Need To Know	96
9.2 The DNS Entry Screen	96
9.2.1 Add/Edit DNS Entry	97
9.3 The Dynamic DNS Screen	98
Chapter 10	
Firewall	100

10.1 Overview	100
10.1.1 What You Need to Know About Firewall	100
10.2 The Firewall Screen	101
10.2.1 What You Can Do in this Chapter	101
10.3 The Firewall General Screen	101
10.4 The Protocol (Customized Services) Screen	102
10.4.1 Add Customized Service	103
10.5 The Access Control (Rules) Screen	104
10.5.1 Access Control Add New ACL Rule Screen	105
10.5.2 Scheduler Rules	107
10.6 DoS Screen	108
10.7 Firewall Technical Reference	109
10.7.1 Firewall Rules Overview	109
10.7.2 Guidelines For Enhancing Security With Your Firewall	110
10.7.3 Security Considerations	110
Chapter 11	
Certificates	112
11.1 Overview	112
11.1.1 What You Can Do in this Chapter	112
11.2 Local Certificates	112
11.2.1 Create Certificate Request	113
11.2.2 View Certificate Request	114
11.3 Trusted CA	116
11.4 Import Trusted CA Certificate	117
11.5 View Trusted CA Certificate	118
11.6 Certificates Technical Reference	119
11.6.1 Verifying a Certificate	120
Chapter 12	
System Monitor	122
12.1 Overview	122
12.1.1 What You Can Do in this Chapter	122
12.2 The System Log Screen	122
12.3 The Security Log Screen	123
12.4 The WAN Traffic Status Screen	124
12.5 The LAN Traffic Status Screen	125
Chapter 13	
ARP Table	127
13.1 ARP Table Overview	127
13.1.1 How ARP Works	127
13.2 ARP Table Screen	128

Chapter 14	
Routing Table.....	129
14.1 Routing Table Overview	129
14.2 The Routing Table Screen	129
Chapter 15	
System.....	131
15.1 System Screen Overview	131
15.2 The System Screen	131
Chapter 16	
User Account.....	132
16.1 User Account Overview	132
16.2 The User Account Screen	132
16.2.1 Add/Edit User Account	133
Chapter 17	
Remote Management.....	134
17.1 Overview	134
17.2 The MGMT Services Screen	134
17.3 The Trust Domain Screen	135
17.4 The Add Trust Domain Screen	136
Chapter 18	
TR-069 Client.....	137
18.1 Overview	137
18.2 The TR-069 Client Screen	137
Chapter 19	
Time Setting	139
19.1 Overview	139
19.2 The Time Setting Screen	139
Chapter 20	
E-mail Notification	141
20.1 E-mail Notification Overview	141
20.2 The E-mail Notification Screen	141
20.2.1 E-mail Notification Add/Edit	142
Chapter 21	
Log Setting	143
21.1 Log Setting Overview	143
21.2 The Log Setting Screen	143

Chapter 22	
Firmware Upgrade	145
22.1 Overview	145
22.2 The Firmware Upgrade Screen	145
Chapter 23	
Backup/Restore	147
23.1 Backup/Restore Overview	147
23.2 The Backup/Restore Screen	147
23.3 The Reboot Screen	148
Chapter 24	
Diagnostic.....	150
24.1 Diagnostic Overview	150
24.2 The Ping/TraceRoute/Nslookup Test Screen	150
Chapter 25	
Troubleshooting.....	152
25.1 Overview	152
25.2 Power and Hardware Connections	152
25.3 Zyxel Device Access and Login	152
25.4 Internet Access	154
25.5 UPnP	155
Appendix A Customer Support	156
Appendix B Legal Information	162
Index	170

PART I

User's Guide

CHAPTER 1

Introduction

1.1 Overview

The Zyxel Device is an outdoor LTE (Long Term Evolution) router that also supports a Gigabit Ethernet connection. The Zyxel Device also includes a robust firewall that uses Stateful Packet Inspection (SPI) technology and protects against Denial of Service (DoS) attacks.

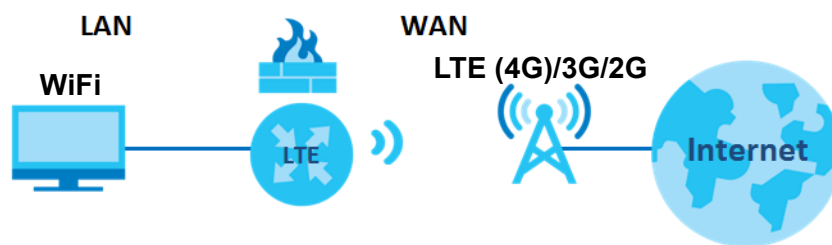
Your Zyxel Device is easy to install, configure and use. The embedded Web-based Configurator enables simple, straightforward management and maintenance. Just insert the SIM card (that has Internet access settings) and make the hardware connections. See the Quick Start Guide for how to do the hardware installation, wall mounting, Internet setup and turning on/off WiFi (optional).

1.2 Application for the Zyxel Device

Internet Access

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

Figure 1 Zyxel Device's Internet Access Application



1.3 Managing the Zyxel Device

Use the Web Configurator for everyday management of the Zyxel Device using a (supported) web browser.

1.4 Good Habits for Managing the LTE Device

Do the following things regularly to make the Zyxel Device more secure and to manage the Zyxel 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). Refer to [Section 23.2 on page 147](#). 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 Zyxel Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the Zyxel Device. You could simply restore your last configuration.

1.5 LEDs (Lights)

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

Table 1 LTE7240-M403 LED Descriptions

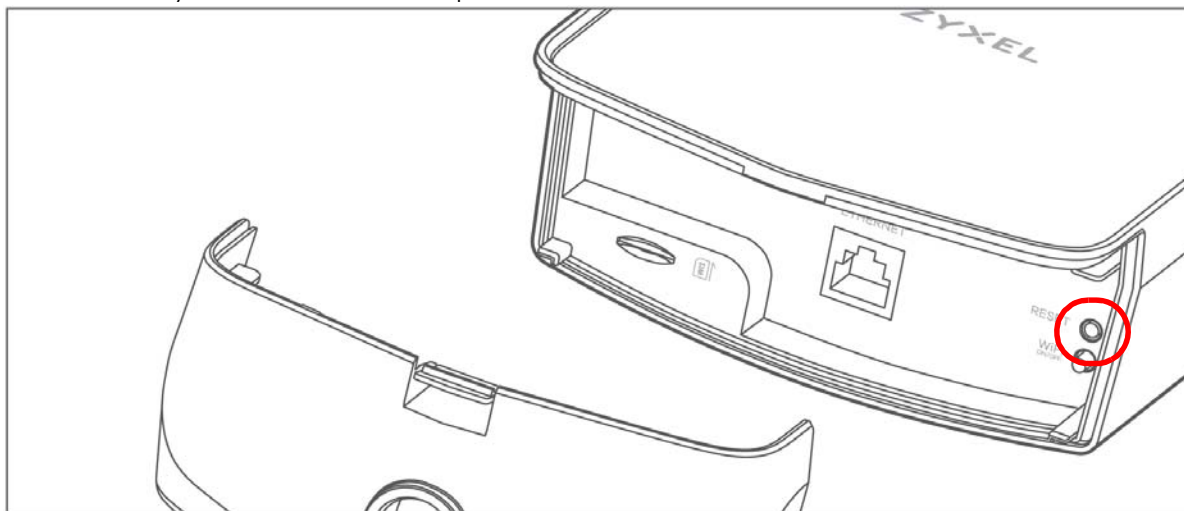
LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The Zyxel Device is receiving power and ready for use.
		Blinking	The Zyxel Device is booting or self-testing.
		Off	The Zyxel Device is not receiving power.
ETHERNET	Green	On	The Zyxel Device has a successful 10/100/1000 Mbps Ethernet connection with a device on the Local Area Network (LAN).
		Off	The Zyxel Device does not have an Ethernet connection with the LAN.
LTE/3G/2G	Green	On	The Zyxel Device is registered and successfully connected to a 4G network.
		Blinking (slow)	The Zyxel Device is connected to a 3G/2G network.
		Blinking (fast)	The Zyxel Device is trying to connect to a 4G/3G/2G network.
		Off	There is no service.
WLAN	Green	On	The wireless network is activated.
		Off	The wireless network is not activated.
Signal Strength	Green	On	The signal strength is Excellent.
	Orange	On	The signal strength is Fair.
	Red	On	The signal strength is Poor.
		Blinking	There is no SIM card inserted, the SIM card is invalid, the PIN code is not correct.
		Off	There is no signal or the signal strength is below the Poor level.

Note: Blinking (slow) means the LED blinks once per second. Blinking (fast) means the LED blinks once per 0.2 second.

1.6 The RESET Button

If you forget your password or cannot access the Web Configurator, you will need to use the RESET button of the device as shown in the following figure to reload the factory-default configuration file. This means that you will lose all configurations that you had previously saved, the password will be reset to **1234** and the IP address will be reset to **192.168.1.1**.

Note: Use only insulator material to press the RESET button.



- 1 Make sure the Zyxel Device is connected to power and **POWER** LED on the left is on.
- 2 To set the device back to the factory default settings, press the **RESET** button for 5 seconds.

Note: If you press the RESET button for more than 2 seconds but less than 5 seconds, it will cause the system to reboot.

CHAPTER 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:

- Internet Explorer 8.0 and later versions
- Chrome 40 and later versions
- Mozilla Firefox 36 and later versions
- Safari 7.0 and later versions

The recommended screen resolution is 1024 by 768 pixels.

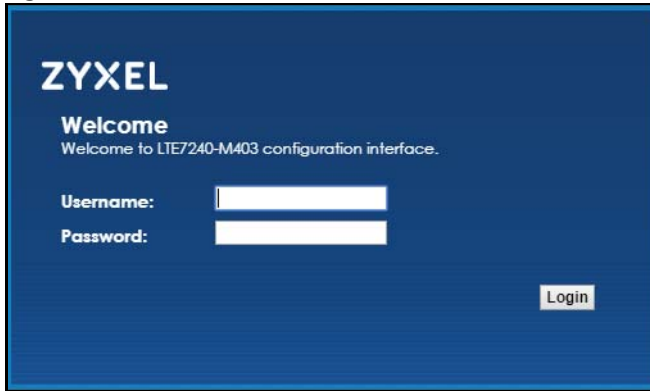
In order to use the Web Configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows 10.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

2.1.1 Accessing the Web Configurator

- 1 Make sure your Zyxel Device hardware is properly connected (refer to the Quick Start Guide).
- 2 Launch your web browser.
- 3 Type "192.168.1.1" as the URL.
- 4 A password screen displays. Welcome to the Zyxel Device configuration interface. Type "admin" as the default Username and "1234" as the default password to access the Web Configurator. Then click **Login**. If you have changed the password, enter your password and click **Login**.

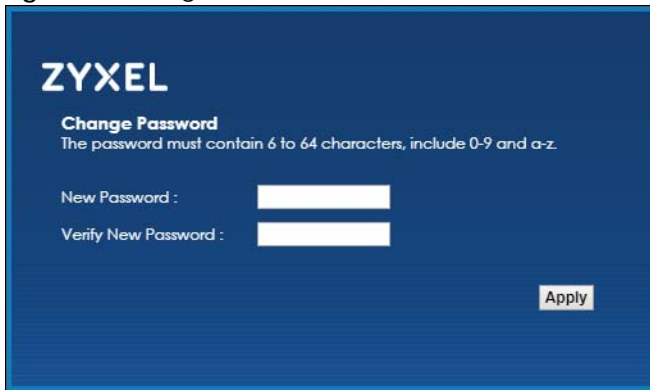
Figure 2 Password Screen

The image shows the ZyXEL login screen. It has a dark blue background with the ZyXEL logo at the top left. Below the logo, it says "Welcome" and "Welcome to LTE7240-M403 configuration interface." There are two white input fields: one for "Username:" and one for "Password:". A "Login" button is located at the bottom right of the form area.

Note: For security reasons, the Zyxel 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. The new password must contain 6 to 64 characters (include 0-9 and a-z), retype it to confirm and click **Apply**.

Figure 3 Change Password Screen

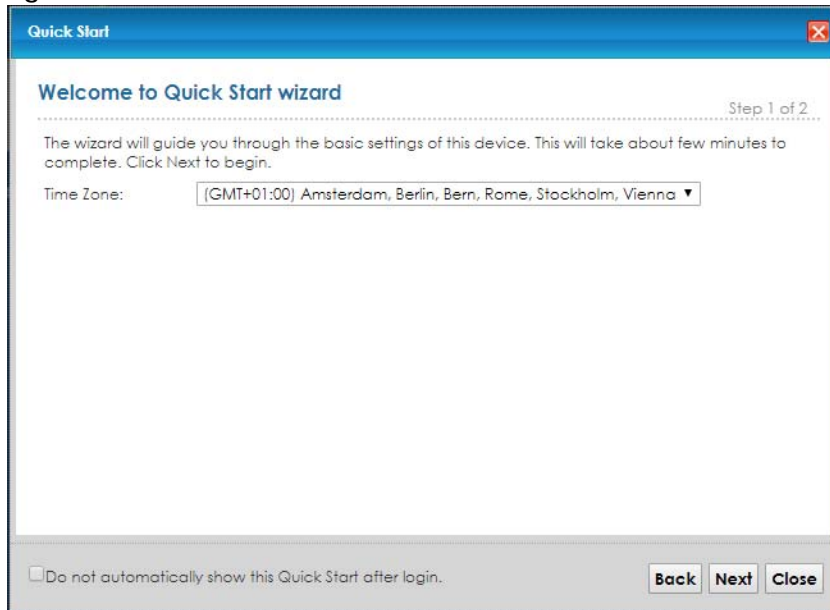
The image shows the ZyXEL change password screen. It has a dark blue background with the ZyXEL logo at the top left. Below the logo, it says "Change Password" and "The password must contain 6 to 64 characters, include 0-9 and a-z." There are two white input fields: one for "New Password :" and one for "Verify New Password :". An "Apply" button is located at the bottom right of the form area.

2.2 Quick Start Wizard

The **Quick Start** screen displays the first time after you change the password in your device's Web Configurator. You can also click the **Quick Start** icon in the **Connection Status** screen to open the **Quick Start** screens. See [Section 2.3 on page 19](#) for more information. The wizard will guide you through the basic settings of the Zyxel Device. This will take about a few minutes to complete. You can also click **Close** to leave the **Wizard** screens without saving your changes.

2.2.1 Time Zone

Select the time zone where your device is located. Click **Next**.

Figure 4 Welcome to Quick Start Wizard Screen > Time Zone

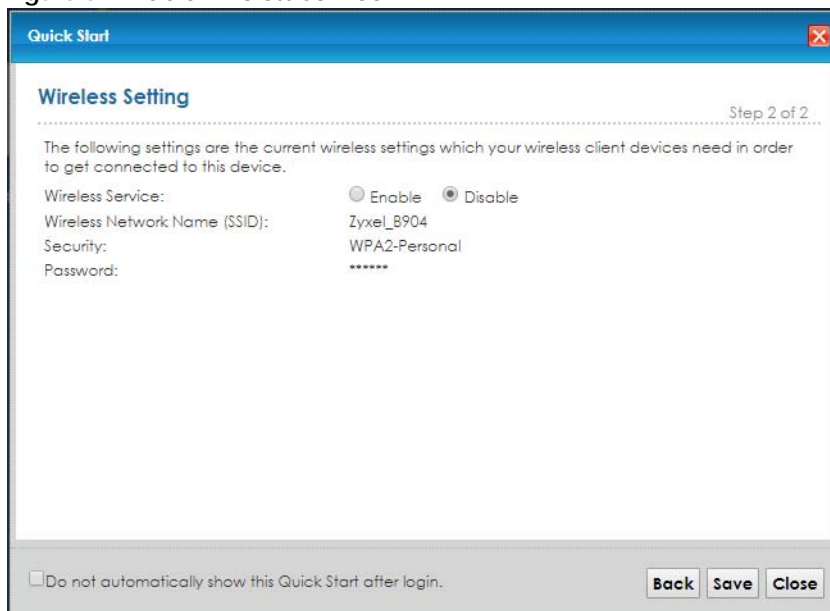
2.2.2 Wireless Setup

The following settings are the current WiFi settings which your wireless client devices need in order to get connected to the Zyxel Device. **Enable** the wireless service and click **Save**.

Note: You can also enable the wireless service using any of the following methods:

Click **Network Setting** > **Wireless** to open the **General** screen. Then select **Enable** in the **Wireless** field. Or,

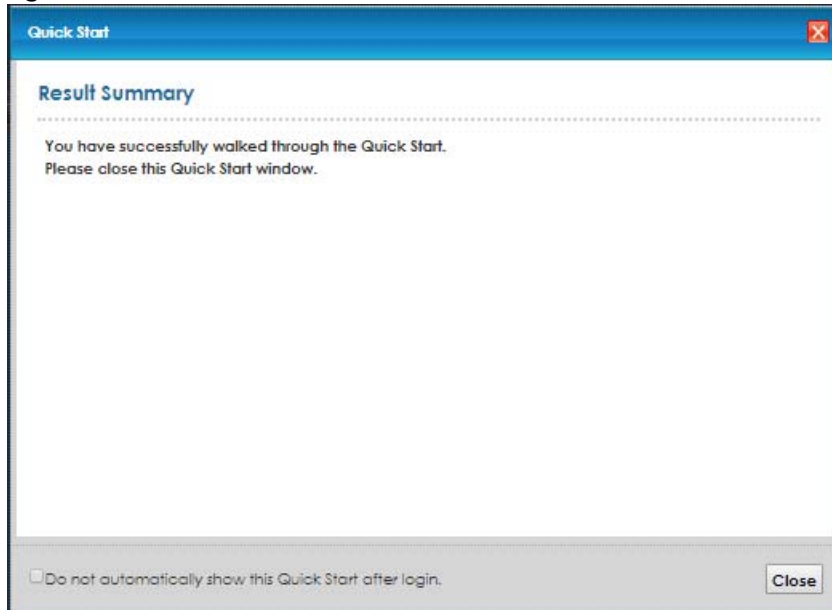
Press the **WiFi** button located under the **RESET** button (see [Section 1.6 on page 14](#) for the location) for one second.

Figure 5 Enable Wireless Service

Note: You might wish to check the option **Do not automatically show this Quick Start after login** so as not to display the wizard every time you login. You can always access the wizard via the **Quick Start** icon in the upper right corner of the **Connection Status** screen.

When the **Result Summary** screen appears, click **Close**.

Figure 6 Enable Wireless Service



The **Connection Status** screen appears.

Figure 7 Connection Status

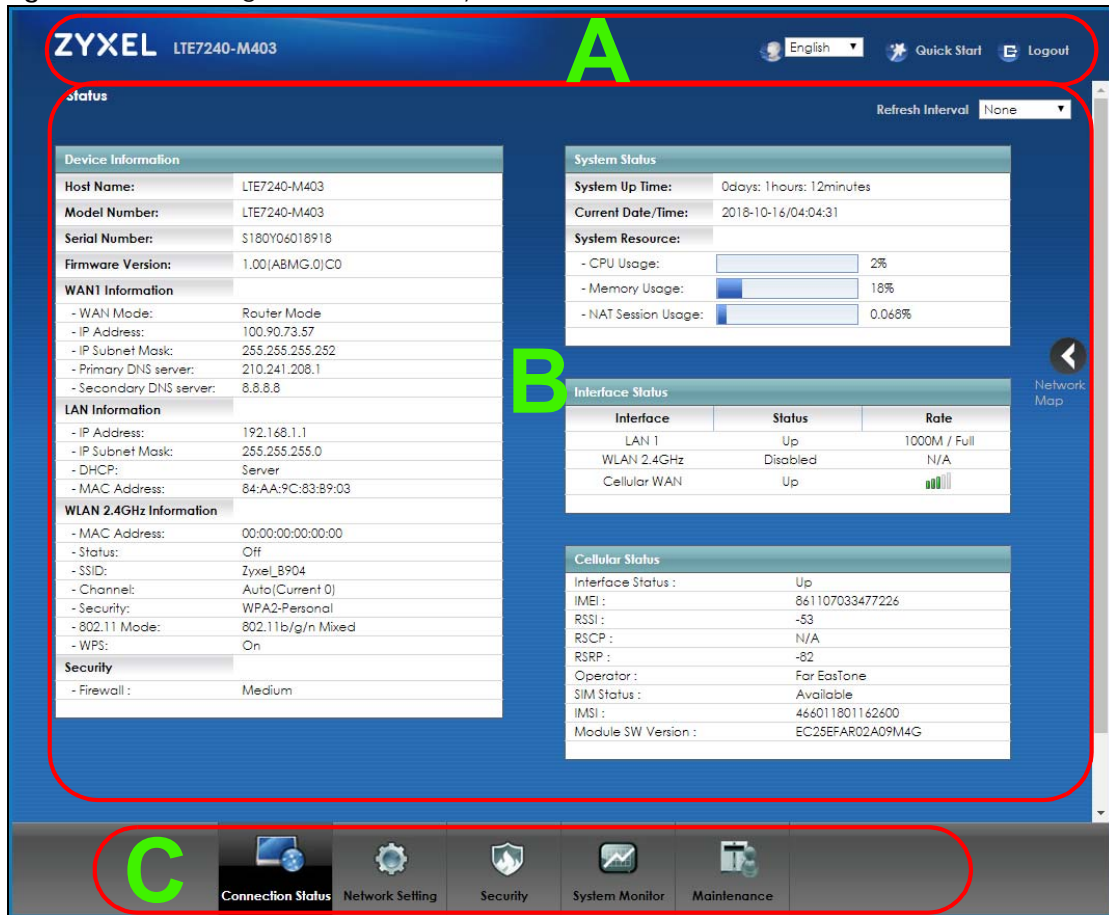


- 6 Click **Status** to display the **Status** screen, where you can view the Zyxel Device's interface and system information.

2.3 The Web Configurator Layout

Click **Status** to show the following screen.

Figure 8 Web Configurator in Status Layout

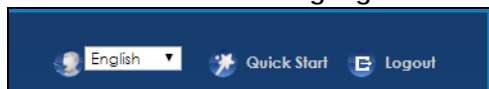


As illustrated above, the main screen is divided into these parts:

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

2.3.1 Title Bar

The title bar shows the **Language Selector**, **Quick Start** and **Logout** icons in the upper right corner.



Click the **Language Selector** to select the preferred Web Configurator language.

Click **Quick Start** to set your time zone and enable WiFi service.

Click the **Logout** icon to log out of the Web Configurator.

2.3.2 Main Window

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

Click **Connection Status** to display the **Device Information** and **System/Interface/Cellular Status** screen. See [Chapter 3 on page 25](#) for more information.

PART II

Technical Reference

CHAPTER 3

Connection Status and System Info

3.1 Overview

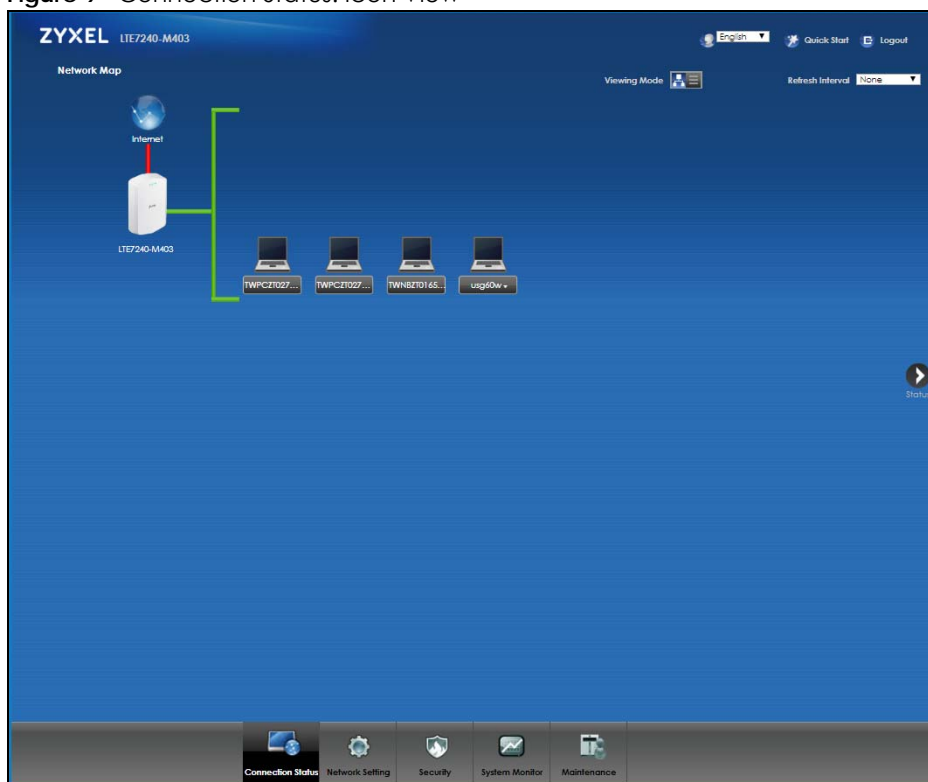
After you log into the Web Configurator, the **Connection Status** screen appears. This shows the network connection status of the Zyxel Device and clients connected to it.

Use the **Connection Status** screen to view the Network Map of the Zyxel Device.

3.2 The Connection Status Screen

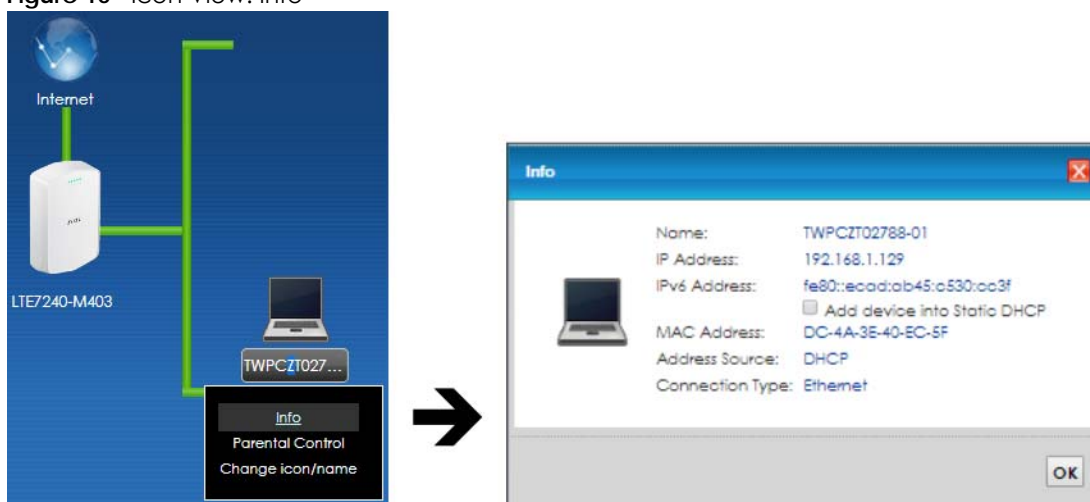
Use this screen to view the Network Map of the Zyxel Device and its clients. A warning message appears if there is a connection problem. You can select to view the **Connection Status** screen in **Icon** or **List View** in **Viewing Mode**. You can also configure how often you want the Zyxel Device to update this screen in **Refresh Interval**.

Figure 9 Connection Status: Icon View



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


Figure 10 Icon View: Info



Information related to the client device appears such as **Name**, **IP Address**, **IPv6 Address**, **MAC Address**, **Address Source** and **Connection Type**. Click the option **Add device into Static DHCP** to allow the DHCP server to always assign the same IP address to the client device on your LAN.

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

Figure 11 Connection Status: List View

Network Map					
			Viewing Mode	Refresh Interval	
#	Device Name	IP Address	MAC Address	Address Source	Connection Type
	TWPCZT02788-01	192.168.1.129	dc:4a:3e:40:ec:5f	DHCP	Ethernet

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

3.3 The Status Screen

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

Figure 12 Status Screen

Status		Refresh Interval	
Device Information			
Host Name:	LTE7240-M403		
Model Number:	LTE7240-M403		
Serial Number:	S180Y06018918		
Firmware Version:	1.00 (ABMG.0) C0		
WAN1 Information			
- WAN Mode:	Router Mode		
- IP Address:	0.0.0.0		
- IP Subnet Mask:	0.0.0.0		
- Primary DNS server:	N/A		
- Secondary DNS server:	N/A		
LAN Information			
- IP Address:	192.168.1.1		
- IP Subnet Mask:	255.255.255.0		
- DHCP:	Server		
- MAC Address:	84:AA:9C:83:B9:03		
WLAN 2.4GHz Information			
- MAC Address:	84:AA:9C:83:B9:04		
- Status:	On		
- SSID:	ZyxeL_B904		
- Channel:	Auto (Current 11)		
- Security:	WPA2-Personal		
- 802.11 Mode:	802.11b/g/n Mixed		
- WPS:	On		
Security			
- Firewall:	Medium		
System Status			
System Up Time:	0days: 1hours: 23minutes		
Current Date/Time:	2018-10-18/10:01:08		
System Resource:			
- CPU Usage:	<div><div></div></div>	4%	
- Memory Usage:	<div><div></div></div>	24%	
- NAT Session Usage:	<div><div></div></div>	0.0098%	
Interface Status			
Interface	Status	Rate	
LAN 1	Up	1000M / Full	
WLAN 2.4GHz	Up	144 Mbps	
Cellular WAN	Down	<div></div>	
Cellular Status			
Interface Status:	Down		
IMEI:	861107033477226		
RSSI:	N/A		
RSCP:	N/A		
RSRP:	N/A		
Operator:	Far EastOne		
SIM Status:	Available		
IMSI:	466011801162600		
Module SW Version:	EC25EFAR02A09M4G		

Each field is described in the following table.

