

User's Guide LTE Series

Default Login Details

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

Version 1.00_2.00 Ed 4, 3/2020



Copyright © 2020 Zyxel Communications Corporation

IMPORIANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

This is a series User's Guide. 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 Zyxel Device.

• More Information

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



Document Conventions

Warnings and Notes

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

Warnings tell you about things that could harm you or your Zyxel 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 LTE device 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
 Routing > DNS Route means you first click Network Setting in the navigation panel, then the Routing submenu and finally the DNS Route 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 Zyxel Device.

Zyxel Device	Generic Router	Switch
Server	Firewall	USB Storage Device
Printer		

Contents Overview

User's Guide	
Introduction	
The Web Configurator	
Quick Start	
Tutorials	
Te chnic al Reference	70
Connection Status	
Broadband	
Wireless	
Home Networking	
Routing	
Network Address Translation (NAT)	
Dynamic DNS Setup	
USB Service	
Firewall	
MAC Filter	
Parental Control	
Certificates	
Voice	
Log	
Traffic Status	
ARP Table	
Routing Table	
WLAN Station Status	
VoIP Status	
Cellular WAN Status	
System	
User Account	
Remote Management	
TR-069 Client	
Time Settings	
E-mail Notification	
Log Setting	
Firmware Upgrade	
Backup/Restore	
Diagnostic	
Troubleshooting	

Appendices	278
------------	-----

Table of Contents

Document Conventions		
Contents Overview		
lable of Contents		
Part I: Use r's Guide	15	
Chapter 1 Introduction	16	
1.1 Overview		
1.2 Application for the Zyxel Device		
1.2.1 WAN Priority (LTE3301-PLUS / LTE5388-M804 / LTE5398-M904 / LTE3316-M604)	20	
1.3 Manage the Zyxel Device	20	
1.4 Good Habits for Managing the Zyxel Device	20	
1.5 Front and Bottom Panels	21	
1.5.1 LEDs (Lights)		
1.5.2 Panel Ports & Buttons		
1.5.3 Turning On/Off WiFi		
1.5.4 The RESET Button		
1.6 Wall Mounting	33	
Chapter 2		
The Web Configurator	35	
2.1 Overview	35	
2.1.1 Access the Web Configurator	35	
2.2 Web Configurator Layout		
2.2.1 Settings Icon		
2.2.2 Widget Icon	42	
Chapter 3		
Quick Start	44	
3.1 Overview		
3.2 Quick Start Setup	44	
3.3 Time Zone	44	
3.4 The Internet Connection Setup	45	
3.4.1 Successful Internet Connection	45	
3.4.2 Unsuccessful Internet Connection	46	

3.5 Quick Start Setup-Wireless	
3.6 Quick Start Setup-Finish	
Chapter 4	
Tuto ria ls	
4.1 Overview	
4.2 Set Up a Wireless Network Using WPS	
4.2.1 Push Button Configuration (PBC)	
4.2.2 PIN Configuration	
4.3 Connect to the Zyxel Device's WiFi Network	
4.4 Use Multiple SSIDs on the Zyxel Device	
4.4.1 Configure Security Settings of Multiple SSIDs	
4.5 Make a VoIP/VoLTE Phone Call	
4.6 Configure a Firewall Rule	
4.7 Configure MAC Filter	
4.8 Upgrade Firmware on the Zyxel Device	
4.9 Back up a Configuration File	
4.10 Restore Configuration	
4.11 Connect to the Internet	
4.12 Configure DHCP	
4.12.1 Add Devices to Your Static DHCP List	
4.13 Configure Static Route for Routing to Another Network	
4.14 Access the Zyxel Device Using DDNS	
4.14.1 Register a DDNS Account on www.dyndns.org	
4.14.2 Configure DDNS on Your Zyxel Device	
4.14.3 Test the DDNS Settings	

Part II:	Te chnic a l	Re fe re nc e	70
----------	--------------	---------------	----

Chapter 5 Connection State

Connection Status			
5.1 Connection Status Overview	71		
5.1.1 Connectivity	71		
5.1.2 System Info	72		
5.1.3 Cellular Info	74		
5.1.4 WiFi Settings	78		
5.1.5 Guest WiFi Settings	79		
5.1.6 LAN	81		
apter 6			
adband	33		

6.1 Overview	83
6.1.1 What You Can Do in this Chapter	83
6.1.2 What You Need to Know	84
6.1.3 Before You Begin	84
6.2 Broadband	84
6.2.1 Add/Edit Internet Connection	85
6.3 WAN Backup	89
6.4 Ethernet WAN	90
6.5 Cellular WAN	91
6.6 Cellular SIM Configuration	92
6.7 Cellular Band Configuration	93
6.8 Cellular PLMN Configuration	94
6.9 IP Passthrough	97