Table 2 Status Screen

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Zyxel Device to update this screen from the drop-down list box.
Device Information	
Host Name	This field displays the Zyxel 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 the Zyxel Device.
Serial Number	This is the product serial number of the Zyxel Device.

Table 2 Status Screen (continued)

LABEL	DESCRIPTION
Firmware Version	This field displays the current version of the firmware inside the Zyxel Device. It also shows the date the firmware version was created. Go to the Maintenance > Firmware Upgrade screen to change it.
WAN1 Information	
WAN Mode	This shows whether the connection is in routing or bridge mode.
IP Address	This field displays the current LTE IP address of the Zyxel Device in the WAN.
IP Subnet Mask	This field displays the current subnet mask in the WAN.
Primary DNS Server	Enter the first DNS server address assigned by the ISP.
Secondary DNS Server	Enter the second DNS server address assigned by the ISP.
LAN Information	
IP Address	This field displays the current IP address of the Zyxel 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 Zyxel Device is providing to the LAN: Server - The Zyxel Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. None - The Zyxel Device is not providing any DHCP services to the LAN.
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your Zyxel Device.
WLAN 2.4GHz Information	
MAC Address	This field displays the 2.4GHz wireless adapter MAC Address of Zyxel Device.
Status	This field displays whether wireless LAN is currently enabled or disabled.
SSID	This field displays the SSID (Service Set IDentity) with which the wireless device is associated.
Channel	This field displays the Channel the wireless device is associated.
Security	This field displays the Encryption mode used by the wireless device.
802.11 Mode	This field displays the WiFi network mode used by the wireless device.
WPS	This field displays whether WiFi Protected Setup (WPS) is currently enabled or disabled.
Security	
Firewall	This shows whether or not the firewall is enabled (on).
System Status	
System Up Time	This field displays how long the Zyxel Device has been running since it last started up. The Zyxel Device starts up when you plug it in or when you restart it (Maintenance > Reboot).
Current Date/Time	This field displays the current date and time in the Zyxel Device. You can change this in Maintenance > Time .
System Resource	
CPU Usage	This field displays what percentage of the Zyxel Device's processing ability is currently used. When this percentage is close to 100%, the Zyxel 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 Zyxel Device's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100%, the Zyxel Device is probably becoming unstable, and you should restart the device. See Chapter 23 on page 148 , or turn off the device (unplug the power) for a few seconds.
NAT Session Usage	This field displays the percentage of concurrent NAT sessions of client host.

Table 2 Status Screen (continued)

LABEL	DESCRIPTION
Interface Status	
LAN1	This displays Up for a LAN connection. Down displays when the Zyxel Device does not have a LAN connection. It also shows the Rate of current connection.
WLAN 2.4GHz	This displays Up when wireless LAN is enabled in the Zyxel Device. Disabled displays when the Zyxel Device does not have wireless LAN enabled. It also shows the speed of wireless LAN connection.
Cellular WAN	This displays Up when LTE is enabled in the Zyxel Device. Disabled displays when the Zyxel Device does not have LTE enabled. It also shows the signal strength of LTE connection.
Cellular Status	
Interface Status	This displays Up for an LTE connection. Down displays when the Zyxel Device does not have a cellular connection.
IMEI	This displays the Zyxel Device's International Mobile Equipment Identity number (IMEI). An IMEI is a unique ID used to identify a mobile device.
RSSI (dBm)	This displays the strength of the LTE connection that the Zyxel Device has with the base station which is also known as eNodeB or eNB.
RSCP	This displays the Received Signal Code Power (RSCP) which measures the power on the channel use by the Zyxel Device.
RSRP (dBm)	This displays the LTE RSRP (Reference Signal Received Power).
Operator	This displays the service provider's name of the connected LTE network.
SIM Status	<p>This displays the SIM card status:</p> <p>None - the Zyxel Device does not detect that there is a SIM card inserted.</p> <p>Available - the SIM card could either have or doesn't have PIN code security.</p> <p>Locked - the SIM card has PIN code security, but you did not enter the PIN code yet.</p> <p>Blocked - 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.</p> <p>Error - the Zyxel Device detected that the SIM card has errors.</p>
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.
Module SW Version	This displays the version of the software on the LTE module.

CHAPTER 4

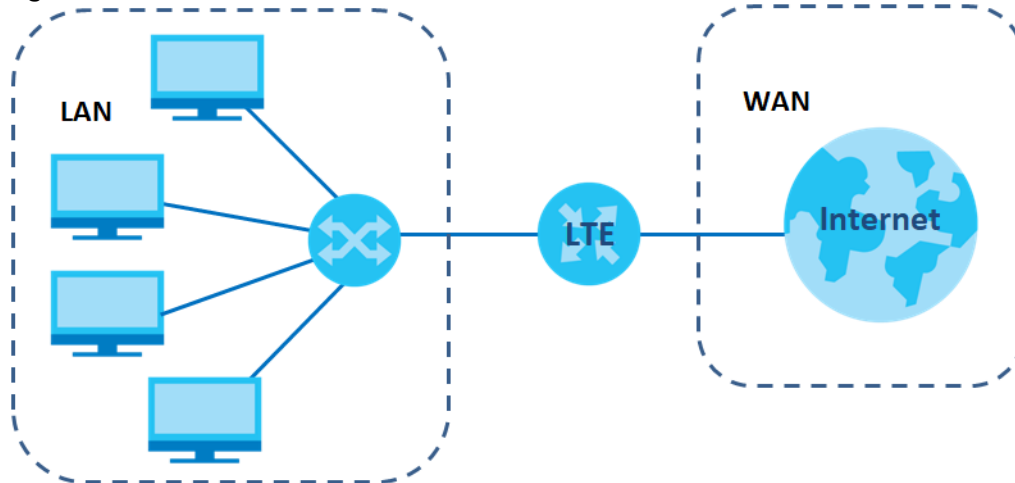
Broadband

4.1 Overview

This chapter discusses the Zyxel Device's **Broadband** screens. Use these screens to configure your Zyxel 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 13 LAN and WAN



4.1.1 What You Can Do in this Chapter

- Use the **Cellular WAN** screen to configure an LTE WAN connection ([Section 4.2 on page 29](#)).
- Use the **SIM** screen to enter the PIN of your SIM card ([Section 4.3 on page 30](#)).
- Use the **Band** screen to view or edit an LTE WAN interface. You can also configure the WAN settings on the Zyxel Device for Internet access ([Section 4.4 on page 32](#)).
- Use the **PLMN** screen to display available Public Land Mobile Networks ([Section 4.5 on page 33](#)).
- Use the **IP Passthrough** screen to configure an LTE WAN connection ([Section 4.6 on page 34](#)).
- Use the **Detail Statistics** screen to specify limiting the amount of data package and view the Zyxel Device's traffic statistics ([Section 4.7 on page 35](#)).

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 Zyxel Device, which makes it accessible from an outside network. It is used by the Zyxel Device to communicate with other devices in other networks. The ISP dynamically assigns it each time the Zyxel 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 Zyxel Device is off. Get this information from your service provider.

4.2 Cellular WAN Screen

Click **Network Setting > Broadband > Cellular WAN** to display the following screen. Use this screen to configure an LTE WAN connection that includes the Access Point Name (APN) provided by your service provider.

Note: The APN information can be obtained from the service provider of your SIM card.

Figure 14 Network Setting > Broadband > Cellular WAN

Cellular WAN configuration page.

General

Data Roaming : ☐ Enable ☒ Disable

Note:
Enable Roaming may charge extra cost.

APN Settings

APN Mode : ☒ Automatic ☐ Manual

APN :

Username : (Optional)

Password : (Optional)

Authentication Type :

Note:
Automatic APN is not supported in 3G only Mode.

Apply Cancel

Note: Roaming charges may apply when **Data Roaming** is enabled.
Automatic APN Mode is not supported when operating in 3G only mode.

The following table describes the fields in this screen.

Table 3 Network Setting > Broadband > Cellular WAN

LABEL	DESCRIPTION
General	
Data Roaming	Select this check box to enable data roaming on the Zyxel Device. 4G roaming is to use your mobile device in an area which is not covered by your service provider. Enable roaming to ensure that your Zyxel Device is kept connected to the Internet when you are traveling outside the geographical coverage area of the network to which you are registered.
APN Settings	
APN Mode	Select Auto to have the Zyxel Device configure the APN (Access Point Name) of an LTE network automatically. Otherwise, select Manual and enter the APN manually in the field below
APN	This field displays the Access Point Name (APN) in the profile. Enter the Access Point Name (APN) provided by your service provider. Connections with different APNs may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charging method. You can enter up to 30 printable ASCII characters. Spaces are allowed.
Username	This field displays the user name in the profile. Type the user name (up to 31 printable ASCII characters) given to you by your service provider.
Password	This field displays the password in the profile. Type the password (up to 31 printable ASCII characters) associated with the user name above.
Authentication Type	Select the type of authentication method peers use to connect to the Zyxel Device in LTE connections. In Password Authentication Protocol (PAP) peers identify themselves with a user name and password. In Challenge Handshake Authentication Protocol (CHAP) additionally to user name and password the Zyxel Device sends regular challenges to make sure an intruder has not replaced a peer. Otherwise select PAP/CHAP or None .
Apply	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

4.3 SIM Configuration Screen

Use the **SIM** configuration page to enter a PIN for your SIM card to prevent others from using it.

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 15 Network Setting > Broadband > SIM

Cellular WAN **SIM** Band PLMN IP Passthrough Detail Statistics

SIM Card configuration page.

SIM Status

SIM Card Status : Available

IMSI : 466011801162600

ICCID : 89886018157703499511

PIN Code Management

PIN Protection : ☐ Enable ☒ Disable

PIN :

(Attempts remaining: 3)

Note:

1. PIN code will automatic save in the device.
2. Entering the wrong PIN code too many times will lock SIM card.

Apply Cancel

Note: The PIN is automatically saved in the Zyxel Device.
 Entering the wrong PIN exceeding a set number of times will lock the SIM card.

The following table describes the fields in this screen.

Table 4 Network Setting > Broadband > SIM

LABEL	DESCRIPTION
SIM Status	
SIM Card Status	<p>This displays the SIM card status:</p> <p>None - the Zyxel Device does not detect that there is a SIM card inserted.</p> <p>Available - the SIM card could either have or doesn't have PIN code security.</p> <p>Locked - the SIM card has PIN code security, but you did not enter the PIN code yet.</p> <p>Blocked - 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.</p> <p>Error - the Zyxel Device detected that the SIM card has errors.</p>
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.
ICCID	Integrated Circuit Card Identifier (ICCID). This is the serial number of the SIM card.
PIN Code Management	
PIN Protection	<p>A PIN (Personal Identification Number) code is a key to a SIM card. Without the PIN code, you cannot use the SIM card.</p> <p>Select Enable if the service provider requires you to enter a PIN to use the SIM card.</p> <p>Select Disable if the service provider lets you use the SIM without inputting a PIN.</p>
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 let you use the account to access the Internet.
Attempts Remaining	This is how many more times you can try to enter the PIN code before the ISP blocks your SIM card.

Table 4 Network Setting > Broadband > SIM (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes.
Cancel	Click Cancel to return to the previous screen without saving.

4.4 The Band Configuration Screen

Use this screen to configure the LTE frequency bands that can be used for Internet access as provided by your service provider.

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

Figure 16 Network Setting > Broadband > Band

The following table describes the fields in this screen.

Table 5 Network Setting > Broadband > Band

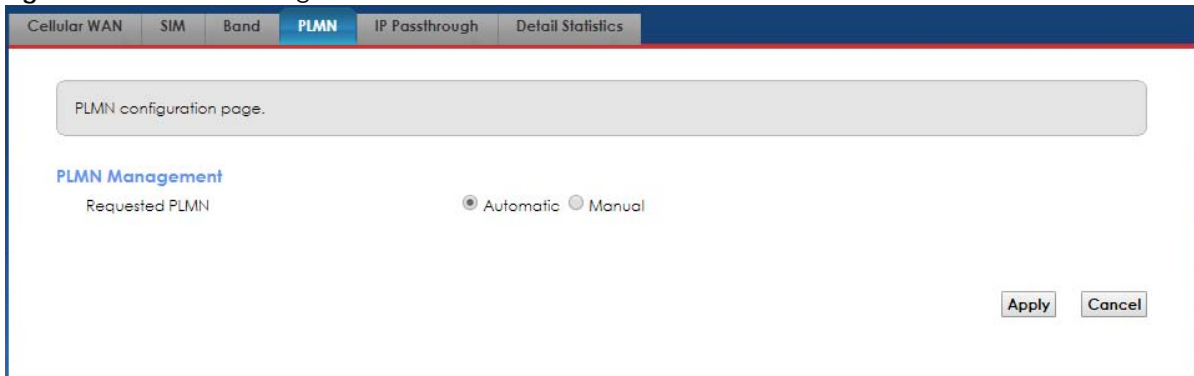
LABEL	DESCRIPTION
Access Technology	
Current Access Technology	This shows the type of the mobile network (such as LTE, UMTS, GSM) to which the Zyxel Device is connecting.
Access Technology Selection	Select the type of the network (4G , 3G , or 2G) to which you want the Zyxel Device to connect and click Apply to save your settings. Otherwise, select Auto to have the Zyxel Device connect to an available network using the default settings on the SIM card. If the currently registered mobile network is not available or the mobile network's signal strength is too low, the Zyxel Device switches to another available mobile network.
Band Management	
Current Band	This displays the current LTE band of your Zyxel Device (WCDMA2100).
Band Selection	Select the LTE bands to use for the Zyxel Device's WAN connection. Select Manual if you know which LTE frequency band to enable as provided by your service provider. Otherwise, select Automatic .
Apply	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

4.5 PLMN Configuration Screen

A Public Land Mobile Network (PLMN) is identified by the Mobile Country Code (MCC) and the Mobile Network Code (MNC). Each service provider has its own PLMN. Use this screen to view available PLMNs and select your preferred network.

Click **Network Setting > Broadband > PLMN**. The screen appears as shown next.

Figure 17 Network Setting > Broadband > PLMN



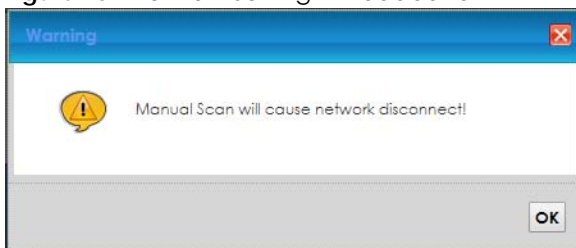
The following table describes the labels in this screen.

Table 6 Network Setting > Broadband > PLMN

LABEL	DESCRIPTION
PLMN Management	
Requested PLMN	Select Automatic to have the Zyxel Device automatically connect to the first available mobile network. Select Manual to display the network list and manually select a preferred network.
Apply	Click Apply to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving.

After selecting **Manual** the following warning appears. Click **OK** to continue.

Figure 18 Network Setting > Broadband > PLMN > Manual Scan Warning



When the next screen appears, clicking **Scan** will allow the Zyxel Device to check for available PLMNs in its surroundings and display the network list.

Figure 19 Network Setting > Broadband > PLMN

PLMN configuration page.

PLMN Management

Requested PLMN ☐ Automatic ☒ Manual

#	Status	Name	Type	PLMN
<input type="radio"/>	Available	FET	LTE	46601
<input checked="" type="radio"/>	Current	FET	UMTS	46601
<input type="radio"/>	Forbidden	466 05	GPRS	46605
<input type="radio"/>	Forbidden	466 05	LTE	46605
<input type="radio"/>	Available	Chunghwa	UMTS	46692
<input type="radio"/>	Available	Chunghwa	LTE	46692
<input type="radio"/>	Forbidden	TWM	LTE	46697
<input type="radio"/>	Forbidden	T Star	LTE	46689
<input type="radio"/>	Forbidden	TWM	UMTS	46697
<input type="radio"/>	Forbidden	T Star	UMTS	46689

The following table describes the labels in this screen.

Table 7 Network Setting > Broadband > PLMN

LABEL	DESCRIPTION
#	Click the radio button so the Zyxel Device connects to this ISP.
Status	This shows Current to show the ISP the Zyxel Device is currently connected to. This shows Forbidden to indicate the Zyxel Device cannot connect to this ISP. This shows Available to indicate an available ISP your Zyxel Device can connect to.
Name	This shows the ISP name.
Type	This shows the type of network the ISP provides.
PLMN	This shows the PLMN number.
Apply	Click Apply to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving.

Select from the network list and click **Apply**.

4.6 IP Passthrough Screen

Click **Network Setting > Broadband > IP Passthrough** to display the following screen. Use this screen to enable IP Passthrough mode (bridge mode).

Figure 20 Network Setting > Broadband > IP Passthrough

IP Passthrough configuration page.

IP Passthrough Settings

IP Passthrough : ☒ Enable ☐ Disable

Passthrough Mode : Fixed

Passthrough to fixed MAC : 1

Change IP Passthrough setting may affect the network setting of clients.

Apply Cancel

Note: Changing the IP Passthrough setting may affect the network setting of client devices.

The following table describes the fields in this screen.

Table 8 Network Setting > Broadband > IP Passthrough

LABEL	DESCRIPTION
IP Passthrough Settings	
IP Passthrough	IP Passthrough allows a LAN computer on the local network of the Zyxel Device to have access to web services using the public IP address. When IP Passthrough is configured, all traffic is forwarded to the LAN computer and will not go through NAT.
Passthrough Mode	Select Dynamic to allow traffic to be forwarded to any LAN computer on the local network of the Zyxel Device. Select Fixed to allow traffic to be forwarded to a specific LAN computer on the local network of the Zyxel Device. Note: This field will show upon enabling IP Passthrough in the previous field.
Passthrough to fixed MAC	Enter the MAC Address of a LAN computer on the local network of the Zyxel Device upon selecting Fixed in the previous field. Note: This field will show upon selecting Fixed in the previous field.
Apply	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

4.7 Detail Statistics Screen

This screen allows you to view the Zyxel Device's LTE-related connection and traffic statistics.

Click **Network Setting > Broadband > Detail Statistics**. The screen appears as shown next.

Figure 21 Network Setting > Broadband > Detail Statistics

Cellular WAN	SIM	Band	PLMN	IP Passthrough	Detail Statistics
Detail statistics.					
Connection Statistics					
IMEI	CurrentBand		CellID	RFCN	
861107033477226	WCDMA2100		14718426	10613	
RSRP	RSRQ		RSCP	EcNo	
N/A	N/A		-59	-2	
TAC	LAC		RAC	BSIC	
N/A	9242		1	N/A	

The following table describes the labels in this screen.

Table 9 Network Setting > Broadband > Detail Statistics

LABEL	DESCRIPTION
Connection Statistics	
IMEI	This shows the International Mobile Equipment Identity of the Zyxel Device.
Current Band	<p>This displays the network type and the frequency band used by the mobile network to which the Zyxel Device is connecting.</p> <p>Examples are: GSM900, GSM1800, WCDMA2100, WCDMA850, WCDMA900, LTE_BC1, LTE_BC3, LTE_BC5, LTE_BC7, LTE_BC8, LTE_BC20.</p> <p>'N/A' is displayed if there is no network connection.</p>
Cell ID	<p>This shows the cell ID, which is a unique number used to identify the Base Transceiver Station to which the Zyxel Device is connecting.</p> <p>The value depends on the Current Access Technology:</p> <ul style="list-style-type: none"> For GPRS, it is the Cell Identity as specified in 3GPP-TS.25.331. For UMTS, it is the Cell Identity as defined in SIB3 3GPP-TS.25.331, 3GPP-TS.24.008. For LTE, it is the 28-bit binary number Cell Identity as specified in SIB1 in 3GPP-TS.36.331. <p>The value is '0' (zero) or 'N/A' if there is no network connection.</p>
RFCN	<p>This displays the Radio Frequency Channel Number of DL carrier frequency used by the mobile network to which the Zyxel Device is connecting.</p> <p>The value depends on the Current Access Technology:</p> <ul style="list-style-type: none"> For GPRS, it is the ARFCN (Absolute Radio-Frequency Channel Number) as specified in 3GPP-TS.45.005. For UMTS, it is the UARFCN (UTRA Absolute Radio-Frequency Channel Number) as specified in 3GPP-TS.25.101. For LTE, it is the EARFCN (E-UTRA Absolute Radio-Frequency Channel Number) as specified in 3GPP-TS.36.101. <p>The value is '0' (zero) or 'N/A' if there is no network connection.</p>

Table 9 Network Setting > Broadband > Detail Statistics

LABEL	DESCRIPTION
RSRP -30 to -140	<p>This displays the Reference Signal Receive Power (RSRP), which is the average received power of all Resource Element (RE) that carry cell-specific Reference Signals (RS) within the specified bandwidth.</p> <p>The received RSRP level of the connected E-UTRA cell, in dBm, is as specified in 3GPP-TS.36.214. The reporting range is specified in 3GPP-TS.36.133.</p> <p>An undetectable signal is indicated by the lower limit, example -140 dBm.</p> <p>This parameter is for LTE only. The value is -140 if the Current Access Technology is not LTE. The value is 'N/A' if there is no network connection.</p>
RSRQ -30 to -240	<p>This displays the Reference Signal Receive Quality (RSRQ), which is the ratio of RSRP to the E-UTRA carrier RSSI and indicates the quality of the received reference signal.</p> <p>The received RSRQ level of the connected E-UTRA cell, in 0.1 dB, is as specified in 3GPP-TS.36.214. An undetectable signal is indicated by the lower limit, example -240.</p> <p>This parameter is for LTE only. The value is -240 if the Current Access Technology is not LTE. The value is 'N/A' if there is no network connection.</p>
RSCP -30 to -120	<p>This displays the Received Signal Code Power, which measures the power of channel used by the Zyxel Device.</p> <p>The received signal level, in dBm, is of the CPICH channel (Ref. 3GPP TS 25.133). An undetectable signal is indicated by the lower limit, example -120 dBm.</p> <p>This parameter is for UMTS only. The value is -120 if the Current Access Technology is not UMTS. The value is 'N/A' if there is no network connection.</p>
EcNo -30 to -240	<p>This displays the ratio (in dB) of the received energy per chip and the interference level.</p> <p>The measured EcNo is in 0.1 dB and is received in the downlink pilot channel. An undetectable signal is indicated by the lower limit, example -240 dB.</p> <p>This parameter is for UMTS only. The value is -240 if the Current Access Technology is not UMTS or there is no network connection.</p>
TAC	<p>This displays the Tracking Area Code (TAC), which is used to identify the country of a mobile subscriber.</p> <p>The physical cell ID of the connected E-UTRAN cell, is as specified in 3GPP-TS.36.101.</p> <p>This parameter is for LTE only. The value is '0' (zero) or 'N/A' if the Current Access Technology is not LTE or there is no network connection.</p>
LAC	<p>This displays the 2-octet Location Area Code (LAC), which is used to identify a location area within a PLMN.</p> <p>The LAC of the connected cell is as defined in SIB 1 [3GPP-TS.25.331]. The concatenation of PLMN ID (MCC+MNC) and LAC uniquely identifies the LAI (Location Area ID) [3GPP-TS.23.003].</p> <p>This parameter is for UMTS or GPRS. The value is '0' (zero) if the Current Access Technology is not UMTS or GPRS. The value is 'N/A' if there is no network connection.</p>

Table 9 Network Setting > Broadband > Detail Statistics

LABEL	DESCRIPTION
RAC	<p>This displays the RAC (Routing Area Code), which is used in mobile network "packet domain service" (PS) to identify a routing area within a location area.</p> <p>In a mobile network, it uses LAC (Location Area Code) to identify the geographical location for the old 3G voice only service, and use RAC to identify the location of data service like HSDPA or LTE.</p> <p>The RAC of the connected UTRAN cell is as defined in SIB 1 [3GPP-TS.25.331]. The concatenation of PLMN ID (MCC+MNC), LAC, and RAC uniquely identifies the RAI (Routing Area ID) [3GPP-TS.23.003].</p> <p>This parameter is for UMTS or GPRS. The value is '0' (zero) if the Current Access Technology is not UMTS or GPRS. The value is 'N/A' if there is no network connection.</p>
BSIC	<p>The Base Station Identity Code (BSIC), which is a code used in GSM to uniquely identify a base station.</p> <p>This parameter is for GPRS only. The value is '0' (zero) if the Current Access Technology is not GPRS. The value is 'N/A' if there is no network connection.</p>

CHAPTER 5

Wireless

5.1 Overview

This chapter describes the Zyxel Device's **Network Setting > Wireless** screens. Use these screens to set up your Zyxel Device's WiFi network and security settings.

5.1.1 What You Can Do in this Chapter

This section describes the Zyxel Device's **Wireless** screens. Use these screens to set up your Zyxel Device's WiFi connection.

- Use the **General** screen to enable the Wireless LAN, enter the SSID and select the WiFi security mode ([Section 5.2 on page 40](#)).
- Use the **MAC Authentication** screen to allow or deny wireless clients based on their MAC addresses from connecting to the Zyxel Device ([Section 5.3 on page 44](#)).
- Use the **WPS** screen to enable or disable WPS, view or generate a security PIN (Personal Identification Number) ([Section 5.4 on page 45](#)).
- Use the **WMM** screen to enable WiFi MultiMedia (WMM) to ensure quality of service in WiFi networks for multimedia applications ([Section 5.5 on page 47](#)).
- Use the **Others** screen to configure WiFi advanced features, such as the RTS/CTS Threshold ([Section 5.6 on page 48](#)).

5.1.2 What You Need to Know

Wireless Basics

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

Finding Out More

See [Section 5.7 on page 50](#) for advanced technical information on WiFi networks.

5.2 The General Screen

A WiFi network name (also known as SSID) and a security level are basic elements to start a WiFi service. Set a **Security Level** to protect your data from unauthorized access or damage via WiFi. Use this screen to enable the Wireless LAN, enter the SSID and select the WiFi security mode. It's recommended that you select **More Secure** to enable **WPA2-PSK** data encryption.

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

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

Figure 22 Network Setting > Wireless > General

General | MAC Authentication | WPS | WMM | Others

A wireless network name (also known as SSID) and a security level are basic elements to start a wireless service. It is recommended to set a security level other than no security to protect your data from unauthorized access or damage via wireless network.

Wireless Network Setup

Band: 2.4GHz

Wireless: ☒ Enable ☐ Disable (Settings are invalid when disabled)

Channel: Auto Current : 11

Bandwidth: 20MHz

Control Sideband: None

Wireless Network Settings

Wireless Network Name: Zyxel_B904

Max Clients: 32

☐ Hide SSID

☒ Multicast Forwarding

BSSID: 84:AA:9C:83:B9:04

Security Level

No Security | **More Secure (Recommended)**

Security Mode: WPA2-PSK

☒ Generate password automatically

Enter 8-63 ASCII characters or 64 hexadecimal digits ("0-9", "A-F").

Password: *****

☐ password unmask

[more...](#)

Apply **Cancel**

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

Table 10 Network Setting > Wireless > General

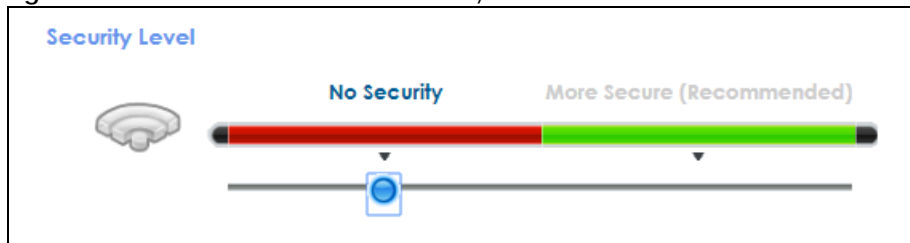
LABEL	DESCRIPTION
Wireless Network Setup	
Band	This shows the WiFi band which this radio profile is using. 2.4GHz is the frequency used by IEEE 802.11b/g/n WiFi clients while 5GHz is used by IEEE 802.11a/ac WiFi clients.
Wireless	Click Enable to enable the wireless LAN in this field.
Channel	Use Auto to have the Zyxel Device automatically determine a channel to use.
Bandwidth	<p>Select whether the Zyxel Device uses a WiFi channel width of 20MHz, 40MHz or 80MHz.</p> <p>A standard 20MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300Mbps.</p> <p>40MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The WiFi clients must also support 40MHz. It is often better to use the 20MHz setting in a location where the environment hinders the WiFi signal.</p> <p>An 80MHz channel groups adjacent 40MHz channels into pairs to increase bandwidth even higher.</p> <p>Select 20MHz if you want to lessen radio interference with other WiFi devices in your neighborhood or the WiFi clients do not support channel bonding.</p>
Control Sideband	This is available for some regions when you select a specific channel and set the Bandwidth field to 40MHz . Set whether the control channel (set in the Channel field) should be in the Lower or Upper range of channel bands.
Wireless Network Settings	
Wireless Network Name	<p>The SSID (Service Set IDentity) identifies the service set with which a WiFi device is associated. WiFi devices associating to the access point (AP) must have the same SSID.</p> <p>Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.</p>
Max Clients	Specify the maximum number of clients that can connect to this network at the same time.
Hide SSID	<p>Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.</p> <p>This check box is grayed out if the WPS function is enabled in the Network > Wireless > WPS screen.</p>
Multicast Forwarding	Select this check box to allow the Zyxel Device to convert wireless multicast traffic into wireless unicast traffic.
BSSID	This shows the MAC address of the wireless interface on the Zyxel Device when wireless LAN is enabled.
Security Level	
Security Mode	<p>Select More Secure (WPA2-PSK) to add security on this WiFi network. The WiFi clients which want to associate to this network must have same WiFi security settings as the Zyxel Device. When you select to use a security, additional options appears in this screen.</p> <p>Or you can select No Security to allow any client to associate this network without any data encryption or authentication.</p> <p>See the following sections for more details about this field.</p>
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

5.2.1 No Security

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

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

Figure 23 Wireless > General: No Security



The following table describes the labels in this screen.

Table 11 Wireless > General: No Security

LABEL	DESCRIPTION
Security Level	Choose No Security to allow all WiFi connections without data encryption or authentication.

5.2.2 More Secure (WPA2-PSK)

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

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

Figure 24 Wireless > General: More Secure: WPA2-PSK

Security Level

No Security **More Secure (Recommended)**

Security Mode: WPA2-PSK

☒ Generate password automatically

Enter 8-63 ASCII characters or 64 hexadecimal digits ('0-9', 'A-F').

Password:

☐ password unmask

[hide](#)

Encryption: AES

Group Key Update Timer: 3600 sec

The following table describes the labels in this screen.

Table 12 Wireless > General: More Secure: WPA2-PSK

LABEL	DESCRIPTION
Security Level	Select More Secure to enable WPA2-PSK data encryption.
Security Mode	Select WPA-PSK/WPA2-PSK or WPA2-PSK from the drop-down list box.
Generate password automatically	Select this option to have the Zyxel Device automatically generate a password. The password field will not be configurable when you select this option.
Password	<p>Select Generate password automatically or enter a Password.</p> <p>The password has two uses.</p> <ol style="list-style-type: none"> 1. Manual. Manually enter the same password on the Zyxel Device and the client. Enter 8-63 ASCII characters or exactly 64 hexadecimal ('0-9', 'a-f') characters. 2. WPS. When using WPS, the Zyxel Device sends this password to the client. <p>Note: Enter 8-63 ASCII characters only. 64 hexadecimal characters are not accepted for WPS.</p> <p>Click the password unmask check box to show the password of your WiFi network. When it is checked, you'll see the password in plain text. Otherwise, it's hidden.</p>
more...	Click this to show more fields in this section. Click hide to hide them.
Encryption	<p>Select the encryption type (AES or TKIP+AES) for data encryption.</p> <p>Select AES if your WiFi clients can all use AES.</p> <p>Select TKIP+AES to allow the WiFi clients to use either TKIP or AES.</p>
Group Key Update Timer	This is the rate at which the RADIUS server sends a new group key out to all clients.

5.3 MAC Authentication

Configure the Zyxel Device to give exclusive access to specific devices (**Allow**) or exclude specific devices from accessing the Zyxel Device (**Deny**) based on the device(s) MAC address. Every Ethernet device has a unique MAC (Media Access Control) address. It is assigned at the factory and consists of six pairs of hexadecimal characters; for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the device(s) you want to allow/deny to configure this screen. Edit the list in the table to decide the rule of access on device(s).

Use this screen to view your Zyxel Device's MAC filter settings and add new MAC filter rules. Click **Network Setting > Wireless > MAC Authentication**. The screen appears as shown.

Figure 25 Network Setting> Wireless > MAC Authentication

The following table describes the labels in this screen.

Table 13 Network Setting> Wireless > MAC Authentication

LABEL	DESCRIPTION
General	
SSID	Select the SSID for which you want to configure MAC filter settings.
MAC Restrict Mode	<p>Define the filter action for the list of MAC addresses in the MAC Address table.</p> <p>Select Disable to turn off MAC filtering.</p> <p>Select Deny to block access to the Zyxel Device. MAC addresses not listed will be allowed to access the Zyxel Device.</p> <p>Select Allow to permit access to the Zyxel Device. MAC addresses not listed will be denied access to the Zyxel Device.</p>
MAC address List	
Add new MAC address	<p>This field is available when you select Deny or Allow in the MAC Restrict Mode field.</p> <p>Click this if you want to add a new MAC address entry to the MAC filter list below.</p> <p>Enter the MAC addresses of the WiFi devices that are allowed or denied access to the Zyxel Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.</p>
#	This is the index number of the entry.

Table 13 Network Setting> Wireless > MAC Authentication (continued)

LABEL	DESCRIPTION
MAC Address	This is the MAC addresses of the WiFi devices that are allowed or denied access to the Zyxel Device.
Modify	Click the Edit icon and type the MAC address of the peer device in a valid MAC address format (six hexadecimal character pairs, for example 12:34:56:78:9a:bc). Click the Delete icon to delete the entry.
Cancel	Click Cancel to exit this screen without saving.
Apply	Click Apply to save your changes.

5.4 The WPS Screen

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

WiFi Protected Setup (WPS) allows you to quickly set up a WiFi network with strong security, without having to configure security settings manually. Select one of the WPS methods and follow the instructions to establish a WPS connection. To set up a WPS connection between two devices, both devices must support WPS. It is recommended to use the Push Button Configuration (**PBC**) method if your WiFi client supports it. See [Section 5.7.7.3 on page 58](#) for more information about WPS.

Note: The Zyxel Device uses the security settings of the **SSID1** profile (see [Section 5.2.2 on page 42](#)). The WPS button will gray-out when wireless LAN or WPS is disabled.

Note: If WPS is enabled, UPnP will automatically be turned on.

Click **Network Setting > Wireless > WPS**. The following screen displays. Click this switch and it will turn blue. Click **Apply** to activate the WPS function. Then you can configure the WPS settings in this screen.

Figure 26 Network Setting > Wireless > WPS

Enabling Wi-Fi Protected Setup (WPS) lets you add new WPS-compatible devices to the wireless network with ease. Select one of the WPS methods and follow the instructions to establish WPS connection. If your wireless client device is equipped with a WPS button, Push Button Configuration (PBC) method would be the preferable way to do WPS.

General

WPS ☒ Enable ☐ Disable (Settings are invalid when disabled)

Add a new device with WPS Method

Method 1 PBC <input checked="" type="radio"/> Enable <input type="radio"/> Disable	Method 2 PIN <input type="radio"/> Enable <input checked="" type="radio"/> Disable	Method 3 <input type="radio"/> Enable <input checked="" type="radio"/> Disable
<p>Step 1. Click WPS button </p> <p>Step 2. Press the WPS button on your new wireless client device within 120 seconds</p>	<p>Step 1. Enter the PIN of your new wireless client device and then click Register</p> <p>Enter PIN here <input type="text"/> <input type="button" value="Register"/></p> <p>Step 2. Press the WPS button on your new wireless client device within 120 seconds</p>	<p>Enter AP's PIN Number in Wireless Client</p> <p>Current state: Configured</p> <p>1. Please release configuration if you want to configure the wireless settings</p> <p><input type="button" value="Release Configuration"/></p> <p>2. Enter current PIN number on your wireless client</p> <p><input type="button" value="Generate New PIN"/></p>

Note

- 1.If WPS is Enabled, UPnP will automatically be turned on.
- 2.This feature is available only when WPA2-PSK or No Security mode is configured.
- 3.The WPS button will be grey-out when Wireless or WPS is disabled.

The following table describes the labels in this screen.

Table 14 Network Setting > Wireless > WPS

LABEL	DESCRIPTION
General	
WPS	Click Enable to activate WPS on this Zyxel Device. Otherwise, select Disable .
Add a new device with WPS Method	
Method 1	Use this section to set up a WPS WiFi network using Push Button Configuration (PBC). Click this switch to make it turn blue. Click Apply to activate WPS method 1 on the Zyxel Device.
WPS	Click this button to add another WPS-enabled WiFi device (within WiFi range of the Zyxel Device) to your WiFi network. This button may either be a physical button on the outside of a device, or a menu button similar to the WPS button on this screen. Note: You must press the other WiFi device's WPS button within two minutes of pressing this button.
Method 2	Use this section to set up a WPS WiFi network by entering the PIN of the client into the Zyxel Device. Click this switch to make it turn blue. Click Apply to activate WPS method 2 on the Zyxel Device.
Register	Enter the PIN of the device that you are setting up a WPS connection with and click Register to authenticate and add the WiFi device to your WiFi network. You can find the PIN either on the outside of the device, or by checking the device's settings. Note: You must also activate WPS on that device within two minutes to have it present its PIN to the Zyxel Device.

Table 14 Network Setting > Wireless > WPS (continued)

LABEL	DESCRIPTION
Method 3	Use this section to set up a WPS WiFi network by entering the PIN of the Zyxel Device into the client. Click this switch to make it turn blue. Click Apply to activate WPS method 3 on the Zyxel Device.
Release Configuration	The default WPS status is configured. Click this button to remove all configured WiFi and WiFi security settings for WPS connections on the Zyxel Device.
Generate New PIN Number	If this method has been enabled, the PIN (Personal Identification Number) of the Zyxel Device is shown here. Enter this PIN in the configuration utility of the device you want to connect to using WPS. The PIN is not necessary when you use the WPS push-button method. Click the Generate New PIN button to have the Zyxel Device create a new PIN.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

5.5 The WMM Screen

Use this screen to enable Wi-Fi MultiMedia (WMM) and WMM Automatic Power Save (APSD) in WiFi networks for multimedia applications. WMM and APSD have beneficial effects on delay-sensitive applications over WiFi connections such as multimedia streaming. WMM enhances data transmission quality, while APSD improves power management of WiFi clients. This allows delay-sensitive applications, such as videos, to run more smoothly.

Click **Network Setting > Wireless > WMM** to display the following screen.

Figure 27 Network Setting > Wireless > WMM

WMM and APSD have beneficial effects on delay-sensitive applications over wireless connection such as, VoIP and multimedia streaming, because WMM enhances data transmission quality and APSD improves power management on wireless clients.

WMM of SSID1 : ☒ Enable ☐ Disable

WMM Automatic Power Save Delivery (APSD) : ☒ Enable ☐ Disable

Note

1. WMM is mandatory to be enabled if 802.11 mode includes 802.11n or 802.11ac

Apply Cancel

Note: WMM cannot be disabled if 802.11 mode includes 802.11n or 802.11ac.

The following table describes the labels in this screen.

Table 15 Network Setting > Wireless > WMM

LABEL	DESCRIPTION
WMM of SSID1~4	Select On to have the Zyxel Device automatically give the WiFi network (SSIDx) a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (WiFi MultiMedia Quality of Service) gives high priority to video, which makes them run more smoothly. If the 802.11 Mode in Network Setting > Wireless > Others is set to include 802.11n or 802.11ac, WMM cannot be disabled.
WMM Automatic Power Save Delivery (APSD)	Select this option to extend the battery life of your mobile devices (especially useful for small devices that are running multimedia applications). The Zyxel Device goes to sleep mode to save power when it is not transmitting data. The AP buffers the packets sent to the Zyxel Device until the Zyxel Device "wakes up." The Zyxel Device wakes up periodically to check for incoming data. Note: This works only if the WiFi device to which the Zyxel Device is connected also supports this feature.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

5.6 The Others Screen

Additional security, power saving and data transmission settings are available in this page. Click **Network Setting > Wireless > Others**. The screen appears as shown.

See [Section 5.7.2 on page 52](#) for detailed definitions of the terms listed in this screen.

Figure 28 Network Setting > Wireless > Others

The configurations below are the advanced wireless settings.

RTS/CTS Threshold :	<input type="text" value="2347"/>
Fragmentation Threshold :	<input type="text" value="2346"/>
Output Power :	<input type="text" value="100%"/> ▼
Beacon Interval :	<input type="text" value="100"/> ms
DTIM Interval :	<input type="text" value="1"/> ms
802.11 Mode :	<input type="text" value="802.11b/g/n Mixed"/> ▼
802.11 Protection :	<input type="text" value="Auto"/> ▼
Preamble :	<input type="text" value="Long"/> ▼

The following table describes the labels in this screen.

Table 16 Network Setting > Wireless > Others

LABEL	DESCRIPTION
RTS/CTS Threshold	<p>Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake.</p> <p>Enter a value between 0 and 2347.</p>
Fragmentation Threshold	<p>This is the maximum data fragment size that can be sent. Enter a value between 256 and 2346.</p>
Output Power	<p>Set the output power of the Zyxel Device. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs. Select one of the following: 20%, 40%, 60%, 80% or 100%.</p>
Beacon Interval	<p>When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again.</p> <p>The interval tells receiving devices on the network how long they can wait in low power mode before waking up to handle the beacon. This value can be set from 50ms to 1000ms. A high value helps save current consumption of the access point.</p>
DTIM Interval	<p>Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Power Saving mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 255.</p>
802.11 Mode	<p>For 2.4GHz frequency WLAN devices:</p> <ul style="list-style-type: none"> • Select 802.11b Only to allow only IEEE 802.11b compliant WLAN devices to associate with the Zyxel Device. • Select 802.11g Only to allow only IEEE 802.11g compliant WLAN devices to associate with the Zyxel Device. • Select 802.11n Only to allow only IEEE 802.11n compliant WLAN devices to associate with the Zyxel Device. • Select 802.11b/g Mixed to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select 802.11b/g/n Mixed to allow IEEE 802.11b, IEEE 802.11g or IEEE802.11n compliant WLAN devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. <p>For 5GHz frequency WLAN devices:</p> <ul style="list-style-type: none"> • Select 802.11a Only to allow only IEEE 802.11a compliant WLAN devices to associate with the Zyxel Device. • Select 802.11n Only to allow only IEEE 802.11n compliant WLAN devices to associate with the Zyxel Device. • Select 802.11ac Only to allow only IEEE 802.11ac compliant WLAN devices to associate with the Zyxel Device. • Select 802.11a/n Mixed to allow either IEEE 802.11a or IEEE 802.11n compliant WLAN devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select 802.11n/ac Mixed to allow either IEEE 802.11n or IEEE 802.11ac compliant WLAN devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select 802.11a/n/ac Mixed to allow IEEE 802.11a, IEEE 802.11n or IEEE802.11ac compliant WLAN devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced.
802.11 Protection	<p>Enabling this feature can help prevent collisions in mixed-mode networks (networks with both IEEE 802.11b and IEEE 802.11g traffic).</p> <p>Select Auto to have the wireless devices transmit data after a RTS/CTS handshake. This helps improve IEEE 802.11g performance.</p> <p>Select Off to disable 802.11 protection. The transmission rate of your Zyxel Device might be reduced in a mixed-mode network.</p> <p>This field displays Off and is not configurable when you set 802.11 Mode to 802.11b Only.</p>

Table 16 Network Setting > Wireless > Others (continued)

LABEL	DESCRIPTION
Preamble	Select a preamble type from the drop-down list box. Choices are Long or Short . See Section 5.7.6 on page 55 for more information. This field is configurable only when you set 802.11 Mode to 802.11b .
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

5.7 Technical Reference

This section discusses wireless LANs in depth.

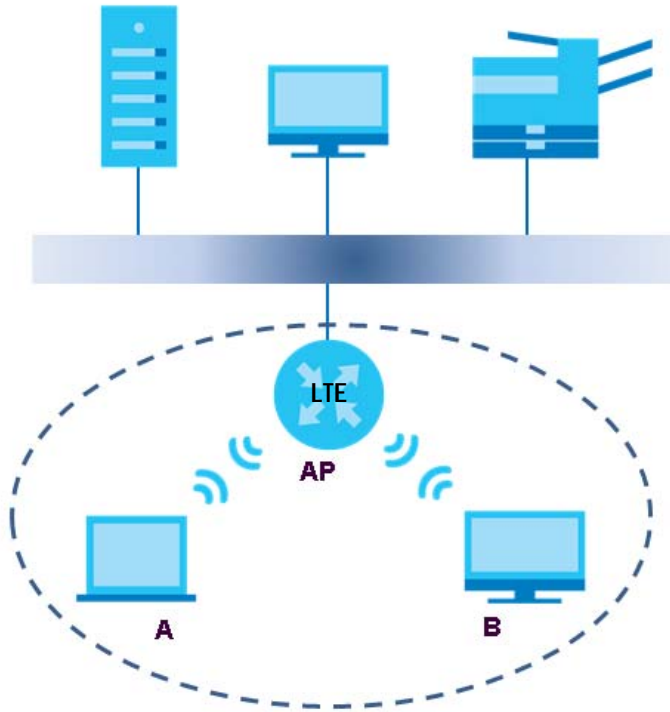
5.7.1 WiFi Network Overview

WiFi networks consist of WiFi clients, access points and bridges.

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

Normally, a WiFi network operates in an "infrastructure" type of network. An "infrastructure" type of network has one or more access points and one or more WiFi clients. The WiFi clients connect to the access points.

The following figure provides an example of a WiFi network.

Figure 29 Example of a WiFi Network

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

Every WiFi network must follow these basic guidelines.

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

Radio Channels

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

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

5.7.2 Additional Wireless Terms

The following table describes some WiFi network terms and acronyms used in the Zyxel Device's Web Configurator.

Table 17 Additional WiFi Terms

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

5.7.3 WiFi Security Overview

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

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

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

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

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

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

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

5.7.3.1 SSID

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

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

5.7.3.2 MAC Address Filter

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

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

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

5.7.3.3 User Authentication

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

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

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

5.7.3.4 Encryption

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

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

The types of encryption you can choose depend on the type of authentication. (See [Section 5.7.3.3 on page 53](#) for information about this.)

Table 18 Types of Encryption for Each Type of Authentication

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

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

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

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

5.7.4 Signal Problems

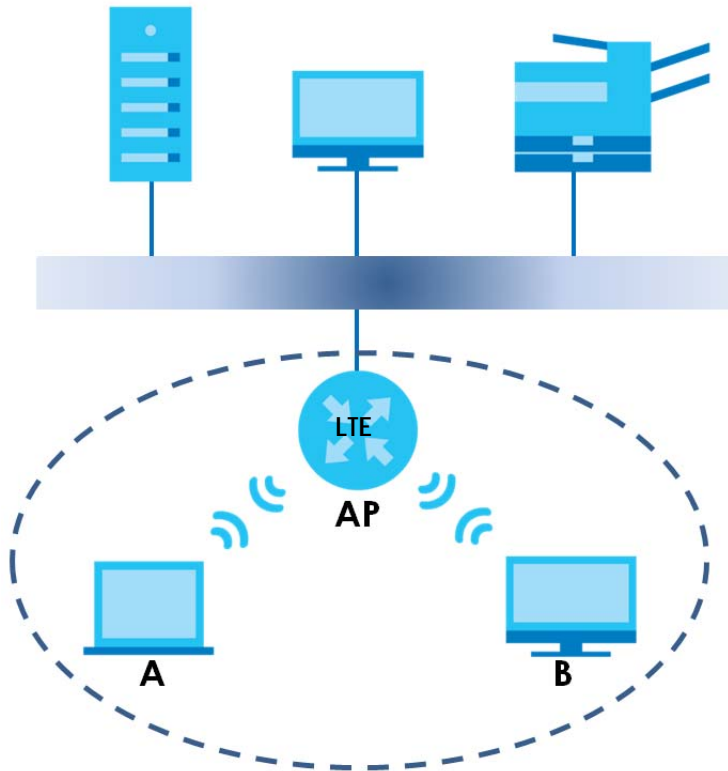
Because WiFi networks are radio networks, their signals are subject to limitations of distance, interference and absorption.

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

5.7.5 BSS

A Basic Service Set (BSS) exists when all communications between wireless stations go through one access point (AP).

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

Figure 30 Basic Service Set

5.7.6 Preamble Type

Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant wireless adapters support long preamble, but not all support short preamble.

Use long preamble if you are unsure what preamble mode other WiFi devices on the network support, and to provide more reliable communications in busy WiFi networks.

Use short preamble if you are sure all WiFi devices on the network support it, and to provide more efficient communications.

Use the dynamic setting to automatically use short preamble when all WiFi devices on the network support it, otherwise the Zyxel Device uses long preamble.

Note: The WiFi devices **MUST** use the same preamble mode in order to communicate.

5.7.7 WiFi Protected Setup (WPS)

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

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

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

5.7.7.1 Push Button Configuration

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

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

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

- 1 Ensure that the two devices you want to set up are within wireless range of one another.
- 2 Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the Zyxel Device, see [Section 5.5 on page 47](#)).
- 3 Press the button on one of the devices (it doesn't matter which). For the Zyxel Device you must press the **WiFi** button for more than five seconds.
- 4 Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through a secure connection to the enrollee.

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

5.7.7.2 PIN Configuration

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

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

When you use the PIN method, you must enter the PIN from one device (usually the WiFi client) into the second device (usually the Access Point or wireless router). Then, when WPS is activated on the first device, it presents its PIN to the second device. If the PIN matches, one device sends the network and security information to the other, allowing it to join the network.

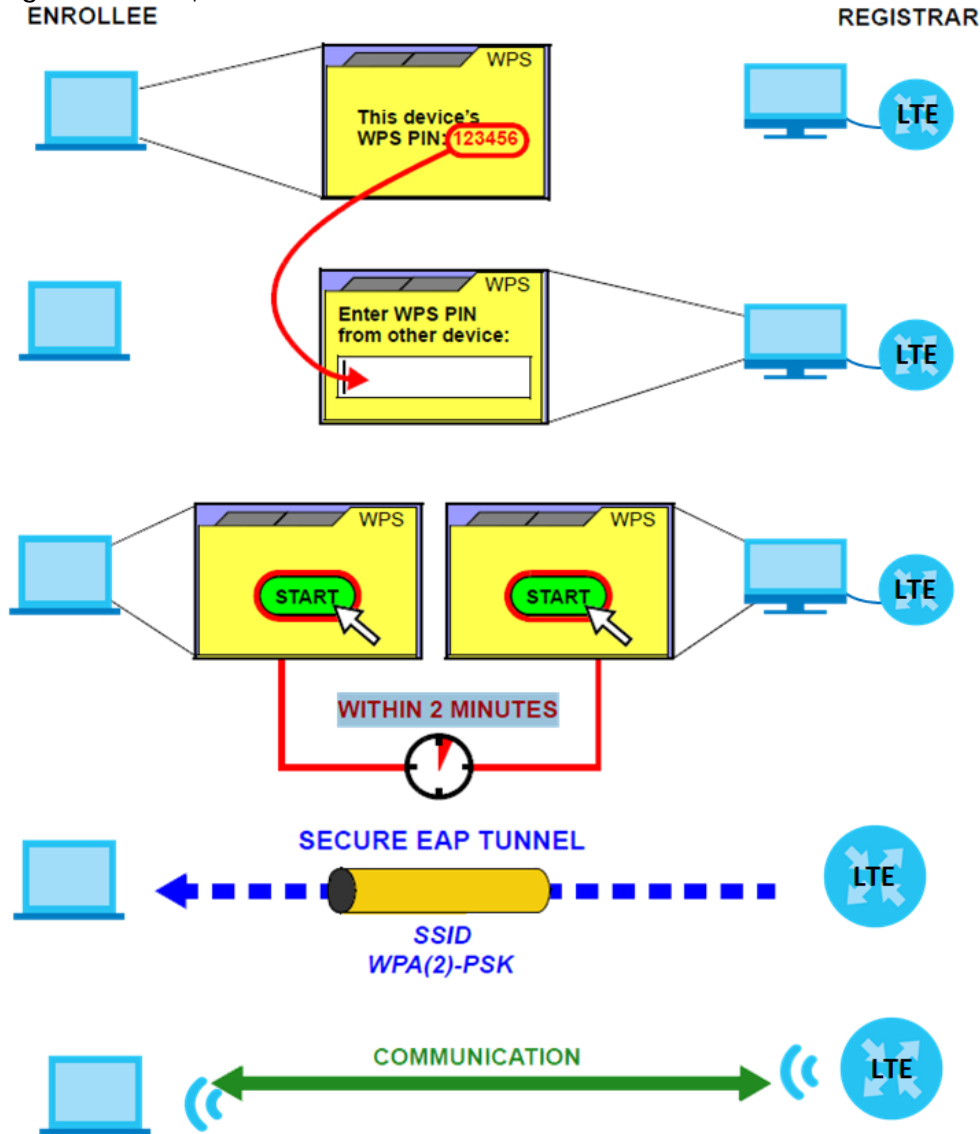
Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

- 1** Ensure WPS is enabled on both devices.
- 2** Access the WPS section of the AP's configuration interface. See the device's User's Guide on how to do this.
- 3** Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide on how to find the WPS PIN - for the Zyxel Device, see [Section 5.4 on page 45](#)).
- 4** Enter the client's PIN in the AP's configuration interface.
- 5** If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client - it does not matter which.
- 6** Start WPS on both devices within two minutes.
- 7** Use the configuration utility to activate WPS, not the push-button on the device itself.
- 8** On a computer connected to the WiFi client, try to connect to the Internet. If you can connect, WPS was successful.

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

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

Figure 31 Example WPS Process: PIN Method
ENROLLEE

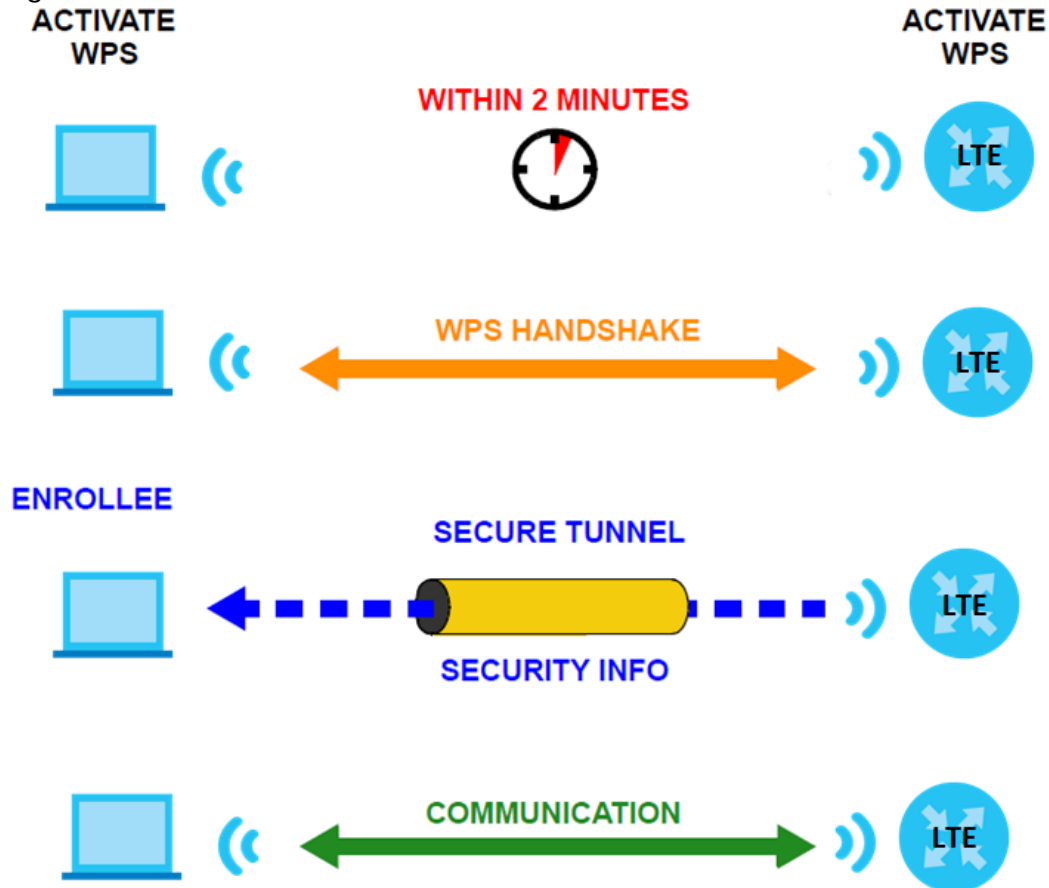


5.7.7.3 How WPS Works

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

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

Figure 32 How WPS works



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

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

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

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

5.7.7.4 Example WPS Network Setup

This section shows how security settings are distributed in a sample WPS setup.

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

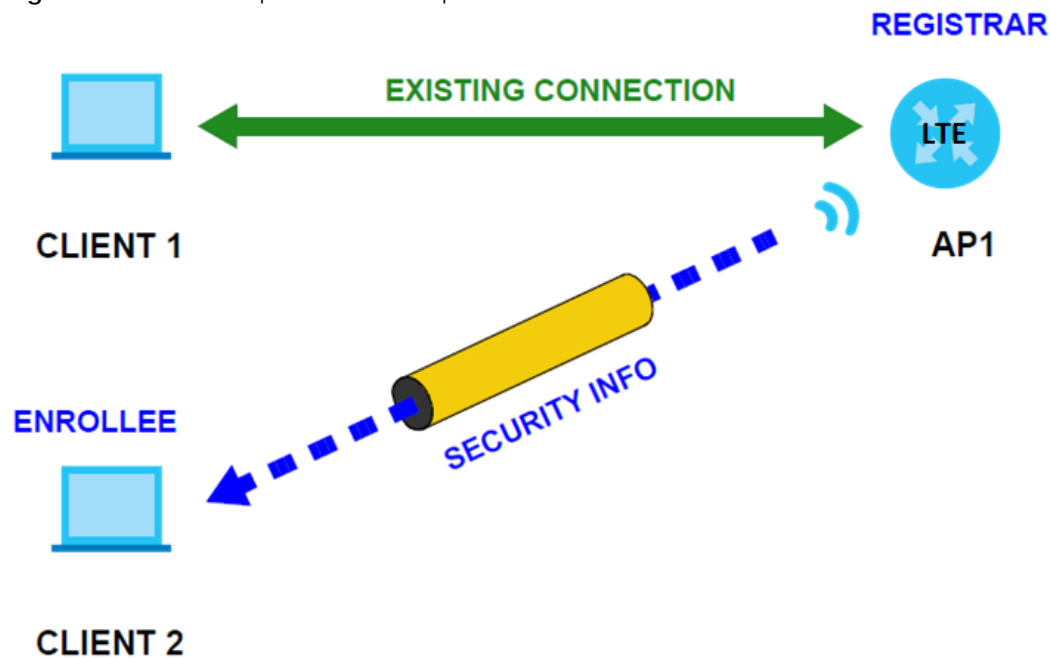
is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information.

Figure 33 WPS: Example Network Step 1



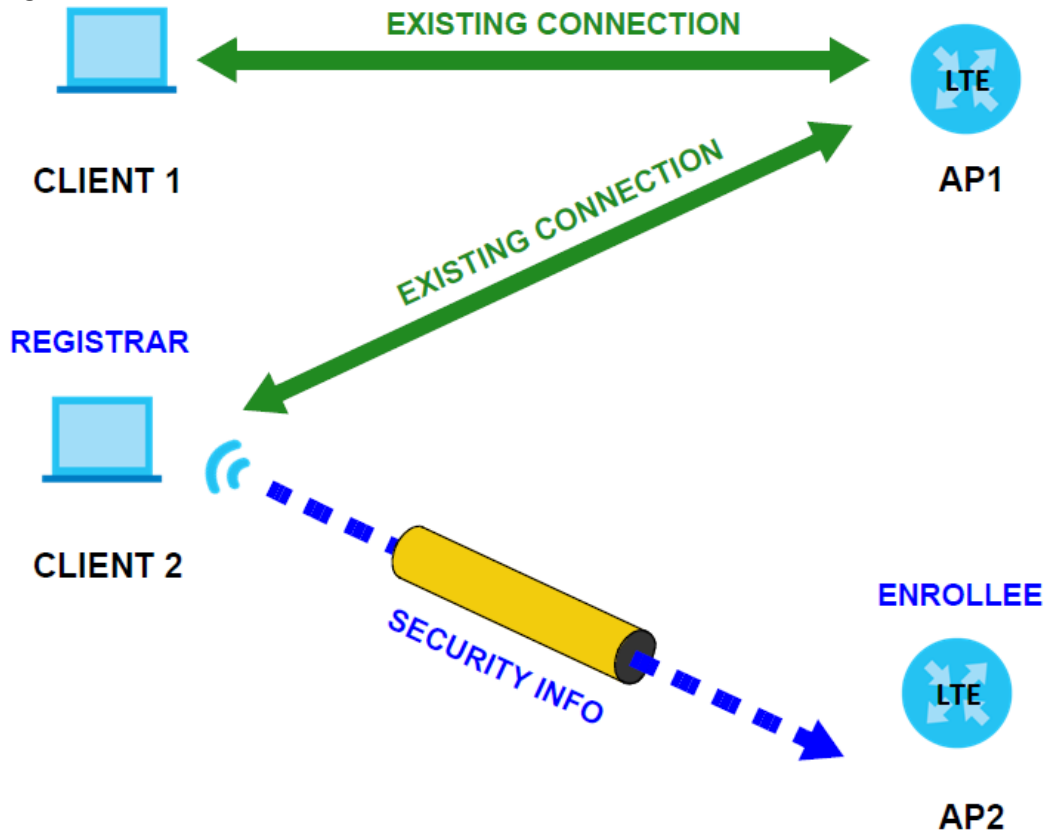
In step 2, you add another WiFi client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar,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

Figure 34 WPS: Example Network Step 2



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

Figure 35 WPS: Example Network Step 3



5.7.7.5 Limitations of WPS

WPS has some limitations of which you should be aware.

- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously, you must enroll one after the other.

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

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

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

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

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

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

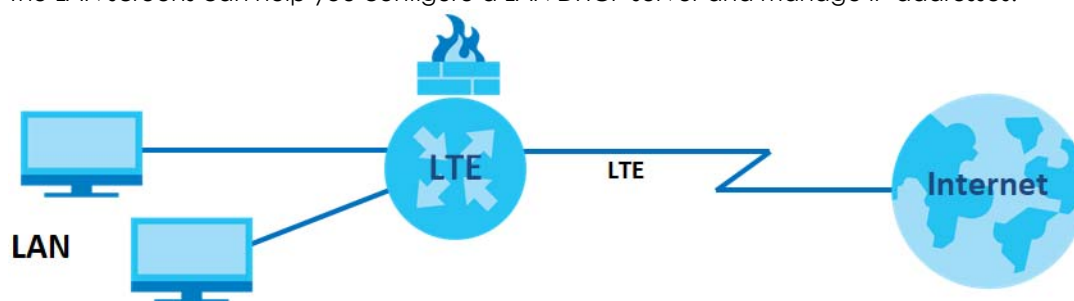
CHAPTER 6

Home Networking

6.1 Overview

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

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



6.1.1 What You Can Do in this Chapter

- Use the **LAN Setup** screen to set the LAN IP address, subnet mask, and DHCP settings ([Section 6.2 on page 64](#)).
- Use the **IPv6 LAN Setup** screen to configure the IPv6 settings on your Zyxel Device's LAN interface ([Section 6.3 on page 66](#)).
- Use the **Static DHCP** screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses ([Section 6.3 on page 66](#)).
- Use the **UPnP** screen to enable UPnP ([Section 6.4 on page 68](#)).

6.1.2 What You Need To Know

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

6.1.2.1 About LAN

IP Address

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

Subnet Mask

The subnet mask specifies the network number portion of an IP address. Your Zyxel 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 Zyxel 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 Zyxel Device has a built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

DNS

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

6.1.2.2 About UPnP

How do I know if I'm using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows 7). 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 Zyxel 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 6.6 on page 70](#) for examples on installing and using UPnP.

6.2 The LAN Setup Screen

A LAN IP address is the IP address of a networking device in the LAN. You can use the Zyxel Device's LAN IP address to access its web configurator from the LAN. The DHCP server settings define the rules on assigning IP addresses to LAN clients on your network. Set the Local Area Network IP address and subnet mask of your Zyxel Device and configure the DNS server information that the Zyxel Device sends to the DHCP clients on the LAN in this page. Click **Network Setting > Home Networking** to open the **LAN Setup** screen.

Figure 36 Network Setting > Home Networking > LAN Setup

The LAN IP address is the IP address you use to log into the web configurator. The DHCP server settings define the rules on how to assign IP addresses to the LAN clients on your network.

Interface Group
Group Name:

LAN IP Setup
IP Address:
Subnet Mask:

DHCP Server State
DHCP: ☒ Enable ☐ Disable ☐ DHCP Relay

IP Addressing Values
Beginning IP Address:
Ending IP Address:
Auto reserve IP for the same host: ☐ Enable ☒ Disable

DHCP Server Lease Time
 Days Hours Minutes

DNS Values
DNS: ☒ DNS Proxy ☐ Static ☐ From ISP

LAN IPv6 Mode Setup
IPv6 Active: ☐ Enable ☒ Disable

The following table describes the fields in this screen.

Table 19 Network Setting > Home Networking > LAN Setup

LABEL	DESCRIPTION
Interface Group	
Group Name	This displays the name of the group that your Zyxel Device belongs to.
LAN IP Setup	
IP Address	Enter the LAN IP address you want to assign to your Zyxel 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 Zyxel 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	<p>Select Enable to have your Zyxel Device assign IP addresses, an IP default gateway and DNS servers to LAN computers and other devices that are DHCP clients.</p> <p>If you select Disable, you need to manually configure the IP addresses of the computers and other devices on your LAN.</p> <p>If you select DHCP Relay, the Zyxel 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.</p> <p>When DHCP is used, the following fields need to be set:</p>
IP Addressing Values	

Table 19 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
Beginning IP Address	This field specifies the first of the contiguous addresses in the IP address pool.
Ending IP Address	This field specifies the last of the contiguous addresses in the IP address pool.
Auto reserve IP for the same host	Enable this if you want to reserve the IP address for the same host.
DHCP Server Lease Time	
Days/Hours/Minutes	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	<p>The Zyxel Device supports DNS proxy by default. The Zyxel 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 Zyxel Device. The Zyxel Device sends a response directly if it has a record of the domain-name to IP address mapping. If it does not, the Zyxel Device queries an outside DNS server and relays the response to the DHCP client.</p> <p>Select From ISP if your ISP dynamically assigns DNS server information (and the Zyxel Device's WAN IP address).</p> <p>Select Static if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right.</p> <p>Select DNS Proxy to have the DHCP clients use the Zyxel Device's own LAN IP address. The Zyxel Device works as a DNS relay.</p>
LAN IPv6 Mode Setup	
IPv6 Active	Use this field to Enable or Disable IPv6 activation on the Zyxel Device.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

6.3 The Static DHCP Screen

When any of the LAN clients in your network want an assigned fixed IP address, add a static lease for each LAN client. Knowing the LAN client's MAC addresses is necessary. This page allows you to assign IP addresses on the LAN to specific individual computers based on their MAC addresses.

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

6.3.1 Before You Begin

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

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

Figure 37 Network Setting > Home Networking > Static DHCP

When any of the LAN clients on your network want an assigned fixed IP address, add a static lease for each LAN client. You may need to know the clients' MAC addresses in advance in order to process the setup quickly.

Static DHCP Configuration

#	Status	MAC Address	IP Address	Modify
---	--------	-------------	------------	--------

The following table describes the labels in this screen.

Table 20 Network Setting > Home Networking > Static DHCP

LABEL	DESCRIPTION
Static DHCP Configuration	Click this to configure a static DHCP entry.
#	This is the index number of the entry.
Status	Active
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 **Static DHCP Configuration** in the **Static DHCP** screen, the following screen displays.

Figure 38 Static DHCP: Static DHCP Configuration

Static DHCP Configuration

Active ☐ Enable ☒ Disable

Group Name: Default

IP Type: IPv4

Select Device Info: Manual Input

MAC Address : - - - -

IP Address : - - -

OK Cancel

The following table describes the labels in this screen.

Table 21 Static DHCP: Configuration

LABEL	DESCRIPTION
Active	Enable static DHCP in your Zyxel Device.
Group Name	This displays the Group Name , usually Default .
IP Type	The IP Type is normally IPv4 (non-configurable).
Select Device Info	Select between Manual Input which allows you to enter the next two fields (MAC Address and IP Address); or selecting an existing device would show its MAC address and IP address.
MAC Address	Enter the MAC address of a computer on your LAN if you select Manual Input in the previous field.
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 if you select Manual Input in the previous field.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

6.4 The UPnP Screen

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between networking devices and software that also have UPnP enabled. 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 70](#) for more information on UPnP.

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

Figure 39 Network Setting > Home Networking > UPnP

Universal Plug and Play (UPnP) is a networking standard for easy network connectivity among networking devices and software that also have UPnP enabled.

UPnP State
UPnP ☐ Enable ☒ Disable

UPnP NAT-T State
UPnP NAT-T: ☐ Enable ☒ Disable

Note :
UPnP NAT-T only works when NAT is enable

#	Description	Destination IP Address	External Port	Internal Port	Protocol
---	-------------	------------------------	---------------	---------------	----------

Apply Cancel

The following table describes the labels in this screen.

Table 22 Network Settings > Home Networking > UPnP

LABEL	DESCRIPTION
UPnP State	
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 Zyxel Device's IP address (although you must still enter the password to access the Web Configurator).
UPnP NAT-T State	
UPnP NAT-T	Select Enable to activate UPnP with NAT enabled. UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions.
#	This field displays the index number of the entry.
Description	This field displays the description of the UPnP NAT-T connection.
Destination IP Address	This field displays the IP address of the other connected UPnP-enabled device.
External Port	This field displays the external port number that identifies the service.
Internal Port	This field displays the internal port number that identifies the service.
Protocol	This field displays the protocol of the NAT mapping rule (TCP or UDP).
Apply	Click Apply to save your changes.
Cancel	Click this to restore your previously saved settings.

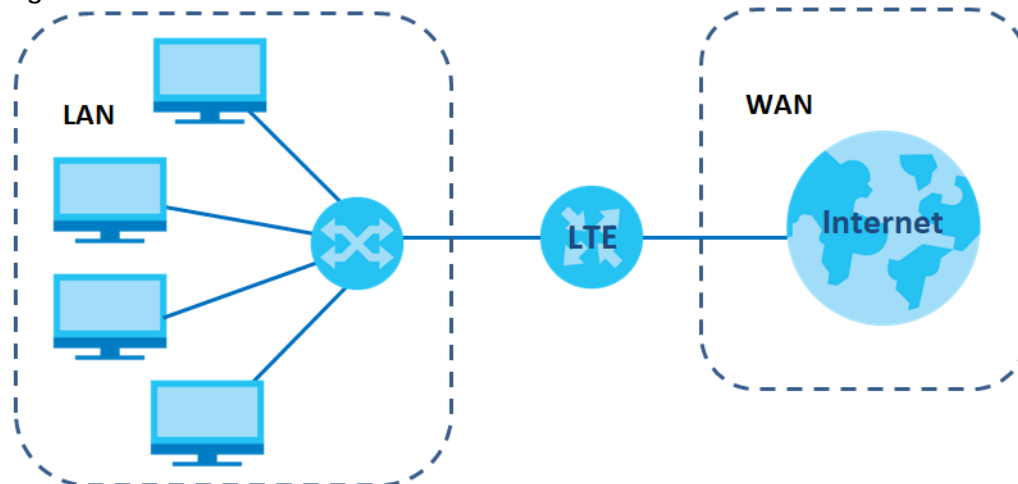
6.5 Technical Reference

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

LANs, WANs and the Zyxel Device

The actual physical connection determines whether the Zyxel Device ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 40 LAN and WAN IP Addresses



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

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

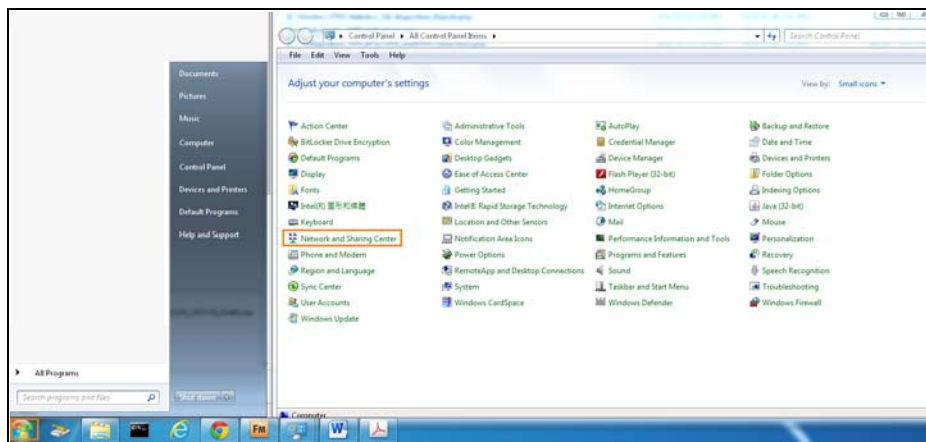
Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, "Address Allocation for Private Internets" and RFC 1466, "Guidelines for Management of IP Address Space."

6.6 Turning on UPnP in Windows 7 Example

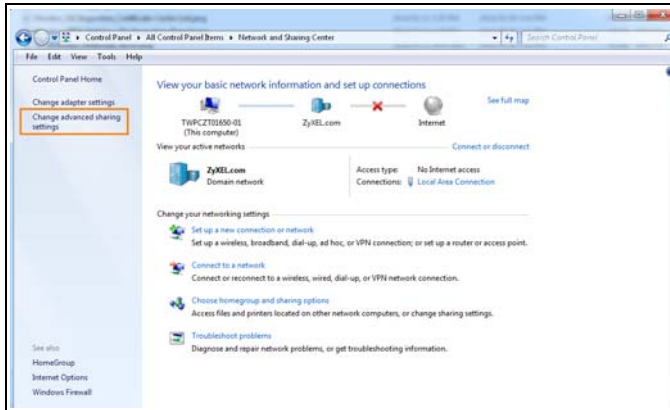
This section shows you how to use the UPnP feature in Windows 7. UPnP server is installed in Windows 7. Activate UPnP on the Zyxel Device.

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

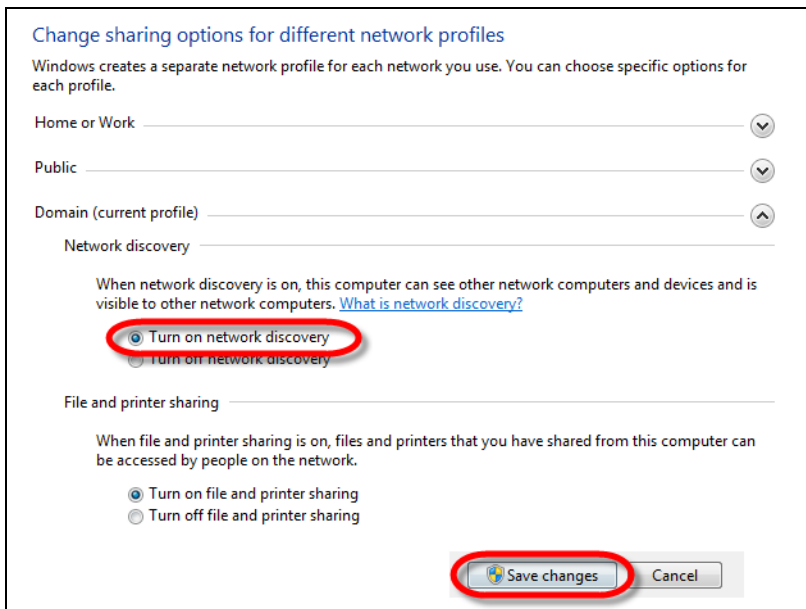
- 1 Click the start icon, **Control Panel** and then the **Network and Sharing Center**.



- 2 Click **Change Advanced Sharing Settings**.



- 3 Select **Turn on network discovery** and click **Save Changes**. Network discovery allows your computer to find other computers and devices on the network and other computers on the network to find your computer. This makes it easier to share files and printers.

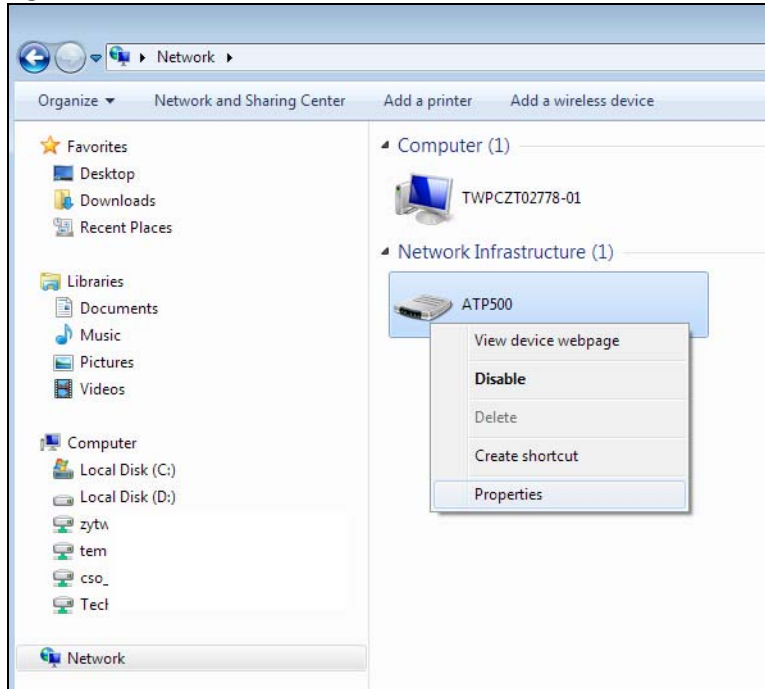


6.6.1 Auto-discover Your UPnP-enabled Network Device

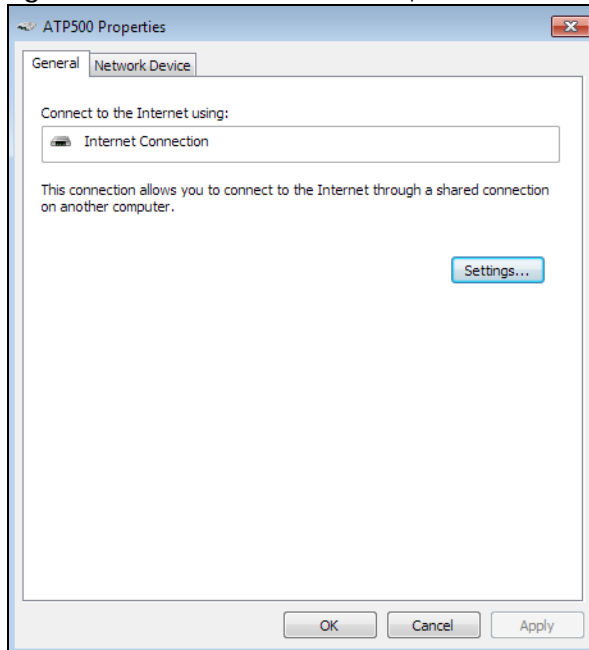
Before you follow these steps, make sure you already have UPnP activated on the Zyxel Device and in your computer.

Make sure your computer is connected to a LAN port of the Zyxel Device.

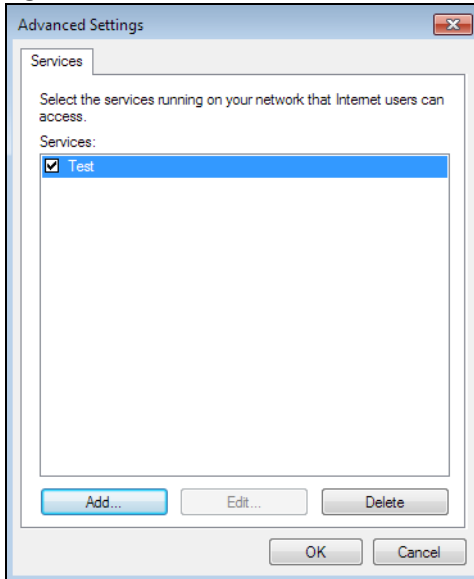
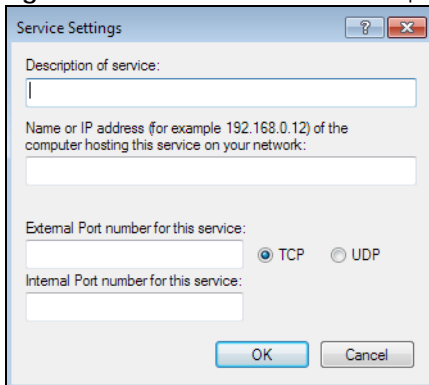
- 1 Open **Windows Explorer** and click **Network**.
- 2 Right-click the device icon and select **Properties**.

Figure 41 Network Connections

- 3 In the **Internet Connection Properties** window, click **Settings** to see port mappings.

Figure 42 Internet Connection Properties

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

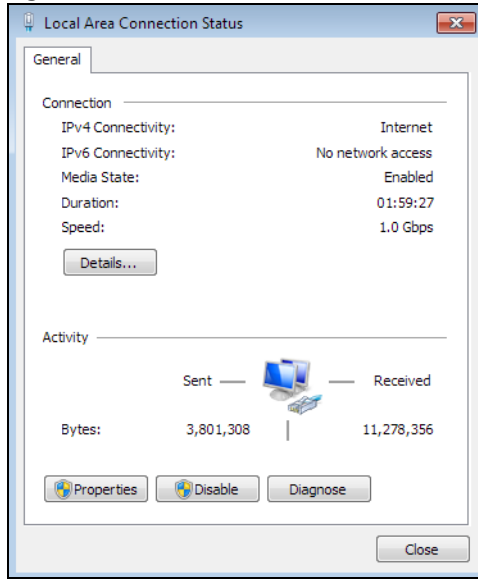
Figure 43 Internet Connection Properties: Advanced Settings**Figure 44** Internet Connection Properties: Advanced Settings: Add

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

- 5 Click **OK**. Check the network icon on system tray to see your Internet connection status.

Figure 45 System Tray Icon

- 6 To see more details about your current Internet connection status, right click the network icon in the system tray and click **Open Network and Sharing Center**. Click **Local Area Network**.

Figure 46 Internet Connection Status

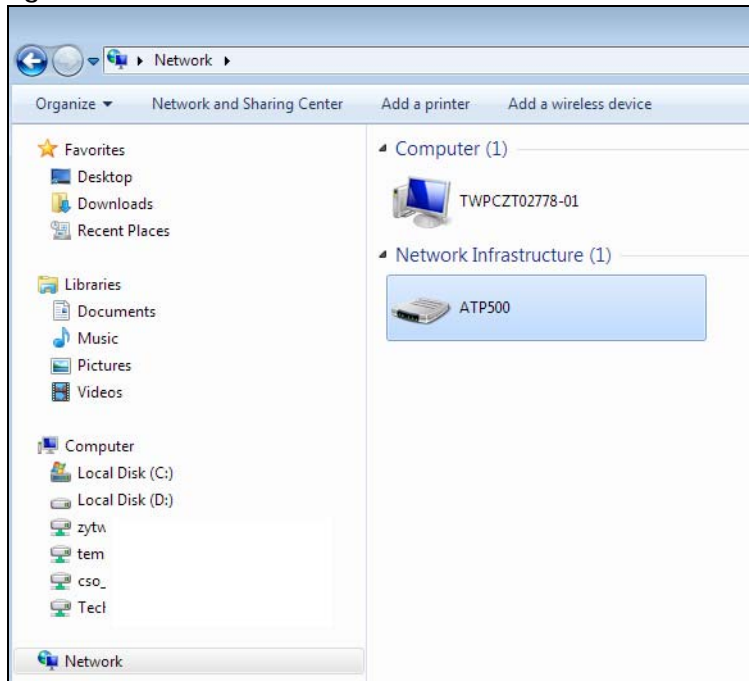
6.7 Web Configurator Easy Access

With UPnP, you can access the Web-based Configurator on the Zyxel Device without needing to find out the IP address of the Zyxel Device first. This comes helpful if you do not know the IP address of the Zyxel Device.

Follow the steps below to access the web configurator.

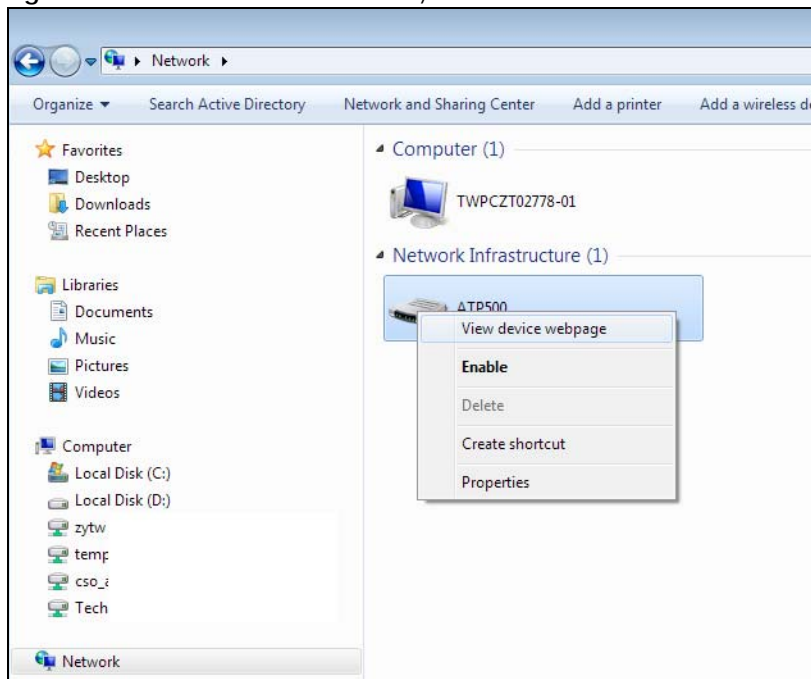
- 1 Open **Windows Explorer**.
- 2 Click **Network**.

Figure 47 Network Connections

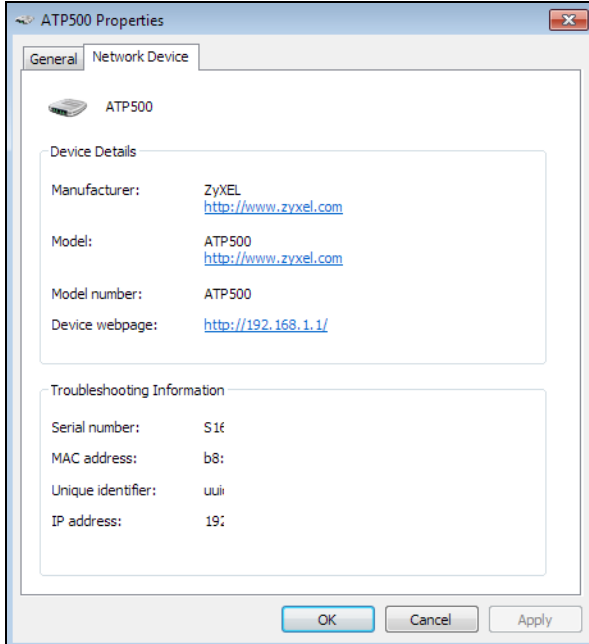


- 3 An icon with the description for each UPnP-enabled device displays under **Network Infrastructure**.
- 4 Right-click the icon for your Zyxel Device and select **View device webpage**. The Web Configurator login screen displays.

Figure 48 Network Connections: My Network Places



- 5 Right-click the icon for your Zyxel Device and select **Properties**. Click the **Network Device** tab. A window displays with information about the Zyxel Device.

Figure 49 Network Connections: My Network Places: Properties: Example

CHAPTER 7

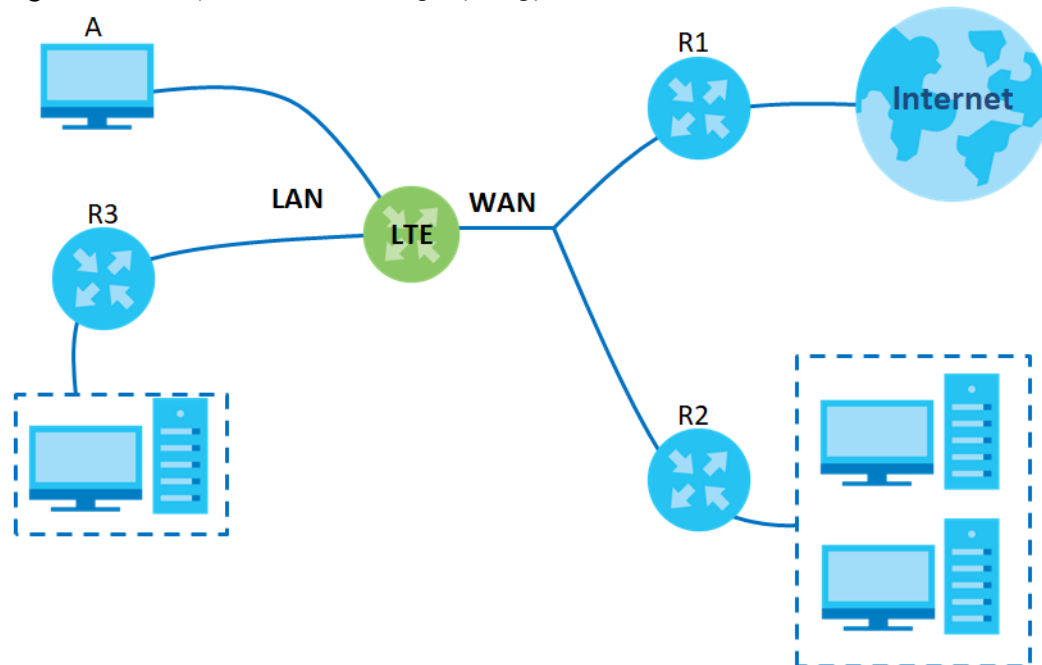
Routing

7.1 Overview

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

For example, the next figure shows a computer (**A**) connected to the Zyxel Device's LAN interface. The Zyxel Device routes most traffic from **A** to the Internet through the Zyxel 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 50 Example of Static Routing Topology



7.2 Configuring Static Route

Use this screen to view and configure the static route rules on the Zyxel Device. The purpose of a static route is to configure a preferred route other than the default route to reduce loading on the default route or to configure routes to networks not (efficiently) reachable via the default gateway. Click **Network Setting > Routing** to open the **Static Route** screen.

Figure 51 Network Setting > Routing > Static Route

The purpose of a Static Route is to save time and bandwidth usage when LAN devices within an Intranet are transferring files or packets, especially when there are more than two Internet connections available in your home or office network.

[Add New Static Route](#)

#	Status	Name	Destination IP	Subnet Mask/Prefix Length	Gateway	Interface	Modify
---	--------	------	----------------	---------------------------	---------	-----------	--------

The following table describes the labels in this screen.

Table 23 Network Setting > Routing > Static Route

LABEL	DESCRIPTION
Add New Static Route	Click this to set up a new static route on the Zyxel Device.
#	This is the number of an individual static route.
Status	This field indicates whether the rule is active (yellow bulb) or not (gray bulb).
Name	This is the name of the static route.
Destination IP	This parameter specifies the IP network address of the final destination. Routing is always based on the network number.
Subnet Mask/Prefix Length	This parameter specifies the IP network subnet mask of the final destination.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Interface	This is the WAN interface through which the traffic is routed.
Modify	Click the Edit icon to go to the screen where you can set up a static route on the Zyxel Device. Click the Delete icon to remove a static route from the Zyxel Device.

7.2.1 Add/Edit Static Route

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

Note: The **Gateway IP Address** must be within the range of the selected interface in **Use Interface**.

Figure 52 Routing: Add New Static Route

The following table describes the labels in this screen.

Table 24 Routing: Add/Edit

LABEL	DESCRIPTION
Active	Activates static route.
Route Name	Assign a name for your static route.
IP Type	Select between IPv4 or IPv6 . Compared to IPv4 , IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 x 1038 IP addresses. The Zyxel Device can use IPv4/IPv6 dual stack to connect to IPv4 and IPv6 networks, and supports IPv6 rapid deployment (6RD).
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.
Use Gateway IP Address	Enables forwarding packets to a gateway IP address or a bound interface.
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 the 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.
Use Interface	You can decide if you want to forward packets to a gateway IP address (Default) or a bound interface (Cellular WAN). 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.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

7.3 The DNS Route Screen

Use this screen to view and configure DNS routes on the Zyxel Device. DNS route entry defines a policy for the device to forward a particular DNS query to a specific WAN interface. The **DNS Route** screen lets you view and configure DNS routes on the Zyxel Device. Click **Network Setting > Routing > DNS Route** to open the **DNS Route** screen.

Figure 53 Network Setting > Routing > DNS Route

A DNS route entry defines a policy for the device to forward particular DNS query to a specific WAN interface.

Add New DNS Route

#	Status	Domain Name	WAN Interface	Subnet Mask	Modify
---	--------	-------------	---------------	-------------	--------

Note
Maximum of 20 entries can be added.

The following table describes the labels in this screen.

Table 25 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.
Status	This field indicates whether the rule is active (yellow bulb) or not (gray bulb).
Domain Name	This is the domain name to which the DNS route applies.
WAN Interface	This is the WAN interface through which the matched DNS request is routed.
Subnet Mask	This parameter specifies the IP network subnet mask.
Modify	Click the Edit icon to configure a DNS route on the Zyxel Device. Click the Delete icon to remove a DNS route from the Zyxel Device.

7.3.1 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 54 Add New DNS Route

The following table describes the labels in this screen.

Table 26 DNS Route: Add/Edit

LABEL	DESCRIPTION
Active	Enable DNS route in your Zyxel Device.
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 Zyxel 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.
WAN 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.
Cancel	Click this to exit this screen without saving.

7.4 The Policy Route Screen

Traditionally, routing is based on the destination address only and the Zyxel Device takes the shortest path to forward a packet. Policy routes allow the Zyxel Device to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to outgoing packets, prior to the normal routing. This allows you to save time and bandwidth usage when LAN devices within an Intranet are transferring files or packets, especially when there are more than two Internet connections available in your home or office network.

You can use source-based policy forwarding to direct traffic from different users through different connections or distribute traffic among multiple paths for load sharing.

Use this screen to view and configure routing policies on the Zyxel Device. Click **Network Setting > Routing > Policy Route** to open the following screen.

Figure 55 Network Setting > Routing > Policy Route

#	Status	Name	Source IP	Source Subnet Mask	Protocol	Source Port	Source MAC	Source Interface	WAN Interface	Modify
---	--------	------	-----------	--------------------	----------	-------------	------------	------------------	---------------	--------

The following table describes the labels in this screen.

Table 27 Network Setting > Routing > Policy Route

LABEL	DESCRIPTION
Add New Policy Route	Click this to create a new policy forwarding rule.
#	This is the index number of the entry.
Status	This field displays whether the DNS route is active or not. A yellow bulb signifies that this DNS route is active. A gray bulb signifies that this DNS route is not active.
Name	This is the name of the rule.
Source IP	This is the source IP address.
Source Subnet Mask	This is the source subnet mask address.
Protocol	This is the transport layer protocol.
Source Port	This is the source port number.
Source MAC	This is the source MAC address.
Source Interface	This is the interface from which the matched traffic is sent.
WAN Interface	This is the WAN interface through which the traffic is routed.
Modify	Click the Edit icon to edit this policy. Click the Delete icon to remove a policy from the Zyxel Device. A window displays asking you to confirm that you want to delete the policy.

7.4.1 Add/Edit Policy Route

Click **Add New Policy Route** in the **Policy Route** screen or click the **Edit** icon next to a policy. Use this screen to configure the required information for a policy route.

Figure 56 Policy Route: Add/Edit

The following table describes the labels in this screen.

Table 28 Policy Route: Add/Edit

LABEL	DESCRIPTION
Active	Click Enable to activate the policy route. Otherwise, select Disable .
Route Name	Enter a descriptive name of up to 8 printable English keyboard characters, not including spaces.
Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the source subnet mask address.
Protocol	Select the transport layer protocol (TCP or UDP).
Source Port	Enter the source port number.
Source MAC	Enter the source MAC address.
Source Interface (ex: br0 or LAN1~LAN4)	Type the name of the interface from which the matched traffic is sent.
WAN Interface	Select a WAN interface through which the traffic is sent. You must have the WAN interface(s) already configured in the Broadband screens.
Cancel	Click Cancel to exit this screen without saving.
OK	Click OK to save your changes.

7.5 RIP

Routing Information Protocol (RIP, RFC 1058 and RFC 1389) allows a device to exchange routing information with other routers. To activate RIP for the WAN interface, select the desired RIP version and operation.

7.5.1 The RIP Screen

Click **Network Setting** > **Routing** > **RIP** to open the **RIP** screen. Select the desired RIP version and operation by clicking the check box. To stop RIP on the WAN interface, clear the check box. Click the **Apply** button to start/stop RIP and save the configuration.

Figure 57 Network Setting > Routing > RIP

#	Interface	Version	Operation	Enable	Disable Default Gateway
1	Cellular WAN	2	Active	<input type="checkbox"/>	<input type="checkbox"/>

Apply Cancel

The following table describes the labels in this screen.

Table 29 Network Setting > Routing > RIP

LABEL	DESCRIPTION
#	This is the index of the interface in which the RIP setting is used.
Interface	This is the name of the interface in which the RIP setting is used.
Version	The RIP version controls the format and the broadcasting method of the RIP packets that the Zyxel Device sends (it recognizes both formats when receiving). RIP version 1 is universally supported but RIP version 2 carries more information. RIP version 1 is probably adequate for most networks, unless you have an unusual network topology.
Operation	<p>Select Passive to have the Zyxel Device update the routing table based on the RIP packets received from neighbors but not advertise its route information to other routers in this interface.</p> <p>Select Active to have the Zyxel Device advertise its route information and also listen for routing updates from neighboring routers.</p>
Enable	Select the check box to activate the settings.
Disable Default Gateway	Select the check box to set the Zyxel Device to not send the route information to the default gateway.
Cancel	Click Cancel to exit this screen without saving.
Apply	Click Apply to save your changes back to the Zyxel Device.

CHAPTER 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 **Port Forwarding** screen to configure forward incoming service requests to the servers on your local network ([Section 8.2 on page 86](#)).
- Use the **Applications** screen to provide commonly seen Internet activities by categories and make configuring port forwarding easier ([Section 8.3 on page 89](#)).
- Use the **Port Triggering** screen to add and configure the Zyxel Device's trigger port settings ([Section 8.4 on page 91](#)).
- Use the **DMZ** screen to configure a default server ([Section 8.5 on page 94](#)).
- Use the **ALG** screen to enable or disable the SIP ALG ([Section 8.6 on page 95](#)).

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 Zyxel 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 on page 95](#) for advanced technical information on NAT.

8.2 The Port Forwarding Screen

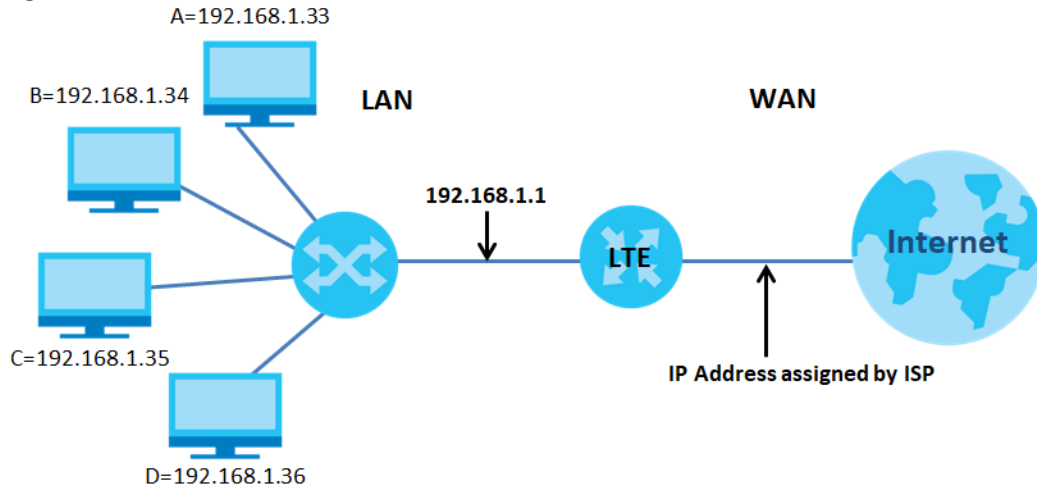
Use **Port Forwarding** to forward incoming service requests from the Internet to the server(s) on your local network. Port forwarding is commonly used when you want to host online gaming, P2P file sharing, or other servers on your network.

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), a default server IP address of 192.168.1.35 to a third (**C** in the example), and a default server IP address of 192.168.1.36 to a fourth (**D** 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 58 Multiple Servers Behind NAT Example

8.2.1 The Port Forwarding Screen

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

Note: TCP port 7547 is reserved for system use.

Figure 59 Network Setting > NAT > Port Forwarding

The following table describes the fields in this screen.

Table 30 Network Setting > NAT > Port Forwarding

LABEL	DESCRIPTION
Add New Rule	Click this to add a new port forwarding rule.
#	This is the index number of the entry.
Status	This field indicates whether the rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Service Name	This is the service's name. This shows User Defined if you manually added a service. You can change this by clicking the edit icon.
Originating IP	This is the source's IP address.
WAN Interface	Select the WAN interface for which to configure NAT port forwarding rules.

Table 30 Network Setting > NAT > Port Forwarding (continued)

LABEL	DESCRIPTION
Server IP Address	This is the server's IP address.
Start Port	This is the first external port number that identifies a service.
End Port	This is the last external port number that identifies a service.
Translation Start Port	This is the first internal port number that identifies a service.
Translation End Port	This is the last internal port number that identifies a service.
Protocol	This field displays the protocol (TCP, UDP, TCP+UDP) used to transport the packets for which you want to apply the rule.
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.

8.2.2 Add/Edit Port Forwarding

This screen lets you create or edit a port forwarding rule. Specify either a port or a range of ports, a server IP address, and a protocol to configure 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 60 Port Forwarding: Add/Edit

Add New Rule

Active: ☐ Enable ☒ Disable

Service Name:

WAN Interface:

Start Port:

End Port:

Translation Start Port:

Translation End Port:

Server IP Address:

Configure Originating IP: ☐ Enable

Protocol:

Note

1. If Start Port and Translation Start Port, End Port and Translation End Port are configured the same, then Port Forwarding is configured. If Start Port and Translation Start Port, End Port and Translation End Port are configured differently, then Port Translation is configured (one to one mapping).
For example: Start Port: 100 End Port: 120; Translation Start Port: 200 Translation End Port: 220
2. Originating IP is optional. User must enable Configure Originating IP to add a source IP address which from the WAN Interface.

OK Cancel

Note: To configure port forwarding, you need to have the same configurations in the **Start Port**, **End Port**, **Translation Start Port**, and **Translation End Port** fields.

To configure port translation, you need to have different configurations in the **Start Port**, **End Port**, **Translation Start Port**, and **Translation End Port** fields.

TCP port 7547 is reserved for system use.

The following table describes the labels in this screen.

Table 31 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.
WAN Interface	Select the WAN interface for which to configure NAT port forwarding rules.
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 End Port field. To forward a series of ports, enter the start port number here and the end port number in the End Port field.
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 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 Start Port field above.
Translation Start Port	Configure this for a user-defined entry. This shows the port number to which you want the Zyxel Device to translate the incoming port. For a range of ports, enter the first number of the range to which you want the incoming ports translated.
Translation End Port	Configure this for a user-defined entry. This shows the last port of the translated port range.
Server IP Address	Enter the inside IP address of the virtual server here.
Protocol	Select the protocol supported by this virtual server. Choices are TCP , UDP , or TCP/UDP .
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

8.3 The Applications Screen

Use this screen to define and forward specific application requests from the Internet to the server(s) on your local network. Use this instead of Port Forwarding when some services, like games are hard to define using port ranges.

Note: TCP port 7547 is reserved for system use.

Click **Network Setting > NAT > Applications** to open the following screen.

Figure 61 Network Setting > NAT > Applications

Each and every Internet activity such as, online gaming and online video streaming, requires at least a port to communicate. Applications provide commonly seen Internet activities by categories and make configuring port forwarding easier.

Add New Application

#	Application Forwarded:	WAN Interface:	Server IP Address:	Modify
<p>Note</p> <p>The TCP port 7547 is reserved for system usage.</p>				

The following table describes the fields in this screen.

Table 32 Network Setting > NAT > Applications

LABEL	DESCRIPTION
Add New Application	Click this to add a new application.
#	This is the index number of the entry.
Application Forwarded	This shows the application's name.
WAN Interface	This shows the WAN interface through which the application is forwarded.
Server IP Address	This is the server's IP address.
Modify	Click the Edit icon to edit this rule. Click the Delete icon to delete an existing rule.

8.3.1 The Applications Add/Edit Screen

This screen lets you create or edit an application rule. Click **Add New Application** in the **Applications** screen or the **Edit** icon next to an existing rule to open the following screen.

Figure 62 Applications: Add/Edit

Add New Application

WAN Interface: Cellular WAN ▼

Server IP Address: . . .

Application Category: Games ▼

Application Forwarded: Age of Empires ▼

View Rules

OK Cancel

The following table describes the labels in this screen.

Table 33 Applications: Add/Edit

LABEL	DESCRIPTION
WAN Interface	Select the WAN interface for which to configure NAT application rules.
Server IP Address	Enter the inside IP address of the virtual server here.
Application Category	Select the application's category supported by this virtual server.
Application Forwarded	Select the correct type of server/service/device from the Application Forwarded list. You can check which ports will be opened by this rule by clicking the View Rules button.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

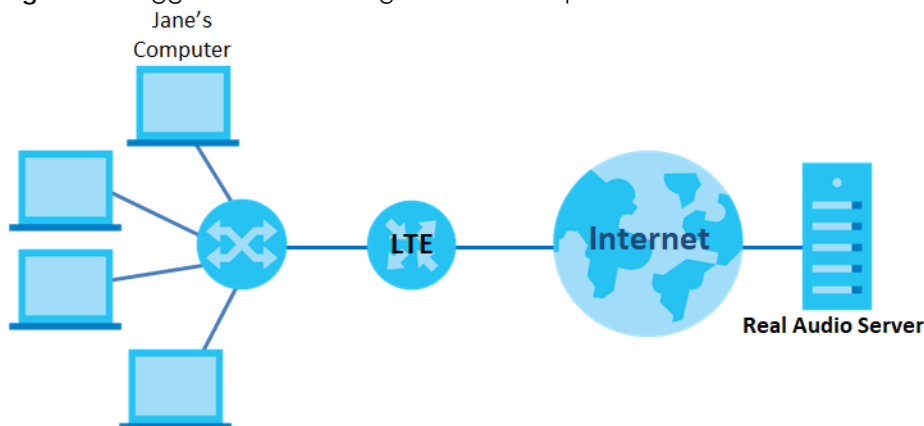
8.4 The Port Triggering Screen

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

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

For example:

Figure 63 Trigger Port Forwarding Process: Example



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

- 2 Port 7070 is a "trigger" port and causes the Zyxel Device to record Jane's computer IP address. The Zyxel Device associates Jane's computer IP address with the "open" port range of 6970-7170.
- 3 The Real Audio server responds using a port number ranging between 6970-7170.
- 4 The Zyxel Device forwards the traffic to Jane's computer IP address.
- 5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The Zyxel Device times out in three minutes with UDP (User Datagram Protocol) or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

Click **Network Setting > NAT > Port Triggering** to open the following screen. Use this screen to view your Zyxel Device's trigger port settings.

Note: TCP port 7547 is reserved for system use.

Note: The maximum number of trigger ports for a single rule or all rules is 999.

Note: The maximum number of open ports for a single rule or all rules is 999.

Figure 64 Network Setting > NAT > Port Triggering

Port Triggering is a way to automate port forwarding with a little better security. It dynamically forwards connection or data to whatever LAN client made a certain outgoing connection. Example: You define port 25 as Trigger Port and port 113 as Open Port. If any of the LAN devices on your network creates an outgoing connection via port 25, all incoming connections via port 113 will temporarily go to that client.

Add New Rule

#	Status	Service Name	WAN Interface	Trigger Start Port	Trigger End Port	Trigger Proto.	Open Start Port	Open End Port	Open Protocol	Modify
<p>Note</p> <p>1. The sum of trigger ports in all rules must be less than 1000 and every open port range must be less than 1000. When the protocol is TCP/UDP, the ports are counted twice.</p> <p>2. The TCP port 7547 is reserved for system usage.</p>										

The following table describes the labels in this screen.

Table 34 Network Setting > NAT > Port Triggering

LABEL	DESCRIPTION
Add New Rule	Click this to create a new rule.
#	This is the index number of the entry.
Status	This field displays whether the port triggering rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Service Name	This field displays the name of the service used by this rule.
WAN Interface	This field shows the WAN interface through which the service is forwarded.
Trigger Start Port	The trigger port is a port (or a range of ports) that causes (or triggers) the Zyxel Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN. This is the first port number that identifies a service.
Trigger End Port	This is the last port number that identifies a service.

Table 34 Network Setting > NAT > Port Triggering (continued)

LABEL	DESCRIPTION
Trigger Proto.	This is the trigger transport layer protocol.
Open Start Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The Zyxel Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. This is the first port number that identifies a service.
Open End Port	This is the last port number that identifies a service.
Open Protocol	This is the open transport layer protocol.
Modify	Click the Edit icon to edit this rule. Click the Delete icon to delete an existing rule.

8.4.1 Add/Edit Port Triggering Rule

This screen lets you create new port triggering rules. Click **Add New Rule** in the **Port Triggering** screen or click a rule's **Edit** icon to open the following screen. Use this screen to configure a port or range of ports and protocols for sending out requests and for receiving responses.

Figure 65 Port Triggering: Add/Edit

The following table describes the labels in this screen.

Table 35 Port Triggering: Configuration Add/Edit

LABEL	DESCRIPTION
Active	Select Enable or Disable to activate or deactivate the rule.
Service Name	Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on).
WAN Interface	Select a WAN interface for which you want to configure port triggering rules.
Trigger Start Port	The trigger port is a port (or a range of ports) that causes (or triggers) the Zyxel Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN. Type a port number or the starting port number in a range of port numbers.
Trigger End Port	Type a port number or the ending port number in a range of port numbers.
Trigger Protocol	Select the transport layer protocol from TCP , UDP , or TCP/UDP .

Table 35 Port Triggering: Configuration Add/Edit (continued)

LABEL	DESCRIPTION
Open Start Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The Zyxel Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. Type a port number or the starting port number in a range of port numbers.
Open End Port	Type a port number or the ending port number in a range of port numbers.
Open Protocol	Select the transport layer protocol from TCP , UDP , or TCP/UDP .
Cancel	Click Cancel to exit this screen without saving.
OK	Click OK to save your changes.

8.5 The DMZ Screen

A client in the Demilitarized Zone (DMZ) is no longer behind the Zyxel Device and therefore can run any Internet applications such as video conferencing and Internet gaming without restrictions. This, however, may pose a security threat to the Zyxel Device. Use this screen to specify the IP address of a default server to receive packets from ports not specified in the **Port Triggering** screen. Click **Network Setting > NAT > DMZ** to open the **DMZ** screen.

Note: Use an IPv4 address for the DMZ server.

Note: Enter the IP address and click "Apply" to activate the DMZ host.

Otherwise, clear the IP address field and click "Apply" to de-activate the DMZ host.

Figure 66 Network Setting > NAT > DMZ

The LAN client in the Demilitarized Zone (DMZ) is no longer behind this device and therefore can run any Internet applications such as, video conferencing and Internet gaming without restrictions, but with the same reason, it also uncover itself to Internet security threats.

Default Server Address :

Note:
Enter IP address and click "Apply" to activate the DMZ host.
Clear the IP address field and click "Apply" to de-activate the DMZ host.

The following table describes the fields in this screen.

Table 36 Network Setting > NAT > DMZ

LABEL	DESCRIPTION
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 Zyxel Device discards all packets received for ports not specified in the virtual server configuration.
Apply	Click this to save your changes back to the Zyxel Device.
Cancel	Click Cancel to restore your previously saved settings.

8.6 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 Zyxel Device.

Application Layer Gateway (ALG) allows certain applications such as File Transfer Protocol (FTP), Session Initiation Protocol (SIP), or file transfer in Instant Messaging (IM) applications to pass through the Zyxel Device.

Figure 67 Network Setting > NAT > ALG

The following table describes the fields in this screen.

Table 37 Network Setting > NAT > ALG

LABEL	DESCRIPTION
SIP ALG	Enable this to make sure SIP (VoIP) works correctly with port-forwarding and address-mapping rules. Otherwise, select Disable to turn off the SIP ALG.
PPTP ALG	Enable this to turn on the PPTP ALG on the Zyxel Device to detect PPTP traffic and help build PPTP sessions through the Zyxel Device's NAT.
Apply	Click this to save your changes back to the Zyxel Device.
Cancel	Click Cancel to restore your previously saved settings.

CHAPTER 9

DNS Setup

9.1 Overview

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 Can Do in this Chapter

- Use the **DNS Entry** screen to view, configure, or remove DNS routes ([Section 9.2 on page 96](#)).
- Use the **Dynamic DNS** screen to enable DDNS and configure the DDNS settings on the Zyxel Device ([Section 9.3 on page 98](#)).

9.1.2 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 DNS Entry Screen

DNS (Domain Name System) is used for mapping a domain name to its corresponding IP address and vice versa. Use this screen to view and configure DNS rules on the Zyxel Device. Click **Network Setting > DNS** to open the **DNS Entry** screen.

Note: The host name should consist of the host's local name and the domain name. For example, Mycomputer.home is a host name where Mycomputer is the host's local name, and .home is the domain name.

Figure 68 Network Setting > DNS > DNS Entry

Domain Name System(DNS) translates hostnames into IP addresses for the purpose of locating and addressing these devices worldwide. You can start by adding a new DNS entry.

Add New DNS Entry

#	HostName	IP Address	Modify
<p>Note:</p> <p>The hostnames requires a combination of the host's local name with its domain name, for example, Mycomputer.home consists of a local hostname (Mycomputer) and the domain name (home).</p>			

The following table describes the fields in this screen.

Table 38 Network Setting > DNS > DNS Entry

LABEL	DESCRIPTION
Add New DNS Entry	Click this to create a new DNS entry.
#	This is the index number of the entry.
Host Name	This indicates the host name or domain name.
IP Address	This indicates the IP address assigned to this computer.
Modify	Click the Edit icon to edit the rule. Click the Delete icon to delete an existing rule.

9.2.1 Add/Edit DNS Entry

You can manually add or edit the Zyxel Device's DNS name and IP address entry. Click **Add New DNS Entry** in the **DNS Entry** screen or the **Edit** icon next to the entry you want to edit. The screen shown next appears.

Figure 69 DNS Entry: Add/Edit

DNS Entry Configuration

Host Name :

IPv4 Address :

The following table describes the labels in this screen.

Table 39 DNS Entry: Add/Edit

LABEL	DESCRIPTION
Host Name	Enter the host name of the DNS entry.
IP Address	Enter the IP address of the DNS entry.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

9.3 The Dynamic DNS Screen

Dynamic DNS can update your current dynamic IP address mapping to a hostname. Use this screen to enable DDNS and configure the DDNS service provider on your Zyxel Device. To change your Zyxel Device's DDNS, click **Network Setting > DNS > Dynamic DNS**. The screen appears as shown.

Figure 70 Network Setting > Dynamic DNS

The following table describes the fields in this screen.

Table 40 Network Setting > DNS > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Dynamic DNS	Select Enable to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
Host/Domain Name	Type the domain name assigned to your Zyxel 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.
Dynamic DNS Status	

Table 40 Network Setting > DNS > Dynamic DNS (continued)

LABEL	DESCRIPTION
User Authentication Result	This field displays the results of the Zyxel Device's attempt to authenticate with the Dynamic DNS service provider.
Last Updated Time	This field displays when the Zyxel Device last updated its WAN IP address to the Dynamic DNS service provider.
Current Dynamic IP	This field displays the Zyxel Device's current WAN IP address.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

CHAPTER 10

Firewall

10.1 Overview

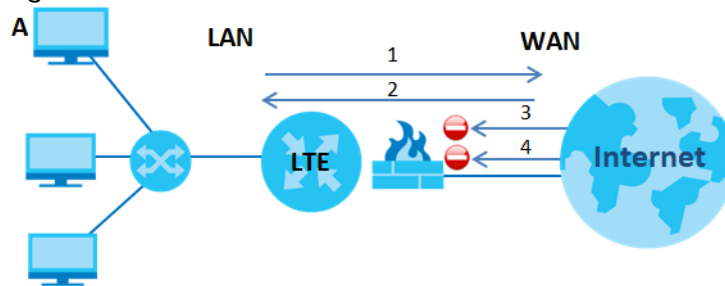
This chapter shows you how to enable the Zyxel Device firewall. Use the firewall to protect your Zyxel Device and network from attacks by hackers on the Internet and control access to it. The firewall:

- 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.

By default, the Zyxel Device blocks DOS 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 71 Default Firewall Action



10.1.1 What You Need to Know About Firewall

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 Zyxel Device is pre-configured to automatically detect and thwart all known DoS attacks.

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 Zyxel 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 The Firewall Screen

10.2.1 What You Can Do in this Chapter

- Use the **General** screen to configure the security level of the firewall on the Zyxel Device ([Section 10.3 on page 101](#)).
- Use the **Protocol** screen to add or remove predefined Internet services and configure firewall rules ([Section 10.4 on page 102](#)).
- Use the **Access Control** screen to view and configure incoming/outgoing filtering rules ([Section 10.5 on page 104](#)).
- Use the **DoS** screen to activate protection against Denial of Service (DoS) attacks ([Section 10.6 on page 108](#)).

10.3 The Firewall General Screen

Use the firewall to protect your Zyxel Device and network from attacks by hackers on the Internet and control access to it. Use this screen to set the security level of the firewall on the Zyxel Device. Firewall rules are grouped based on the direction of travel of packets to which they apply. A higher firewall level means more restrictions on the Internet activities you can perform. Click **Security > Firewall > General** to display the following screen. Use the slider to select the level of firewall protection.

Figure 72 Security > Firewall > General

The firewall blocks unauthorized access to your network. Drag and drop the indicator to set a security level. Also note that a higher firewall level means more restrictions to the Internet activities you want to perform.

IPv4 Firewall ☒ Enable ☐ Disable

IPv6 Firewall ☒ Enable ☐ Disable

Low Medium (Recommended) High

Direction	Low	Medium (Recommended)	High
LAN to WAN	✓	✓	✗
WAN to LAN	✓	✗	✗

Note:

(1) LAN to WAN: Allow access to all internet services

(2) WAN to LAN: Allow access from other computers on the internet

(3) When the security level is set to "High", access to the following services is allowed: Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3, SMTP and IPv6 Ping

Apply Cancel

Note: LAN to WAN is your access to all Internet services. WAN to LAN is the access of other computers on the Internet to devices behind the Zyxel Device.

When the security level is set to **High**, access to Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3, SMTP, and IPv6 Ping are still allowed from the LAN.

The following table describes the labels in this screen.

Table 41 Security > Firewall > General

LABEL	DESCRIPTION
IPv4 Firewall	Enable firewall protection when using IPv4 (Internet Protocol version 4).
IPv6 Firewall	Enable firewall protection when using IPv6 (Internet Protocol version 6).
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.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

10.4 The Protocol (Customized Services) Screen

Services include e-Mail, File sharing, Instant messaging, Online games, Print servers, Voice over IP and so on. You use port numbers to define a service. Define services in this screen that you can apply access

control rules to in the **Access Control** screen. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. Click **Security > Firewall > Protocol** to display the following screen.

Note: Removing a protocol rule will also remove associated ACL rules.

Figure 73 Security > Firewall > Protocol

The following table describes the labels in this screen.

Table 42 Security > Firewall > Protocol

LABEL	DESCRIPTION
Add New Protocol Entry	Click this to configure a customized service.
Name	This is the name of your customized service.
Description	This is a description of your customized service.
Ports/Protocol Number	This shows the port number or range and the IP protocol (TCP or UDP) that defines your customized service.
Modify	Click this to edit a customized service.

10.4.1 Add Customized Service

Use this screen to add a customized rule or edit an existing rule. Click **Add New Protocol Entry** in the **Protocol** screen to display the following screen.

Figure 74 Security > Firewall > Protocol: Add New Protocol Entry

The following table describes the labels in this screen.

Table 43 Security > Firewall > Protocol: Add New Protocol Entry

LABEL	DESCRIPTION
Service Name	Type a unique name for your custom port.
Description	Enter a description for your custom port.
Protocol	Choose the IP port (TCP , UDP , ICMP , ICMPv6 , Other) that defines your customized port from the drop down list box.
Protocol Number	Type a single port number or the range of port numbers (0-255) that define your customized service.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

10.5 The Access Control (Rules) Screen

An Access Control List (ACL) rule is a manually-defined rule that can accept, reject, or drop incoming or outgoing packets from your network based on the type of service. For example, you could block users using Instant Messaging in your network. This screen displays a list of the configured incoming or outgoing filtering rules. Note the order in which the rules are listed. Click **Security > Firewall > Access Control** to display the following screen.

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

Figure 75 Security > Firewall > Access Control

An ACL rule is a manually defined rule to accept, reject, or drop the incoming or outgoing data of your network. You may need to create at least one Protocol entry in order to add an ACL rule.

Rules Storage Space Usage(%): 0%

Add New ACL Rule

#	Name	Src IP	Dst IP	Service	Action	Modify
---	------	--------	--------	---------	--------	--------

The following table describes the labels in this screen.

Table 44 Security > Firewall > Rules

LABEL	DESCRIPTION
Rules Storage Space Usage	This read-only bar shows how much of the Zyxel Device's memory for recording firewall rules it is currently using. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red.
Add New ACL Rule	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 field displays the rule index number. The ordering of your rules is important as rules are applied in turn.
Name	This field displays the rule name.
Src IP	This field displays the source IP addresses to which this rule applies.
Dst IP	This field displays the destination IP addresses to which this rule applies.
Service	This field displays the protocol (TCP, UDP, TCP+UDP or any) used to transport the packets for which you want to apply the rule.
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 allow the passage of (Accept) packets that match this rule.
Modify	Click the Edit icon to edit the firewall rule. Click the Delete icon to delete an existing firewall rule.

10.5.1 Access Control Add New ACL Rule Screen

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

Figure 76 Security > Firewall > Access Control > Add New ACL Rule

The following table describes the labels in this screen.

Table 45 Security > Firewall > Access Control > Add New ACL Rule

LABEL	DESCRIPTION
Filter Name	Type a unique name for your filter rule.
Order	Assign the order of your rules as rules are applied in turn.
Select Source Device	If you want the source to come from a particular (single) IP, select Specific IP Address . If not, select from a detected device.
Source IP Address	If you selected Specific IP Address in the previous item, enter the source device's IP address here. Otherwise this field will be hidden if you select the detected device.
Select Destination Device	If you want your rule to apply to packets with a particular (single) IP, select Specific IP Address . If not, select a detected device.
Destination IP Address	If you selected Specific IP Address in the previous item, enter the destination device's IP address here. Otherwise this field will be hidden if you select the detected device.
IP Type	Select between IPv4 or IPv6 . Compared to IPv4 , IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 x 1038 IP addresses. The Zyxel Device can use IPv4/IPv6 dual stack to connect to IPv4 and IPv6 networks, and supports IPv6 rapid deployment (6RD).
Select Service	Select a service from the Select Service box.
Protocol	Select the protocol (ALL , TCP/UDP , TCP , UDP , ICMP , ICMPv6) used to transport the packets for which you want to apply the rule.
Custom Source Port	This is a single port number or the starting port number of a range that defines your rule.

Table 45 Security > Firewall > Access Control > Add New ACL Rule (continued)

LABEL	DESCRIPTION
Custom Destination Port	This is a single port number or the ending port number of a range that defines your rule.
Policy	Use the drop-down list box to select whether to discard (Drop), deny and send an ICMP destination-unreachable message to the sender (Reject), or allow the passage of (Accept) packets that match this rule.
Direction	Select WAN to LAN to apply the rule to traffic from WAN to LAN. Select LAN to WAN to apply the rule to traffic from LAN to WAN. Select WAN to Router to apply the rule to traffic from WAN to router. Select LAN to Router to apply the rule to traffic from LAN to router.
Enable Rate Limit	Enable the setting of maximum number of packets per maximum number of minute(s) to limit the throughput of traffic that matches this rule.
Scheduler Rules	
Add New Rule	Click this to bring up the next screen.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

10.5.2 Scheduler Rules

A scheduler rule is a defined time period. For example, Monday to Friday, 6-10PM could be a scheduler rule that could be applied to an ACL to only allow gaming at that time. Use this screen to add a new rule, view the list of rules, as well as edit or delete an existing rule. Various details such as **Rule Name**, **Day** and **Time** when the rule will apply, as well as a description of the rule are shown. The ordering is important as rules are applied in turn.

Figure 77 Security > Firewall > Access Control > Add New ACL Rule > Scheduler Rule

#	Rule Name	Day	Time	Description	Modify
---	-----------	-----	------	-------------	--------

The following table describes the labels in this screen.

Table 46 Security > Firewall > Access Control > Add New ACL Rule > Scheduler Rule

LABEL	DESCRIPTION
Add New Rule	Click this to bring up the next screen.
#	This field displays the rule index number. The ordering of your rules is important as rules are applied in turn.
Rule Name	This field displays the rule name.
Day	This field displays the day of the week to which this rule applies.
Time	This field displays the time of the day to which this rule applies.
Description	This is a brief explanation of the rule that use this service.
Modify	Click the Edit icon to edit the scheduler rule. Click the Delete icon to delete an existing scheduler rule.

Figure 78 Security > Firewall > Access Control > Add New ACL Rule > Scheduler Rule > Add New Rule

The following table describes the labels in this screen.

Table 47 Security > Firewall > Access Control > Add New ACL Rule > Scheduler Rule > Add New Rule

LABEL	DESCRIPTION
Rule Name	Assign a name for your scheduler rule.
Day	Select the day(s) during which to apply the rule.
Time of Day Range	Select the time of the day when to apply the rule.
Description	Enter a brief explanation of the rule that use this service.

10.6 DoS Screen

DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable.

Use this screen to activate protection against DoS attacks. Click **Security > Firewall > DoS** to display the following screen.

Figure 79 Security > Firewall > DoS

The following table describes the labels in this screen.

Table 48 Security > Firewall > DoS

LABEL	DESCRIPTION
DoS Protection Blocking	Enable this to protect against DoS attacks. The Zyxel Device will drop sessions that surpass maximum thresholds.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

10.7 Firewall Technical Reference

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

10.7.1 Firewall Rules Overview

Your customized rules take precedence and override the Zyxel Device's default settings. The Zyxel 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 Zyxel 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 Zyxel 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 Zyxel Device (remote management).

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

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

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

Note: You also need to configure the remote management settings to allow a WAN computer to manage the Zyxel 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 Zyxel Device's default rules.

10.7.2 Guidelines For Enhancing Security With Your Firewall

- 1 Change the default password via the 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.

10.7.3 Security Considerations

Note: Incorrectly configuring the firewall may block valid access or introduce security risks to the Zyxel 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 (Internet Relay Chat) 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.

CHAPTER 11

Certificates

11.1 Overview

The Zyxel 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 Zyxel Device's CA-signed (Certification Authority) certificates ([Section 11.2 on page 112](#)).
- Use the **Trusted CA** screen to save the certificates of trusted CAs to the Zyxel Device. You can also export the certificates to a computer ([Section 11.3 on page 116](#)).

11.2 Local Certificates

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

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

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

Figure 80 Security > Certificates > Local Certificates

The screenshot shows the 'Local Certificates' screen with a dark blue header bar containing 'Local Certificates' and 'Trusted CA' tabs. Below the header is a light gray box with the text: 'Certificate (also known as digital IDs) can authenticate users. In Local Certificate, you can generate certification requests and import the signed certificates. Maximum of 4 certificates can be stored.' Below this is a section titled 'Replace PrivateKey/Certificate file in PEM format' with a checkbox 'Private Key is protected by a password.' and a text input field. Below the checkbox are two buttons: 'Choose File' and 'No file chosen'. To the right of these are two buttons: 'Import Certificate' and 'Create Certificate Request'. At the bottom is a table with the following columns: 'Current File', 'Subject', 'Issuer', 'Valid From', 'Valid To', and 'Modify'.

Current File	Subject	Issuer	Valid From	Valid To	Modify
--------------	---------	--------	------------	----------	--------

The following table describes the labels in this screen.

Table 49 Security > Certificates > Local Certificates

LABEL	DESCRIPTION
Replace Private Key/Certificate file in PEM format	
Private Key is protected by a password	Select the check box and enter the private key into the text box to store it on the Zyxel Device. The private key should not exceed 63 ASCII characters (not including spaces).
Choose File	Click this button to find the certificate file you want to upload.
Import Certificate	Click this button to save the certificate that you have enrolled from a certification authority from your computer to the Zyxel Device.
Create Certificate Request	Click this button to go to the screen where you can have the Zyxel Device generate a certification request.
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 a 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.
Modify	<p>Click the View icon to open a screen with an in-depth list of information about the certificate.</p> <p>For a certification request, click Load Signed to import the signed certificate.</p> <p>Click the Remove icon to remove the certificate (or certification request). A window displays asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action.</p>

11.2.1 Create Certificate Request

Click **Security > Certificates > Local Certificates** and then **Create Certificate Request** to open the following screen. Use this screen to have the Zyxel Device generate a certification request. To create a certificate signing request, you need to enter a common name, organization name, state/province name, and the two-letter country code for the certificate.

Figure 81 Create Certificate Request

Create Certificate Request

To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate.

Certificate Name:

Common Name: ☒ Auto ☐ Customize

Organization Name:

State/Province Name:

Country/Region Name:

Apply Cancel

The following table describes the labels in this screen.

Table 50 Create Certificate Request

LABEL	DESCRIPTION
Certificate Name	Type up to 63 ASCII characters (not including spaces) to identify this certificate.
Common Name	Select Auto to have the Zyxel Device configure this field automatically. Or select Customize to enter it manually. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 63 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Organization Name	Type up to 63 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the Zyxel Device drops trailing spaces.
State/Province Name	Type up to 32 characters to identify the state or province where the certificate owner is located. You may use any character, including spaces, but the Zyxel Device drops trailing spaces.
Country/Region Name	Select a country to identify the nation where the certificate owner is located.
Cancel	Click Cancel to exit this screen without saving.
Apply	Click Apply to save your changes.

11.2.2 View Certificate Request

Click the **View** icon in the **Local Certificates** screen to open the following screen. Use this screen to view in-depth information about the certificate request. The **Certificate** is used to verify the authenticity of the

certification authority. The **Private Key** serves as your digital signature for authentication and must be safely stored. The **Signing Request** contains the certificate signing request value that you will copy upon submitting the certificate request to the CA (certificate authority).

Figure 82 Certificate Request: View

The screenshot shows a web application window titled "View Certificate" with a close button (X) in the top right corner. The window is divided into four main sections:

- Certificate Details:** A table with the following information:

Name	Test
Type	none
Subject	/CN=588BF3-VMG8825-B50B-S172V48000015/O=Zyxel/ST=Hsinchu/C=TW
- Certificate:** A large empty rectangular box for displaying the certificate content.
- Private Key:** A text area containing a long string of alphanumeric characters:


```
hGEzXjrkPkeJHmKBehzvdv
KGLNbx22N1C0qtl++BwFFzOK8xTshyNxGW27goeOY
1QpuD2RQy1FB+Ky9zVNCRuP
6C1korOCNOwp2Mds4udfazEZefm7ysyC0P2etwd7
AbLBM49P1qUsWbGWR9snO74
Myqhf+kCc2R801HUQvWX7XbHzTG+8RKtpV/oCkLZy
cUBlyq0IY2f6FkWQBxp9C2H
xteLLgB6SXDfK5vTyQTcj0spmPNdj4ZkxKhqtuLwM8E3
bzHGdujBwvzZXnf6NxAZ
fAdmacECaYEA+SiZJoWxoB90BopN1JP3t//IOLPznbs
```
- Signing Request:** A text area containing a long string of alphanumeric characters, starting with "-----BEGIN CERTIFICATE REQUEST-----":


```
-----BEGIN CERTIFICATE REQUEST-----
MIICoDCCAYgCAQAwWzEqMCgGA1UEAwwhNTg4
QkYzLVZNRzg4MjUtQjUwQjI1TMTcy
VjQ4MDAwMDE1MQ4wDAYDVQQKDAVaeXhlbDEQ
MA4GA1UECAwHSHNpbmNodTElMAkG
A1UEBhMCVFcwggEiMA0GCSqGSIb3DQEBAQUAA4I
BDwAwggEKAoIBAQDMCB3HK+Su
PeKUpWld2QkPL4qsQsYXhL7chHWxCYAFw9QYXP
NDQm4I3bS9rfwLqUMFck3F4HQ
```

At the bottom center of the window, there is a yellow button labeled "Back".

The following table describes the fields in this screen.

Table 51 Certificate Request: View

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate.
Type	This field displays general information about the certificate. ca means that a Certification Authority signed the certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Certificate	This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses base 64 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.
Private Key	This field displays the private key of this certificate.
Signing Request	This field displays the CSR (Certificate Signing Request) information of this certificate. The CSR will be provided to a certificate authority, and it includes information about the public key, organization name, domain name, location, and country of this certificate.
Back	Click Back to return to the previous screen.

11.3 Trusted CA

Click **Security > Certificates > Trusted CA** to open the following screen. This screen displays a summary list of certificates of the certification authorities that you have set the Zyxel Device to accept as trusted. The Zyxel 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.

Note: Maximum of 4 certificates can be stored.

Figure 83 Security > Certificates > Trusted CA

Local Certificates Trusted CA

Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. In Trusted CA, you can save the certificates of trusted CAs.

Import Certificate

#	Name	Subject	Type	Modify
---	------	---------	------	--------

Note
Maximum of 4 certificates can be stored.

The following table describes the labels in this screen.

Table 52 Security > Certificates > Trusted CA

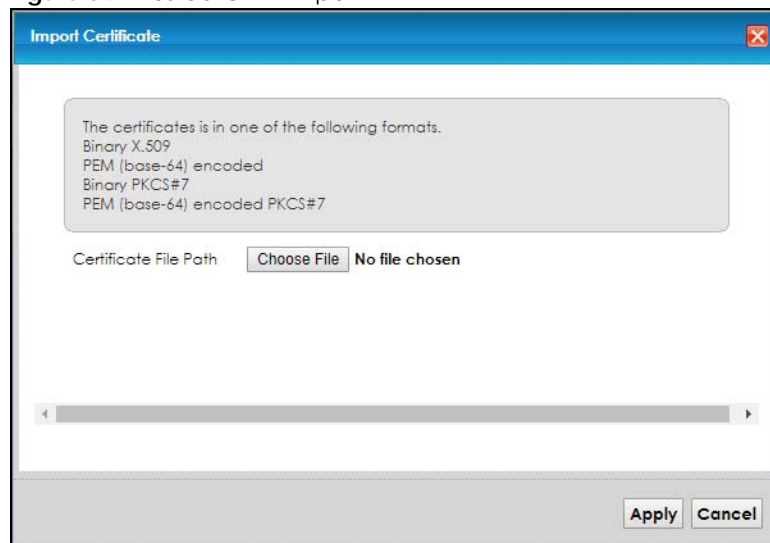
LABEL	DESCRIPTION
Import Certificate	Click this button to open a screen where you can save the certificate of a certification authority that you trust to the Zyxel Device.
#	This is the index number of the entry.
Name	This field displays the name used to identify this certificate.
Subject	This field 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.
Modify	Click the View icon to open a screen with an in-depth list of information about the certificate (or certification request). Click the Remove icon to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

11.4 Import Trusted CA Certificate

Click **Import Certificate** in the **Trusted CA** screen to open the **Import Certificate** screen. The Zyxel Device trusts any valid certificate signed by any of the imported trusted CA certificates. Certificates should be in one of the following formats: Binary X.509, PEM (base-64) encoded, Binary PKCS#7, or PEM (base-64) encoded PKCS#7. You can save a trusted certification authority's certificate to the Zyxel Device.

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

Figure 84 Trusted CA > Import



The following table describes the labels in this screen.

Table 53 Security > Certificates > Trusted CA > Import

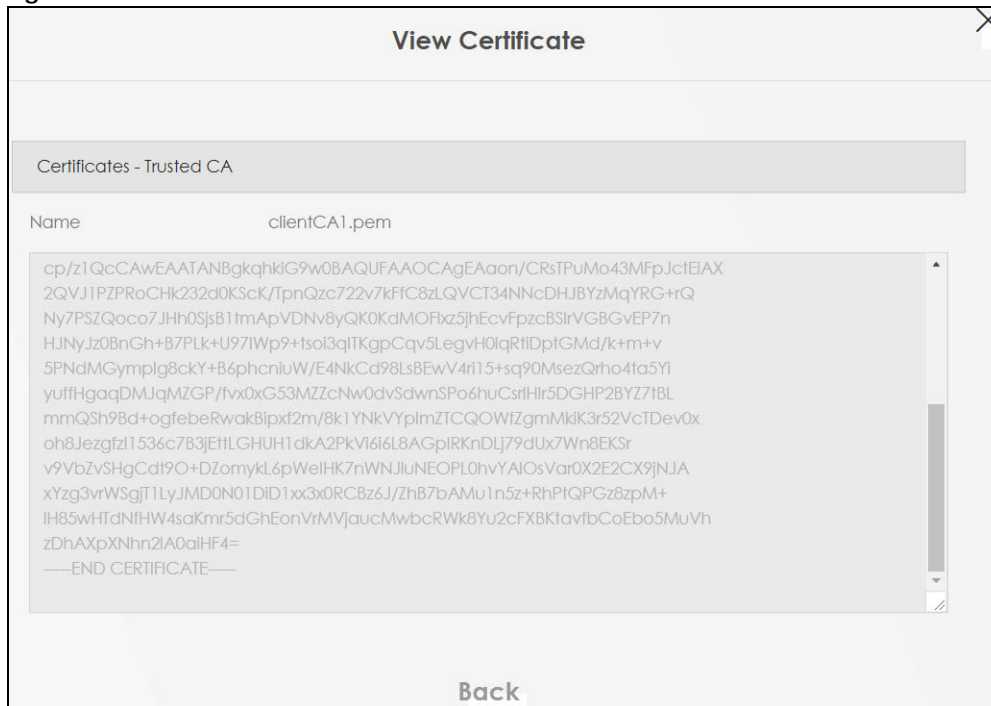
LABEL	DESCRIPTION
Certificate File Path	Type in the location of the file you want to upload in this field or click Choose File to find it.
Choose File	Click this button to find the certificate file you want to upload.
Apply	Click this to save the certificate on the Zyxel Device.
Cancel	Click this to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

11.5 View Trusted CA Certificate

Use this screen to view in-depth information about the certification authority's certificate. The certificate text box is read-only and can be distributed to others.

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

Figure 85 Trusted CA: View



The following table describes the labels in this screen.

Table 54 Trusted CA: View

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate.
	<p>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.</p> <p>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 USB thumb drive for example).</p>
Back	Click this to return to the previous screen.

11.6 Certificates Technical Reference

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

Advantages of Certificates

Certificates offer the following benefits.

- The Zyxel 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.

11.6.1 Verifying a Certificate

Before you import a trusted CA or trusted remote host certificate into the Zyxel Device, you should verify that you have the actual certificate. This is especially true of trusted CA certificates since the Zyxel 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.

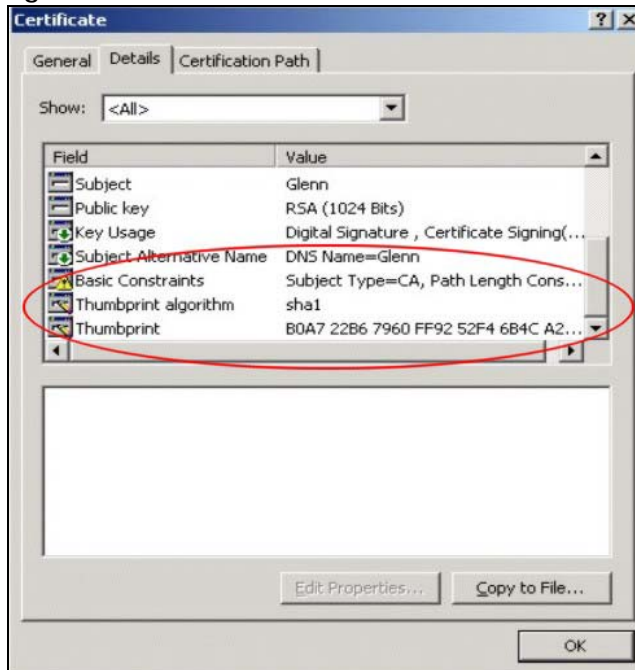
- 1 Browse to where you have the certificate saved on your computer.
- 2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 86 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 87 Certificate Details



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 vary based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

CHAPTER 12

System Monitor

12.1 Overview

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

12.1.1 What You Can Do in this Chapter

- Use the **System Log** screen to see the system-related logs for the categories that you select ([Section 12.2 on page 122](#)).
- Use the **Security Log** screen to see the security-related logs for the categories that you select ([Section 12.3 on page 123](#)).
- Use the **WAN Traffic Status** screen to view the WAN traffic statistics ([Section 12.4 on page 124](#)).
- Use the **LAN Traffic Status** screen to view the LAN traffic statistics ([Section 12.5 on page 125](#)).

12.2 The System Log Screen

Use this screen to specify which logs to display and to where the Zyxel Device is to send logs. You can filter the entries by clicking on the **Level** and/or **Category** drop-down list boxes. Click **System Monitor > Log** to open the **System Log** screen.

Figure 88 System Monitor > Log > System Log

#	Time	Facility	Level	Category	Messages
---	------	----------	-------	----------	----------

The following table describes the fields in this screen.

Table 55 System Monitor > Log > System 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 Zyxel Device searches through all logs of that severity or higher.
Category	Select the type of logs to display.

Table 55 System Monitor > Log > System Log (continued)

LABEL	DESCRIPTION
Clear Log	Click this to delete all the logs.
Refresh	Click this to renew the log screen.
Export Log	Click this to export the selected log(s) to a file on your computer.
E-mail Log Now	Click this to send the log file(s) to the E-mail address you specify in the Maintenance > Log Setting screen.
System Log	
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Level	This field displays the severity level of the log that the device is to send to this syslog server.
Category	This field displays the type of the log.
Messages	This field states the reason for the log.

12.3 The Security Log Screen

Use this screen to specify which logs to display and to where the Zyxel Device is to send logs. You can filter the entries by clicking on the **Level** and/or **Category** drop-down list boxes. Click **System Monitor > Log > Security Log** to open the following screen.

Figure 89 System Monitor > Log > Security Log

All security events will be logged and displayed in the following table. Select a level from the pull-down menu to show filtered results.

Level: Category:

#	Time	Facility	Level	Category	Messages
---	------	----------	-------	----------	----------

The following table describes the fields in this screen.

Table 56 System Monitor > Log > Security 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 Zyxel Device searches through all logs of that severity or higher.
Category	Select the type of logs to display.
Clear Log	Click this to delete all the logs.
Refresh	Click this to renew the log screen.
Export Log	Click this to export the selected log(s) to a file on your computer.

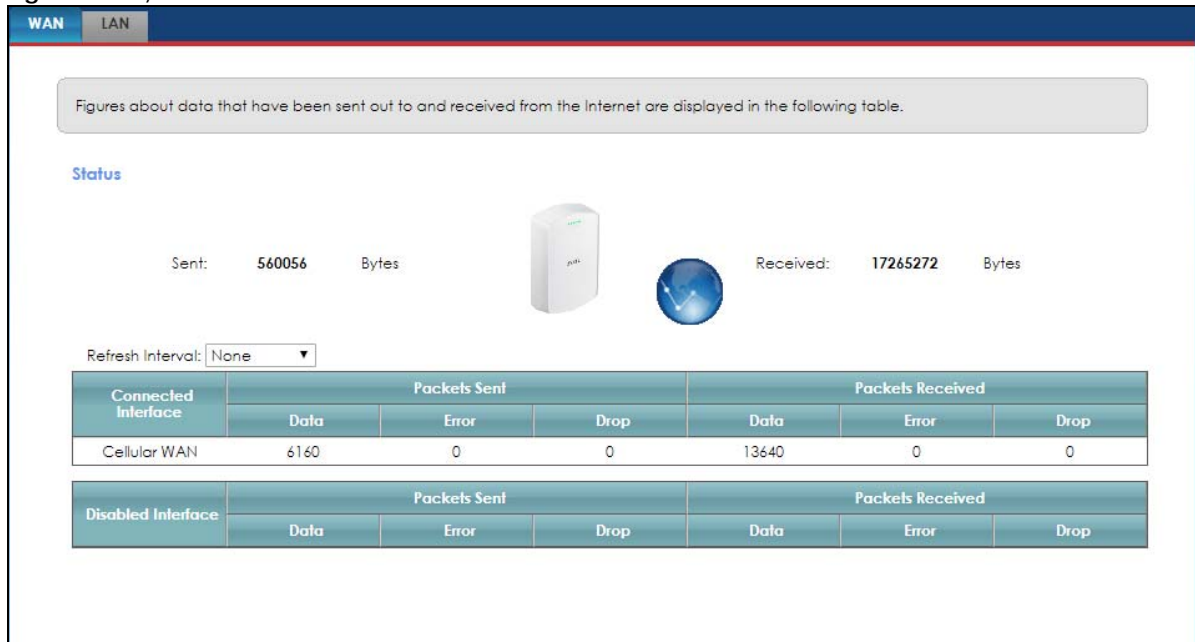
Table 56 System Monitor > Log > Security Log (continued)

LABEL	DESCRIPTION
E-mail Log Now	Click this to send the log file(s) to the E-mail address you specify in the Maintenance > Log Setting screen.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Level	This field displays the severity level of the log that the device is to send to this syslog server.
Category	This field displays the type of the log.
Messages	This field states the reason for the log.

12.4 The WAN Traffic Status Screen

Click **System Monitor > Traffic Status** to open the **WAN** screen. Use the **Traffic Status** screens to look at the network traffic status and statistics of the WAN/LAN interfaces.

The values in this screen show the number of bytes received and sent through the Zyxel Device. Detailed information about each interface are listed in the tables below.

Figure 90 System Monitor > Traffic Status > WAN

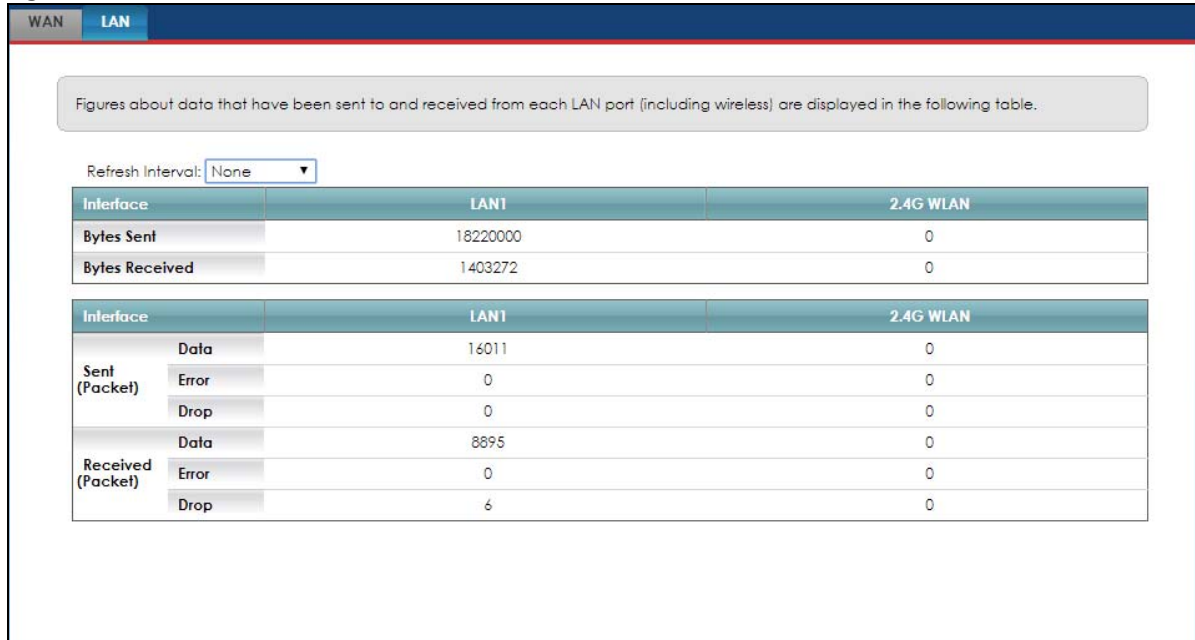
The following table describes the fields in this screen.

Table 57 System Monitor > Traffic Status > WAN

LABEL	DESCRIPTION
Status	This shows the number of bytes sent and received through the WAN interface of the Zyxel Device.
Refresh Interval	Specify how often you want the Zyxel Device to update this screen and click Set Interval to apply the change. Click None to halt updating of the screen.
Connected Interface	This shows the name of the WAN interface that is currently connected.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.
Disabled Interface	This shows the name of the WAN interface that is currently disconnected.
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.

12.5 The LAN Traffic Status Screen

Click **System Monitor > Traffic Status > LAN** to open the following screen. The values in this screen show the number of bytes received and sent from each LAN port and wireless network.

Figure 91 System Monitor > Traffic Status > LAN

The following table describes the fields in this screen.

Table 58 System Monitor > Traffic Status > LAN

LABEL	DESCRIPTION
Refresh Interval	Specify how often you want the Zyxel Device to update this screen and click Set Interval to apply the change. Click None 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.

CHAPTER 13

ARP Table

13.1 ARP Table Overview

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

An IP (version 4) address is 32 bits long. In an Ethernet LAN, MAC addresses are 48 bits long. The ARP table maintains an association between each MAC address and its corresponding IP address.

13.1.1 How ARP Works

When an incoming packet destined for a host device on a local area network arrives at the device, the device's ARP program looks in the ARP table and, if it finds the address, sends it to the device.

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The device fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the device puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP table for future reference and then sends the packet to the MAC address that replied.

13.2 ARP Table Screen

Use the ARP table to view the IPv4-to-MAC address mapping(s) for the LAN. The neighbor table shows the IPv6-to-MAC address mapping(s) of each neighbor. To open this screen, click **System Monitor > ARP Table**.

Figure 92 System Monitor > ARP Table

ARP Table			
ARP Table displays the IPv4 address and MAC address of each DHCP connection. Neighbour Table displays the IPv6 address and MAC address of each Neighbour.			
IPv4 ARP Table			
#	IPv4 Address	MAC Address	Device
1	192.168.1.129	dc:4a:3e:40:ec:5f	br0
IPv6 Neighbour Table			
#	IPv6 Address	MAC Address	Device
1	fe80::ecad:ab45:c530:cc3f	dc:4a:3e:40:ec:5f	br0

The following table describes the labels in this screen.

Table 59 System Monitor > ARP Table

LABEL	DESCRIPTION
#	This is the ARP table entry number.
IPv4/IPv6 Address	This is the learned IPv4 or IPv6 IP address of a device connected to a port.
MAC Address	This is the MAC address of the device with the listed IP address.
Device	This is the type of interface used by the device. You can click on the device type to go to its configuration screen.

CHAPTER 14

Routing Table

14.1 Routing Table Overview

Routing is based on the destination address only and the Zyxel Device takes the shortest path to forward a packet.

14.2 The Routing Table Screen

The table below shows IPv4 and IPv6 routing information. The IPv4 subnet mask is '255.255.255.255' for a host destination and '0.0.0.0' for the default route. The gateway address is written as '*' (IPv4) / '::' (IPv6) if none is set.

Click **System Monitor > Routing Table** to open the following screen.

Figure 93 System Monitor > Routing Table

Routing Table					
Destination: The destination network or destination host. Gateway: The gateway address or '*' (IPv4) / '::' (IPv6) if none set. Subnet Mask (IPv4): The netmask for the destination net; '255.255.255.255' for a host destination and '0.0.0.0' for the default route. Flags: U - up, I - reject, G - gateway, C - cache, H - host, R - reinstate, D - dynamic (redirect), M - modified (redirect). Metric: The distance to the target (usually counted in hops). Interface: Interface to which packets for this route will be sent.					
IPv4 Routing Table					
Destination	Gateway	Subnet Mask	Flag	Metric	Interface
127.0.0.0	0.0.0.0	255.255.0.0	U	0	lo
192.168.1.0	0.0.0.0	255.255.255.0	U	0	br0
239.0.0.0	0.0.0.0	255.0.0.0	U	0	br0
IPv6 Routing Table					
Destination	Gateway	Flag	Metric	Interface	
fe80::/64	::	U	256	eth2	
fe80::/64	::	U	256	br0	
fe80::/64	::	U	256	ra0	
fe80::/64	::	U	256	wwan0	
::1/128	::	U	0	lo	
fe80::/128	::	U	0	lo	
fe80::/128	::	U	0	lo	
fe80::/128	::	U	0	lo	
fe80::/128	::	U	0	lo	
fe80::86aa:9cff:fe83:b903/128	::	U	0	lo	
fe80::86aa:9cff:fe83:b903/128	::	U	0	lo	
fe80::86aa:9cff:fe83:b904/128	::	U	0	lo	
fe80::942e:d2ff:feb3:7d7c/128	::	U	0	lo	
ff00::/8	::	U	256	eth2	
ff00::/8	::	U	256	br0	
ff00::/8	::	U	256	ra0	
ff00::/8	::	U	256	wwan0	

The following table describes the labels in this screen.

Table 60 System Monitor > Routing Table

LABEL	DESCRIPTION
IPv4/IPv6 Routing Table	
Destination	This indicates the destination IPv4 address or IPv6 address and prefix of this route.
Gateway	This indicates the IPv4 address or IPv6 address of the gateway that helps forward this route's traffic.
Subnet Mask	This indicates the destination subnet mask of the IPv4 route.
Flag	<p>This indicates the route status.</p> <p>U-Up: The route is up.</p> <p>!-Reject: The route is blocked and will force a route lookup to fail.</p> <p>G-Gateway: The route uses a gateway to forward traffic.</p> <p>H-Host: The target of the route is a host.</p> <p>R-Reinstate: The route is reinstated for dynamic routing.</p> <p>D-Dynamic (redirect): The route is dynamically installed by a routing daemon or redirect.</p> <p>M-Modified (redirect): The route is modified from a routing daemon or redirect.</p>
Metric	The metric represents the "cost of transmission." A router determines the best route for transmission by choosing a path with the lowest "cost." The smaller the number, the lower the "cost."
Interface	<p>This indicates the name of the interface through which the route is forwarded.</p> <p>brx indicates a LAN interface where x can be 0~3 to represent LAN1 to LAN4 respectively.</p> <p>ptm0 indicates a WAN interface using IPoE or in bridge mode.</p> <p>ppp0 indicates a WAN interface using PPPoE.</p>

CHAPTER 15

System

15.1 System Screen Overview

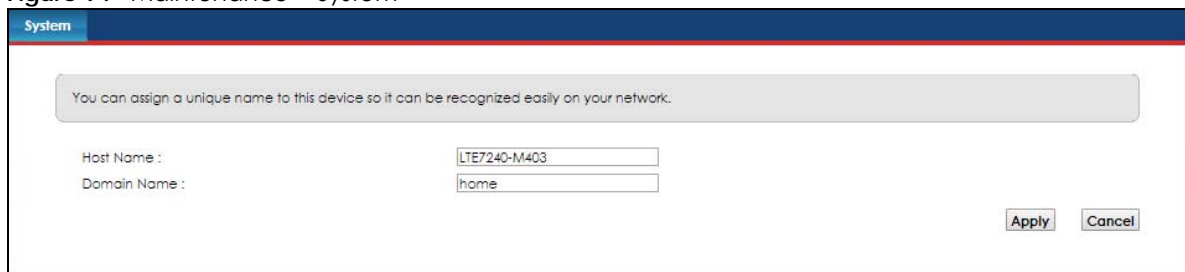
In this screen, you can name your Zyxel Device (Host) and give it an associated domain name for identification purposes.

15.2 The System Screen

Assign a unique name to the Zyxel Device so it can be easily recognized on your network. You can use up to 30 characters, including spaces.

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

Figure 94 Maintenance > System



The following table describes the labels in this screen.

Table 61 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.
Apply	Click this to save your changes back to the Zyxel Device.
Cancel	Click this to begin configuring this screen afresh.

CHAPTER 16

User Account

16.1 User Account Overview

In the **User Account** screen, you can view the settings of the “admin” and other user accounts that you use to log into the Zyxel Device.

16.2 The User Account Screen

A User is someone who can log into the Web Configurator to manage the Zyxel Device. There are two types (groups) of users with different privileges: **Administrator** and **User**. Use this screen to create or manage user accounts and their privileges on the Zyxel Device.

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

Figure 95 Maintenance > User Account

#	Active	User Name	Retry Times	Idle Timeout	Lock Period	Group	Modify
1	<input checked="" type="checkbox"/>	admin	3	5	5	Administrator	
2	<input checked="" type="checkbox"/>	Private	3	5	5	Administrator	

Apply Cancel

The following table describes the labels in this screen.

Table 62 Maintenance > User Account

LABEL	DESCRIPTION
Add New Account	Click this button to add a new user account.
#	This is the number of an individual user account.
Active	This field indicates whether the user account is active (with check mark) or not (blank).
User Name	This field displays the name of the account used to log into the Zyxel Device Web Configurator.
Retry Times	This field displays the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit.
Idle Timeout	This field displays the length of inactive time before the Zyxel Device will automatically log the user out of the Web Configurator.
Lock Period	This field displays the length of time user must wait before attempting to log in again after a number of consecutive wrong passwords have been entered as defined in Retry Times .

Table 62 Maintenance > User Account (continued)

LABEL	DESCRIPTION
Group	This field displays whether this user has Administrator or User privileges.
Modify	Click the Edit icon to configure the entry. Click the Delete icon to remove the entry.
Apply	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

16.2.1 Add/Edit User Account

Click **Add New Account** or the Edit icon of an existing account in the **Maintenance > User Account** screen to open the following screen.

Figure 96 User Account: Add New Account

The following table describes the labels in this screen.

Table 63 User Account: Add/Edit

LABEL	DESCRIPTION
Active	Activates user account.
User Name	Assign a name for the user account
Password	Type the user account's password (up to 256 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you assign the password, use the new password to access the Zyxel Device.
Verify Password	Type the new password again for confirmation.
Retry Times	Enter the number of times consecutive wrong passwords can be entered for this account. Enter 0 for no limit.
Idle Timeout	Enter the length of inactive time before the Zyxel Device will automatically log the user out of the Web Configurator.
Lock Period	Enter the length of time a user must wait before attempting to log in again after a number of consecutive wrong passwords have been entered as defined in Retry Times .
Group	Specify whether this user will have Administrator or User privileges.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

CHAPTER 17

Remote Management

17.1 Overview

Remote management controls through which interface(s), which web services (such as HTTP, HTTPS, FTP, Telnet, SSH and Ping) can access the Zyxel Device.

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

17.2 The MGMT Services Screen

Use this screen to configure through which interface(s) you can access the Zyxel Device using which services. You can also specify the service port numbers computers must use to connect to the Zyxel Device. Click **Maintenance > Remote Management** to open the following screen.

Figure 97 Maintenance > Remote Management

Remote MGMT enables various approaches to access this device remotely from a WAN and/or LAN connection.

Service Control

WAN Interface used for services: ☒ Any_WAN ☐ Multi_WAN

☐ Cellular WAN

Service	LAN/WLAN	WAN	Trust Domain	Port
HTTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	80
HTTPS	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	443
FTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	21
TELNET	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	23
SSH	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	22
PING	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	

Apply Cancel

The following table describes the fields in this screen.

Table 64 Maintenance > Remote Management

LABEL	DESCRIPTION
WAN Interface used for services	Select Any_WAN to have the Zyxel Device automatically activate the remote management service when any WAN connection is up. Select Multi_WAN and then select one or more WAN connections to have the Zyxel Device activate the remote management service when the selected WAN connections are up.
Cellular WAN	Enable the LTE WAN connection configured in Network Setting > Broadband > Cellular WAN to access the service on the Zyxel Device.
Service	This is the service you may use to access the Zyxel Device.
LAN/WLAN	Select the Enable check box for the corresponding services that you want to allow access to the Zyxel Device from the LAN/WLAN.
WAN	Select the Enable check box for the corresponding services that you want to allow access to the Zyxel Device from all WAN connections.
Trust Domain	Select the Enable check box for the corresponding services that you want to allow access to the Zyxel Device from the trusted host IP address.
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Apply	Click Apply to save your changes back to the Zyxel Device.
Cancel	Click Cancel to restore your previously saved settings.

17.3 The Trust Domain Screen

Use this screen to view a list of public IP addresses which are allowed to access the Zyxel Device through the services configured in the **Maintenance > Remote Management > Trust Domain** screen. Click **Maintenance > Remote Management > Trust Domain** to open the following screen.

Note: If this list is empty, all public IP addresses can access the Zyxel Device from the WAN through the specified services.

Figure 98 Maintenance > Remote Management > Trust Domain

The following table describes the fields in this screen.

Table 65 Maintenance > Remote Management > Trust Domain

LABEL	DESCRIPTION
Add Trust Domain	Click this to add a trusted host IP address.

Table 65 Maintenance > Remote Management > Trust Domain (continued)

LABEL	DESCRIPTION
IP Address	This field shows a trusted host IP address.
Delete	Click the Delete icon to remove the trusted IP address.

17.4 The Add Trust Domain Screen

Use this screen to configure a public IP address which is allowed to access the Zyxel Device. Click the **Add Trust Domain** button in the **Maintenance > Remote Management > Trust Domain** screen to open the following screen.

Figure 99 Maintenance > Remote Management > Trust Domain > Add Trust Domain

The following table describes the fields in this screen.

Table 66 Maintenance > Remote MGMT > Trust Domain > Add Trust Domain

LABEL	DESCRIPTION
IP Address	Enter a public IPv4/IPv6 IP address which is allowed to access the service on the Zyxel Device from the WAN.
Apply	Click Apply to save your changes back to the Zyxel Device.
Cancel	Click Cancel to restore your previously saved settings.

CHAPTER 18

TR-069 Client

18.1 Overview

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

18.2 The TR-069 Client Screen

TR-069 defines how Customer Premise Equipment (CPE), for example your Zyxel 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 Zyxel Device, modify settings, perform firmware upgrades as well as monitor and diagnose the Zyxel 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 Zyxel Device to be managed remotely by an Auto Configuration Server (ACS) using TR-069.

Figure 100 Maintenance > TR-069 Client

TR-069 Client

TR-069 is a remote management tool on this device. The operator can upgrade firmware, modify settings, and diagnose problems remotely when TR-069 is enabled.

CWMP Active ☒ Enable ☐ Disable

Inform ☐ Enable ☒ Disable

Inform Interval

IP Protocol ☐ TR069 on IPv4 Only ☐ TR069 on IPv6 Only ☒ Auto Select

ACS URL (URL or IPv4 Address / Global IPv6 Address)

ACS User Name

ACS Password

WAN Interface Used by TR-069 Client ☒ Any_WAN ☐ Multi_WAN

☒ Cellular WAN

Display SOAP Messages on Serial Console ☐ Enable ☒ Disable

Connection Request Authentication ☐ Enable ☒ Disable

Connection Request User Name

Connection Request Password

Connection Request URL

☒ Enable ☐ Disable

Local Certificate Used by TR-069 Client

Apply Cancel

The following table describes the fields in this screen.

Table 67 Maintenance > TR-069 Client

LABEL	DESCRIPTION
CWMP Active	Select Enable to allow the Zyxel Device to be managed by a management server. Otherwise, select Disable to disallow the Zyxel Device to be managed by a management server.
Inform	Select Enable for the Zyxel 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 Zyxel Device sends information to the auto-configuration server.
IP Protocol	Select the type of IP protocol to allow TR-069 to operate on.
ACS URL	Enter the URL or IP address of the auto-configuration server.
ACS User Name	Enter the TR-069 user name for authentication with the auto-configuration server.
ACS Password	Enter the TR-069 password for authentication with the auto-configuration server.
WAN Interface used by TR-069 client	<p>Select a WAN interface through which the TR-069 traffic passes.</p> <p>If you select Any_WAN, the Zyxel Device automatically passes the TR-069 traffic when any WAN connection is up.</p> <p>If you select Multi_WAN, you also need to select two or more pre-configured WAN interfaces. The Zyxel Device automatically passes the TR-069 traffic when one of the selected WAN connections is up.</p>
Cellular WAN	The Zyxel Device automatically passes the TR-069 traffic when cellular WAN connection is up.
Display SOAP messages on serial console	Select Enable to dump all SOAP messages during the ACS server communication with the CPE.
Connection Request Authentication	Select this option to enable authentication when there is a connection request from the ACS.
Connection Request User Name	<p>Enter the connection request user name.</p> <p>When the ACS makes a connection request to the Zyxel Device, this user name is used to authenticate the ACS.</p>
Connection Request Password	<p>Enter the connection request password.</p> <p>When the ACS makes a connection request to the Zyxel Device, this password is used to authenticate the ACS.</p>
Connection Request URL	<p>This shows the connection request URL.</p> <p>The ACS can use this URL to make a connection request to the Zyxel Device.</p>
Local certificate used by TR-069 client	You can choose a local certificate used by TR-069 client. The local certificate should be imported in the Security > Certificates > Local Certificates screen.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore the screen's last saved settings.

CHAPTER 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 Zyxel Device's time and date, click **Maintenance > Time**. The screen appears as shown. Use this screen to configure the Zyxel Device's time based on where it is located. You can add a time server address, select your time zone, and configure daylight savings if your location uses it.

Figure 101 Maintenance > Time Setting

Time

In order to get a correct time for the device, fill in a time server address, select the time zone where this device is physically located, and complete the daylight saving settings if needed.

Current Date/Time

Current Time : 05:22:01

Current Date : 2018-05-01

Time and Date Setup

Time Protocol : SNTP (RFC-1769)

First Time Server Address : pool.ntp.org

Second Time Server Address : clock.nyc.he.net

Third Time Server Address : clock.sjc.he.net

Fourth Time Server Address : None

Fifth Time Server Address : None

Time Zone

Time Zone : [GMT+08:00] Taipei

Daylight Savings

Active ☐ Enable ☒ Disable

Apply Cancel

The following table describes the fields in this screen.

Table 68 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Current Date/Time	
Current Time	This field displays the time of your Zyxel Device.
Current Date	This field displays the date of your Zyxel Device
Time and Date Setup	
Time Protocol	Shows the time protocol your Zyxel Device is currently using.

Table 68 Maintenance > System > Time Setting (continued)

LABEL	DESCRIPTION
First, Second, Third, Fourth, Fifth Time Server Address	<p>Select an NTP time server from the drop-down list box.</p> <p>Otherwise, select Other and enter the IP address or URL (up to 29 extended ASCII characters in length) of your time server.</p> <p>Select None if you don't want to configure the time server.</p> <p>Check with your ISP/network administrator if you are unsure of this information.</p>
Time Zone	
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 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.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore the screen's last saved settings.

CHAPTER 20

E-mail Notification

20.1 E-mail Notification Overview

A mail server is an application or a computer that runs such an application to receive, forward and deliver e-mail messages.

To have the Zyxel Device send reports, logs or notifications via e-mail, you must specify an e-mail server and the e-mail addresses of the sender and receiver.

20.2 The E-mail Notification Screen

Click **Maintenance > E-mail Notification** to open the **E-mail Notification** screen. Use this screen to view, remove and add e-mail account information on the Zyxel Device. This account can be set to receive e-mail notifications for logs.

Figure 102 Maintenance > E-mail Notification

The following table describes the labels in this screen.

Table 69 Maintenance > E-mail Notification

LABEL	DESCRIPTION
Add New E-mail	Click this button to create a new entry.
Mail Server Address	This field displays the server name or the IP address of the mail server.
User name	This field displays the user name of the sender's mail account.
Port	This field displays the e-mail notification service port (default is 25).
Security	This field displays the type of connection security (SSL or STARTTLS).
E-mail Address	This field displays the e-mail address that you want to be in the from/sender line of the e-mail that the Zyxel Device sends.
Remove	Click this button to delete the selected entry(ies).

20.2.1 E-mail Notification Add/Edit

Click the **Add New E-mail** button in the **E-mail Notification** screen. Use this screen to configure the required information for sending e-mail via a mail server.

Figure 103 Email Notification > Add

Note: The default port number of the mail server is 25.

The following table describes the labels in this screen.

Table 70 Email Notification > Add

LABEL	DESCRIPTION
Mail Server Address	Enter the server name or the IP address of the mail server for the e-mail address specified in the Account E-mail Address field. If this field is left blank, reports, logs or notifications will not be sent via e-mail.
Port	E-mail notification default service port is port 25. You can specify a different port.
Authentication User name	Enter the user name (up to 32 characters). This is usually the user name of a mail account you specified in the Account E-mail Address field.
Authentication Password	Enter the password associated with the user name above.
Account E-mail Address	Enter the e-mail address that you want to be in the from/sender line of the e-mail notification that the Zyxel Device sends. If you activate SSL/STARTTLS authentication, the e-mail address must be able to be authenticated by the mail server as well.
OK	Click this button to save your changes and return to the previous screen.
Cancel	Click this button to begin configuring this screen afresh.

CHAPTER 21

Log Setting

21.1 Log Setting Overview

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

21.2 The Log Setting Screen

If there is a LAN client on your network or a remote server that is running a syslog utility, you can save log files from LAN computers to it by enabling **Syslog Logging**, selecting **Remote** or **Local File and Remote** in the **Mode** field, and entering the IP address of the syslog server in the **Syslog Server** field. **Remote** allows you to store logs on a syslog server, while **Local File** allows you to store them on the Zyxel Device. **Local File and Remote** means your logs are stored both on the Zyxel Device and on a syslog server. To change your Zyxel Device's log settings, click **Maintenance > Log Setting**. The screen appears as shown.

Figure 104 Maintenance > Log Setting

The screenshot shows the 'Log Setting' configuration page. At the top, a blue header bar contains the text 'Log Setting'. Below this, a light gray box contains a descriptive paragraph: 'Log Setting defines which types of logs and which log levels you want to record. If you have a LAN client on your network that is running a syslog utility, you can also save the log files there by enabling Syslog Logging and enter the IP address of that LAN client.'

The main configuration area is divided into several sections:

- Syslog Setting**: Includes 'Syslog Logging' (radio buttons for 'Enable' and 'Disable', with 'Disable' selected), 'Mode' (a dropdown menu set to 'Local File'), 'Syslog Server' (a text field with '0.0.0.0' and a note '(Server NAME or IPv4/IPv6 Address)'), and 'UDP Port' (a text field with '514' and a note '(Server Port)').
- E-mail Log Settings**: Includes 'E-mail Log Settings' (radio buttons for 'Enable' and 'Disable', with 'Disable' selected).
- Active Log**: A section with two columns of checkboxes.
 - System Log**: WAN-DHCP, DHCP Server, TR-069, HTTP, UPNP, System, ACL, Wireless, and 3G/LTE.
 - Security Log**: Account, Attack, Firewall, and MAC Filter.

At the bottom right of the form, there are two buttons: 'Apply' and 'Cancel'.

The following table describes the fields in this screen.

Table 71 Maintenance > Log Setting

LABEL	DESCRIPTION
Syslog Settings	
Syslog Logging	Select the Enable check box to enable syslog logging.
Mode	<p>Select Remote to have the Zyxel Device send it to an external syslog server.</p> <p>Select Local File to have the Zyxel Device save the log file on the Zyxel Device itself.</p> <p>Select Local File and Remote to have the Zyxel Device save the log file on the Zyxel Device itself and send it to an external syslog server.</p>
Syslog Server	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
UDP Port	Enter the port number used by the syslog server.
E-mail Log Settings	
E-mail Log Setting	Select Enable to allow the sending via e-mail the logs to the e-mail address specified in Maintenance > E-mail Notifications .
Active Log	
System Log	Select the categories of System Logs that you want to record.
Security Log	Select the categories of Security Logs that you want to record.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

CHAPTER 22

Firmware Upgrade

22.1 Overview

This chapter explains how to upload new firmware to your Zyxel 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 Zyxel Device.

22.2 The Firmware Upgrade Screen

This screen lets you upload new firmware to your Zyxel Device. Click **Maintenance > Firmware Upgrade** to open the following screen.

Download the latest firmware file from the Zyxel website and upload it to your Zyxel Device using this screen. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to three minutes. After a successful upload, the Zyxel Device will reboot.

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

Figure 105 Maintenance > Firmware Upgrade



The screenshot shows the 'Firmware Upgrade' screen. At the top, a grey box contains the text: 'Firmware Upgrade is where you can update the device with newly released features by upgrading the latest firmware. You can download the latest firmware file from the manufacturer website of this device.' Below this, the section is titled 'Upgrade Firmware'. There are two options: 'Restore Default Settings After Firmware Upgrade:' with an unchecked checkbox, and 'Current Firmware Version:' showing 'V1.0.0.0'. Below these, there is a 'File Path:' label, a 'Choose File' button, and the text 'No file chosen'. An 'Upload' button is located at the bottom right of the form.

The following table describes the labels in this screen.

Table 72 Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Upgrade Firmware	Use these fields to upload firmware to the Zyxel Device.
Restore Default Settings After Firmware Upgrade	Click to enable this option that restores the factory-default to the Zyxel Device after upgrading the firmware. Note: Make sure to backup the Zyxel Device's configuration settings first in case the restore to factory-default process is not successful. Refer to Section 23.2 on page 147 .
Current Firmware Version	This is the present firmware version.
File Path	Type in the location of the file you want to upload in this field or click Choose File to find it.
Choose File	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 Zyxel Device again.

The Zyxel 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 106 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.

CHAPTER 23

Backup/Restore

23.1 Backup/Restore Overview

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

23.2 The Backup/Restore Screen

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

Figure 107 Maintenance > Backup/Restore

The screenshot shows the 'Backup/Restore' web interface. At the top is a blue header bar with the text 'Backup/Restore'. Below the header is a light gray informational box stating: 'You can save the current settings in a backup file on your computer, or restore previous settings from a backup file. You can also reset the device back to its factory default state.' The main content area is white and contains three sections. The first section, 'Backup Configuration', has the instruction 'Click Backup to save the current configuration of your system to your computer.' and a 'Backup' button. The second section, 'Restore Configuration', has the instruction 'To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.' Below this is a 'File Path' label followed by a 'Choose File' button, the text 'No file chosen', and an 'Upload' button. The third section, 'Back to Factory Default Settings', has the instruction 'Click Reset to clear all user-entered configuration information and return to factory default settings. After resetting, the' followed by a bulleted list: '- Password will be 1234', '- LAN IP address will be 192.168.1.1', and '- DHCP will be reset to default setting'. At the bottom of this section is a 'Reset' button.

Backup Configuration

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

Table 73 Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Choose File to find it.
Choose File	Click 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 Zyxel Device while configuration file upload is in progress.

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

The Zyxel 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 108 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 Zyxel Device IP address (192.168.1.1).

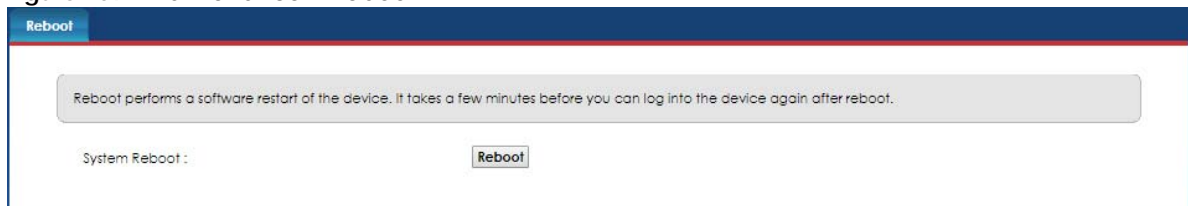
If the upload was not successful, an error screen will appear. Click **OK** to go back to the **Configuration** screen.

23.3 The Reboot Screen

System Reboot allows you to reboot the Zyxel Device remotely without turning the power off. You may need to do this if the Zyxel Device hangs, for example. This does not affect the Zyxel Device's configuration.

Click **Maintenance > Reboot**. Click **Reboot** to have the Zyxel Device reboot.

Figure 109 Maintenance > Reboot



CHAPTER 24

Diagnostic

24.1 Diagnostic Overview

You can use different diagnostic methods to test a connection and see the detailed information. The **Diagnostic** screens display information to help you identify problems with the Zyxel Device.

24.2 The Ping/TraceRoute/Nslookup Test Screen

Use this screen to perform ping, traceroute, or nslookup for troubleshooting. Ping and traceroute are used to test whether a particular host is reachable. After entering an IP address and clicking one of the buttons to start a test, the results will be shown in the Ping/Traceroute Test area. Use nslookup to find the IP address for a host name and vice versa. Click **Maintenance > Diagnostic** to open the **Ping/TraceRoute/Nslookup** screen shown next.

Figure 110 Maintenance > Diagnostic > Ping/Trace Route/Nslookup

Ping&Traceroute&Nslookup

Ping and TraceRoute are network utilities used to test whether a particular host is reachable. Enter either an IP address or a host name and click one of the buttons to start a Ping or TraceRoute test. The test result will be shown in the Info area.

Ping/TraceRoute Test

Info-

TCP/IP

Address

The following table describes the fields in this screen.

Table 74 Maintenance > Diagnostic > Ping/Trace Route/NSLookup

LABEL	DESCRIPTION
Ping/ TraceRoute Test	The result of tests is shown here in the info area.
TCP/IP	
Address	Enter either an IP address or a host name to start a test.

Table 74 Maintenance > Diagnostic > Ping/Trace Route/NSLookup (continued)

LABEL	DESCRIPTION
Ping	Click this button to perform a ping test on the IPv4 address or host name in order to test a connection. The ping statistics will show in the info area.
Ping 6	Click this button to perform a ping test on the IPv6 address or host name in order to test a connection. The ping statistics will show in the info area.
Trace Route	Click this button to perform the IPv4 trace route function. This determines the path a packet takes to the specified host.
Trace Route 6	Click this button to perform the IPv6 trace route function. This determines the path a packet takes to the specified host.
Nslookup	Click this button to perform a DNS lookup on the IP address or host name.

CHAPTER 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](#)
- [Zyxel Device Access and Login](#)
- [Internet Access](#)
- [UPnP](#)

25.2 Power and Hardware Connections

[The Zyxel Device does not turn on.](#)

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

25.3 Zyxel Device Access and Login

[I forgot the IP address for the Zyxel 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 Zyxel 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 Zyxel 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. Refer to [Section 23.2 on page 147](#).

[I forgot the password.](#)

- 1 The default admin password is **1234**.
- 2 If you can't remember the password, you have to reset the device to its factory defaults. Refer to [Section 23.2 on page 147](#).

[I cannot see or access the **Login** screen in the Web Configurator.](#)

- 1 Make sure you are using the correct IP address.
 - The default IP address is 192.168.1.1.
 - If you changed the IP address ([Section 6.2 on page 64](#)), 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 Zyxel 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 default, and try to access the Zyxel Device with the default IP address. Refer to [Section 23.2 on page 147](#).
- 5 If the problem continues, contact the network administrator or vendor, or try the advanced suggestion.

Advanced Suggestion

- Try to access the Zyxel Device using another service, such as Telnet. If you can access the Zyxel Device, check the remote management settings and firewall rules to find out why the Zyxel Device does not respond to HTTP.

[I can see the **Login** screen, but I cannot log in to the Zyxel 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 Zyxel Device. Log out of the Zyxel Device in the other session, or ask the person who is logged in to log out.
- 3 Turn the Zyxel Device off and on.
- 4 If this does not work, you have to reset the device to its factory default. See [Section 25.2 on page 152](#).

[I cannot use FTP, Telnet, SSH or Ping to access the Zyxel Device.](#)

See the Remote Management [Section on page 134](#) for details on allowing web services (such as HTTP, HTTPS, FTP, Telnet, SSH and Ping) to access the Zyxel Device.

25.4 Internet Access

[I cannot access the Internet.](#)

- 1 Check the hardware.
- 2 Check the SIM card. Maybe it has the wrong settings (refer to [Section 4.3 on page 30](#)), the account has expired, it became loose (remove and reinsert it - refer to the Quick Start Guide) or it's missing (stolen).
- 3 Make sure you entered your ISP account information correctly. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 4 Disconnect all the cables from your Zyxel Device, and follow the directions in the Quick Start Guide again.
- 5 If the problem continues, contact your ISP.

[I cannot access the Internet anymore. I had access to the Internet \(with the Zyxel Device\), but my Internet connection is not available anymore.](#)

- 1 Check the hardware connections (refer to the Quick Start Guide).
- 2 Turn the Zyxel 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 Zyxel 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 Zyxel Device off and on.
- 3 If the problem continues, contact the network administrator or vendor, or try the advanced suggestion (refer to [I cannot see or access the Login screen in the Web Configurator](#) in this chapter).

25.5 UPnP

When using UPnP and the Zyxel Device reboots, my computer cannot detect UPnP and refresh [My Network Places > Local Network](#).

- 1 Disconnect the Ethernet cable from the Zyxel 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.

APPENDIX A

Customer Support

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

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

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

Required Information

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

Corporate Headquarters (Worldwide)

Taiwan

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

Asia

China

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

India

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

Kazakhstan

- Zyxel Kazakhstan
- <http://www.zyxel.kz>

Korea

- Zyxel Korea Corp.
- <http://www.zyxel.kr>

Malaysia

- Zyxel Malaysia Sdn Bhd.
- <http://www.zyxel.com.my>

Pakistan

- Zyxel Pakistan (Pvt.) Ltd.
- <http://www.zyxel.com.pk>

Philippines

- Zyxel Philippines
- <http://www.zyxel.com.ph>

Singapore

- Zyxel Singapore Pte Ltd.
- <http://www.zyxel.com.sg>

Taiwan

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

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/>

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 Spain
- <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/homepage.shtml>

North America

USA

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

Oceania

Australia

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

Africa

South Africa

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

APPENDIX B

Legal Information

Copyright

Copyright © 2019 by Zyxel Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of Zyxel Communications Corporation.

Published by Zyxel Communications Corporation. All rights reserved.

Disclaimer

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

Regulatory Notice and Statement

EUROPEAN UNION



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

Declaration of Conformity with Regard to EU Directive 2014/53/EU (Radio Equipment Directive, RED)

- Compliance information for wireless products relevant to the EU and other Countries following the EU Directive 2014/53/EU (RED). And this product may be used in all EU countries (and other countries following the EU Directive 2014/53/EU) without any limitation except for the countries mentioned below table:
- In the majority of the EU and other European countries, the 5GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable. The requirements for any country may evolve. Zyxel recommends that you check with the local authorities for the latest status of their national regulations for the 5GHz wireless LANs.
- If this device for operation in the band 5150-5350 MHz, it is for indoor use only.
- This equipment should be installed and operated with a minimum distance of 20 cm between the radio equipment and your body.
- The maximum RF power operating for each band as follows:
 - the band 2,400 to 2,483.5 MHz is 88.51 mW

Български (Bulgarian)	<p>С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/ЕУ.</p> <p>National Restrictions</p> <ul style="list-style-type: none">• The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details.• Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens.• Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails.
Español (Spanish)	<p>Por medio de la presente Zyxel declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/UE..</p>
Čeština (Czech)	<p>Zyxel tímto prohlašuje, že tento zařízen je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU.</p>
Dansk (Danish)	<p>Undertegnede Zyxel erklærer herved, at følgende udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU.</p> <p>National Restrictions</p> <ul style="list-style-type: none">• In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage.• I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.

Deutsch (German)	Hiermit erklärt Zyxel, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU befindet.
Eesti keel (Estonian)	Käesolevaga kinnitab Zyxel seadme seadme vastavust direktiivi 2014/53/EL põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΙΑ Ζyxel ΔΗΛΩΝΕΙ ΟΤΙ ΕΞΟΠΛΙΣΜΟΣ ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/ΕΕ.
English	Hereby, Zyxel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.
Français (French)	Par la présente Zyxel déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/UE.
Hrvatski (Croatian)	Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 2014/53/UE.
Íslenska (Icelandic)	Hér með lýsir, Zyxel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53/UE.
Italiano (Italian)	Con la presente Zyxel dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/UE. National Restrictions <ul style="list-style-type: none">• This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check http://www.sviluppoeconomico.gov.it/ for more details.• Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare http://www.sviluppoeconomico.gov.it/ per maggiori dettagli.
Latviešu valoda (Latvian)	Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 2014/53/ES būtiskajām prasībām un citiem ar to saistītajiem noteikumiem. National Restrictions <ul style="list-style-type: none">• The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details.• 2.4 GHz frekvenču joslas izmantošanai ārpus telpām nepieciešama atļauja no Elektronisko sakaru direkcijas. Vairāk informācijas: http://www.esd.lv.
Lietuvių kalba (Lithuanian)	Šiuo Zyxel deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/ES Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, Zyxel nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvető követelményeknek és az 2014/53/EU irányelv egyéb előírásainak.
Malti (Maltese)	Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Direttiva 2014/53/UE.
Nederlands (Dutch)	Hierbij verklaart Zyxel dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU.
Polski (Polish)	Niniejszym Zyxel oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/UE.
Português (Portuguese)	Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/UE.
Română (Romanian)	Prin prezenta, Zyxel declară că acest echipament este în conformitate cu cerințele esențiale și alte prevederi relevante ale Directivei 2014/53/UE.
Slovenčina (Slovak)	Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EÚ.
Slovenščina (Slovene)	Zyxel izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU.
Suomi (Finnish)	Zyxel vakuuttaa täten että laitteet tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska (Swedish)	Härmed intygar Zyxel att denna utrustning står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU.
Norsk (Norwegian)	Erklærer herved Zyxel at dette utstyret er i samsvar med de grunnleggende kravene og andre relevante bestemmelser i direktiv 2014/53/EU.

Notes:

- Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 2014/53/EU has also been implemented in those countries.
- The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

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

Safety Warnings

- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Do not expose your device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do not install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do not open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks.
- Only qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adapter first before connecting it to a power outlet.
- Do not allow anything to rest on the power adapter or cord and do NOT place the product where anyone can walk on the power adapter or cord.
- Please use the provided or designated connection cables/power cables/adapters. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adapter 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.
- 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

European Union - Disposal and Recycling Information

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

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

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

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

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

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



台灣



以下訊息僅適用於產品具有無線功能且銷售至台灣地區

- 第十二條 經型式認證合格之低功率射頻電機，非經許可，公司，商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。
- 第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。
- 無線資訊傳輸設備忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用，俟無干擾之虞，始得繼續使用。
- 無線資訊傳輸設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作，發射的信號應維持於操作頻帶中
- 使用無線產品時，應避免影響附近雷達系統之操作。
- 高增益指向性天線只得應用於固定式點對點系統。

以下訊息僅適用於產品屬於專業安裝並銷售至台灣地區

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





安全警告 - 為了您的安全，請先閱讀以下警告及指示：

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

About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

Explanation of the Symbols

SYMBOL	EXPLANATION
	Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction.
	Direct current (DC): DC is the unidirectional flow or movement of electric charge carriers.
	Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor.
	Class II equipment: The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation.

Viewing Certifications

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

Zyxel Limited Warranty

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

Note

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

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

Registration

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

Open Source Licenses

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

Index

A

- access
 - troubleshooting [152](#)
- Access Control (Rules) screen [104](#)
- ACS [137](#)
- activation
 - firewalls [101](#)
- Add New ACL Rule screen [105](#)
- Address Resolution Protocol [127](#)
- administrator password [15](#)
- Any_WAN
 - Remote Management [135](#)
 - TR-069 traffic [138](#)
- APN information
 - obtain [29](#)
- APN Settings [30](#)
- Application Layer Gateway (ALG) [95](#)
- Applications
 - add [90](#)
- applications
 - Internet access [12](#)
- ARP Table [127](#), [129](#)
- ARP Table screen [128](#)
- authentication [52](#), [53](#)
 - RADIUS server [53](#)
- Authentication Type
 - APN [30](#)
- Auto Configuration Server, see ACS [137](#)
- automatic logout [16](#)

B

- backup
 - configuration [147](#)
- backup configuration [147](#)
- Backup/Restore screen [147](#)
- Band Configuration Screen [32](#)
- Basic Service Set, see BSS

- blinking LEDs [13](#)
- bridge mode [26](#)
- Broadband [28](#)
- BSS [54](#)
 - example [55](#)

C

- CA [119](#)
- Cellular WAN [135](#)
 - TR-069 traffic [138](#)
- Cellular WAN Screen [29](#)
- Cellular WAN screen [29](#)
- certificate
 - details [121](#)
 - factory default [113](#)
 - file format [120](#)
 - file path [118](#)
 - import [113](#), [117](#)
 - public and private keys [119](#)
 - verification [120](#)
- certificate request
 - create [113](#)
 - view [115](#)
- certificates [112](#)
 - advantages [120](#)
 - authentication [112](#)
 - CA [119](#)
 - creating [113](#)
 - public key [112](#)
 - replacing [113](#)
 - storage space [113](#)
 - thumbprint algorithms [120](#)
 - thumbprints [120](#)
 - trusted CAs [117](#)
 - verifying fingerprints [120](#)
- Certification Authority, see CA
- certifications [166](#)
 - viewing [168](#)
- Channel

- information [26](#)
- channel, wireless LAN [51](#)
- client list [66](#)
- configuration
 - backup [147](#)
 - firewalls [101](#)
 - restoring [148](#)
 - static route [97](#)
- contact information [156](#)
- copyright [162](#)
- CPU Usage
 - information [26](#)
- Create Certificate Request screen [113](#)
- creating certificates [113](#)
- CTS threshold [49](#), [52](#)
- customer support [156](#)
- customized service
 - add [103](#)
- customized services [103](#), [104](#)

D

- data fragment threshold [49](#), [52](#)
- Data Roaming
 - enable [30](#)
- Date/Time
 - information [26](#)
 - Setup [139](#)
- Daylight Saving Time [140](#)
- default LAN IP address [15](#)
- Denials of Service, see DoS
- Detail Statistics screen [35](#)
- DHCP [64](#), [96](#)
- DHCP server
 - assign IP address [24](#)
- DHCP Server Lease Time [66](#)
- DHCP Server State [65](#)
- diagnostic [150](#)
- diagnostic screens [150](#)
- digital IDs [112](#)
- disclaimer [162](#)
- DMZ screen [94](#)
- DNS [64](#)

- DNS Entry
 - add [97](#)
- DNS Entry screen [96](#)
- DNS Route
 - add [80](#)
 - domain name [80](#)
- DNS Route screen [80](#)
- DNS server address [26](#)
- DNS Values [66](#)
- domain name system, see DNS
- DoS [100](#)
 - thresholds [101](#)
- DoS protection blocking
 - enable [109](#)
- dynamic DNS [96](#)
 - setup [98](#)
 - status [98](#)
- Dynamic DNS screen [98](#)
- Dynamic Host Configuration Protocol, see DHCP
- DYNDNS wildcard [96](#)

E

- e-mail
 - log setting [144](#)
- e-mail notification
 - add/edit [142](#)
- E-mail Notification screen [141](#)
- e-mail notification service port [141](#)
- Encryption mode
 - information [26](#)
- Extended Service Set IDentification [26](#), [41](#)

F

- factory-default
 - RESET button [14](#)
- filters
 - MAC address [44](#), [53](#)
- firewall
 - enhancing security [110](#)
 - information [26](#)
 - security considerations [110](#)

- traffic rule direction [107](#)
- Firewall DoS screen [108](#)
- Firewall General screen [102](#)
- firewall rules
 - direction of travel [109](#)
- firewalls [100, 101](#)
 - actions [107](#)
 - configuration [101](#)
 - customized services [103, 104](#)
 - DoS [100](#)
 - thresholds [101](#)
 - ICMP [100](#)
 - rules [109](#)
 - security [110](#)
- firmware [145](#)
- Firmware Upgrade screen [145](#)
- firmware upload [145](#)
- firmware version
 - check [146](#)
- fragmentation threshold [49, 52](#)
- FTP [86](#)
 - unusable [154](#)

G

- Gateway IP address [78](#)
- gateway IP address [79](#)
- General wireless LAN screen [40](#)

H

- hardware connections
 - troubleshooting [152](#)
- host name [25](#)

I

- IANA [70](#)
- ICMP [100](#)
- IMEI information [27](#)
- Import Certificate screen [117](#)
- importing trusted CAs [117](#)

- Internet
 - no access [154](#)
- Internet access [12](#)
- Internet Assigned Numbers Authority
 - See IANA
- Internet connection
 - slow or erratic [154](#)
- Internet Control Message Protocol, see ICMP
- IP address
 - default [15](#)
 - information [26](#)
 - WAN [29](#)
- IP Passthrough mode [35](#)
- IP Passthrough screen [34](#)
- IPv4 firewall [102](#)
- IPv6 firewall [102](#)

L

- LAN [63](#)
 - client list [66](#)
 - MAC address [67](#)
 - traffic status [125](#)
- LAN connection status
 - information [27](#)
- LAN IP address [65](#)
- LAN IPv6 Mode Setup [66](#)
- LAN Setup screen [64](#)
- LAN subnet mask [65](#)
- LAN traffic
 - packets sent/received [126](#)
- LAN Traffic Status screen [125](#)
- Language Selector [20](#)
- limitations
 - wireless LAN [54](#)
 - WPS [61](#)
- Local Area Network, see LAN
- local certificate
 - TR-069 client [138](#)
- Local Certificates screen [112](#)
- Log Setting screen [143](#)
- login
 - passwords [15](#)
 - troubleshooting [152](#)

Login screen
no access [153](#)

Logout [20](#)

logout [16](#)
automatic [16](#)

Logs
export Log [123](#)

logs [143](#)

LTE connection
strength [27](#)

LTE connection status [27](#)

LTE enabled status
information [27](#)

M

MAC [26](#)

MAC address [44, 67](#)
filter [44, 53](#)
LAN [67](#)

MAC authentication [44](#)

mail server
default port number [142](#)

mail server address [141, 142](#)

managing the device
good habits [13](#)
using FTP. See FTP.

Media Access Control, see MAC Address

Memory Usage
information [26](#)

MGMT Services screen [134](#)

model name [25](#)

MSN Messenger
problem [155](#)

Multi_WAN
Remote Management [135](#)
TR-069 traffic [138](#)

N

NAT
default server [94](#)
DMZ host [94](#)

multiple server example [87](#)

NAT ALG screen [95](#)

NAT Applications screen [89](#)

NAT Session Usage
information [26](#)

Network Address Translation, see NAT

network disconnect
temporary [146](#)

Network Map [23](#)

network type
select [32](#)

Nslookup test [151](#)

P

password
admin [153](#)
good habit [13](#)
lost [153](#)
user [153](#)

passwords [15](#)

PBC [56](#)

PIN Protection [31](#)

PIN, WPS [56](#)
example [58](#)

Ping
unusable [154](#)

Ping test [151](#)

Ping/TraceRoute/Nslookup screen [150](#)

PLMN Configuration Screen [33](#)

PoE injector [12](#)

Policy Route
add/edit [83](#)

Policy Route screen [82](#)

port forwarding rule
add/edit [88](#)

Port Forwarding screen [87, 88](#)

Port Triggering
add new rule [93](#)

Port Triggering screen [91](#)

ports [13](#)

power
troubleshooting [152](#)

preamble [50, 52](#)

preamble mode [55](#)
problem
 troubleshooting [152](#)
Protocol (Customized Services) screen [102](#)
Protocol Entry
 add [103](#)
Push Button Configuration, see PBC
push button, WPS [56](#)

Q

Quick Start Guide [15](#)

R

RADIUS server [53](#)
Reboot screen [148](#)
remote management
 TR-069 [137](#)
Remote Procedure Calls, see RPCs [137](#)
RESET Button [14](#)
restart system [148](#)
restore default settings
 after firmware upgrade [146](#)
restoring configuration [148](#)
RFC 1058. See RIP.
RFC 1389. See RIP.
RFC 1631 [85](#)
RIP [84](#)
 version [84](#)
RIP screen [84](#)
router features [12](#)
Routing Information Protocol. See RIP
routing mode [26](#)
Routing Table screen [129](#)
RPPCs [137](#)
RTS threshold [49, 52](#)

S

scheduler rule [107](#)

 add [107, 108](#)
security
 network [110](#)
 wireless LAN [52](#)
Security Log [123](#)
Security Log screen [123](#)
serial number [25](#)
service access control [134, 136](#)
service provider's name [27](#)
Service Set [41](#)
setup
 firewalls [101](#)
 static route [97](#)
SIM card
 status [27, 31](#)
SIM configuration [30](#)
SSH
 unusable [154](#)
SSID [53](#)
Static DHCP
 add device [24](#)
 Configuration [68](#)
Static DHCP screen [66](#)
Static Route
 add [78](#)
 edit [78](#)
 IP type [79](#)
 name [79](#)
static route [77, 141](#)
 configuration [97](#)
status [23](#)
 connection status [23](#)
status indicators [13](#)
Status Screen [25](#)
 refresh interval [25](#)
Status screen [19](#)
subnet mask [26](#)
 information [26](#)
syslog logging
 enable [144](#)
syslog server
 name or IP address [144](#)
system
 firmware [145](#)
 passwords [15](#)
 status [23](#)

- time [139](#)
- System Info [25](#)
- system log
 - severity level [122](#)
- System Log screen [122](#)
- system name [25](#)
- System screen [131](#)

T

- Telnet
 - unusable [154](#)
- The [29](#)
- thresholds
 - data fragment [49, 52](#)
 - DoS [101](#)
 - RTS/CTS [49, 52](#)
- time [139](#)
- time protocol [139](#)
- Time Server Address [140](#)
- Time Setting screen [139](#)
- Time Zone [140](#)
- time zone
 - set [16](#)
- TR-069 [137](#)
 - ACS setup [137](#)
 - authentication [138](#)
- TR-069 Client screen [137](#)
- Trace Route test [151](#)
- traffic status
 - LAN [125](#)
 - WAN [124](#)
- troubleshooting [152](#)
- Trust Domain
 - add [136](#)
- Trust Domain screen [135](#)
- Trusted CA certificate
 - view [118](#)
- Trusted CA screen [116](#)
- Turning on UPnP
 - Windows 7 example [70](#)

U

- Universal Plug and Play, see UPnP
- Up Time
 - system [26](#)
- upgrading firmware [145](#)
- UPnP [68](#)
 - forum [64](#)
 - security issues [64](#)
 - State [69](#)
 - undetectable [155](#)
 - usage confirmation [64](#)
- UPnP screen [68](#)
- UPnP-enabled Network Device
 - auto-discover [71](#)
- User Account screen [132](#)

V

- version
 - firmware
 - version [26](#)
- Viewing Mode
 - Icon View [23](#)
 - List View [24](#)

W

- WAN
 - packets sent/received [125](#)
 - traffic status [124](#)
 - Wide Area Network, see WAN [28](#)
- WAN Traffic Status screen [124](#)
- warranty [168](#)
 - note [169](#)
- Web Configurator [15](#)
 - Accessing [15](#)
 - easy access [74](#)
 - layout [19](#)
- web configurator
 - passwords [15](#)
- WEP Encryption [43](#)
- WiFi network mode
 - information [26](#)

- WiFi setup [17](#)
- Wireless General screen [40](#)
- wireless LAN [39](#)
 - authentication [52, 53](#)
 - BSS [54](#)
 - example [55](#)
 - channel [51](#)
 - example [50](#)
 - fragmentation threshold [49, 52](#)
 - limitations [54](#)
 - MAC address filter [44, 53](#)
 - preamble [50, 52](#)
 - RADIUS server [53](#)
 - RTS/CTS threshold [49, 52](#)
 - security [52](#)
 - SSID [53](#)
 - WPS [55, 58](#)
 - example [59](#)
 - limitations [61](#)
 - PIN [56](#)
 - push button [56](#)
- wireless LAN status
 - information [27](#)
- wizard
 - Quick Start [16](#)
- WLAN
 - status [26](#)
- WPS [55, 58](#)
 - example [59](#)
 - information [26](#)
 - limitations [61](#)
 - PIN [56](#)
 - example [58](#)
 - push button [56](#)