Chapter 7 Wire less

7.1 Overview	
7.1.1 What You Can Do in this Chapter	
7.1.2 What You Need to Know	
7.2 General Settings	
7.2.1 No Security	
7.2.2 More Secure (WPA2-PSK)	
7.3 Guest/More AP	
7.4 More AP Edit	
7.5 MAC Authentication	
7.6 WPS	
7.7 WMM	
7.8 Others Screen	
7.9 WLAN Scheduler	
7.9.1 Add/Edit Rules	
7.10 Channel Status	
7.11 Technical Reference	
7.11.1 WiFi Network Overview	
7.11.2 Additional Wireless Terms	
7.11.3 WiFi Security Overview	
7.11.4 Signal Problems	
7.11.5 BSS	
7.11.6 Preamble Type	
7.11.7 WiFi Protected Setup (WPS)	

8.1 Overview	131
	-

8.1.1 What You Can Do in this Chapter	
8.1.2 What You Need To Know	
8.2 LAN Setup	
8.3 Static DHCP	
8.3.1 Before You Begin	
8.4 UPnP	
8.5 Technical Reference	
8.6 Turn on UPnP in Windows 7 Example	
8.6.1 Auto-discover Your UPnP-enabled Network Device	
8.7 Turn on UPnP in Windows 10 Example	
8.7.1 Auto-discover Your UPnP-enabled Network Device	
8.8 Web Configurator Easy Access in Windows 7	
8.9 Web Configurator Easy Access in Windows 10	
Chapter 9	
Routing	154
9.1 Overview	
9.2 Configure Static Route	
9.2.1 Add/Edit Static Route	
9.3 DNS Route	
9.3.1 Add/Edit DNS Route	
9.4 Policy Route	
9.4.1 Add/Edit Policy Route	
9.5 RIP Overview	
9.5.1 RIP	
Chapter 10	
Ne twork Address Translation (NAT)	162
10.1 Overview	
10.1.1 What You Can Do in this Chapter	
10.1.2 What You Need To Know	
10.2 Port Forwarding Overview	
10.2.1 Port Forwarding	
10.2.2 Add/Edit Port Forwarding	
10.3 Port Triggering	
10.3.1 Add/Edit Port Triggering Rule	
10.4 DMZ	
10.5 ALG	
10.6 Address Mapping	
10.6.1 Address Mapping Screen	
10.6.2 Add New Rule Screen	
10.7 Sessions	

Chapter 11 Dynamic DNS Setup	175
11.1 DNS Overview	175
11.1.1 What You Can Do in this Chapter	175
11.1.2 What You Need To Know	175
11.2 DNS Entry	176
11.2.1 Add/Edit DNS Entry	176
11.3 Dynamic DNS	177
Chapter 12	
USB Servic e	179
12.1 USB Service Overview	179
12.1.1 What You Need To Know	179
12.1.2 Before You Begin	180
12.2 USB Service	180
12.2.1 Add New Share	182
12.2.2 The Add New User Screen	183
Chapter 13	
Fire wall	184
131 Overview	184
13.1.1 What You Need to Know About Firewall	184
13.2 Firewall	185
13.2.1 What You Can Do in this Chapter	185
13.3 Firewall General Settinas	185
13.4 Protocol (Customized Services)	187
13.4.1 Add Customized Service	187
13.5 Access Control (Rules)	188
13.5.1 Add New ACL Rule Screen	189
13.6 DoS	191
13.7 Firewall Technical Reference	192
13.7.1 Firewall Rules Overview	192
13.7.2 Guidelines For Security Enhancement With Your Firewall	193
13.7.3 Security Considerations	193
Chapter 14	
MAC Filter	195
14.1 MAC Filter Overview	195
14.2 MAC Filter	195
14.2.1 Add New Rule	196
Chapter 15 Parental Control	197

15.1 Overview	
15.2 The Parental Control Screen	
15.2.1 Add New Parental Control Rule	
Chapter 16	
Certificates	
16.1 Certificates Overview	
16.1.1 What You Can Do in this Chapter	
16.2 Local Certificates	
16.2.1 Create Certificate Request	
16.2.2 View Certificate Request	
16.3 Trusted CA	
16.4 Import Trusted CA Certificate	
16.5 View Trusted CA Certificate	
16.6 Certificates Technical Reference	
16.6.1 Verify a Certificate	
Chapter 17	
Voice	210
171 Overview	210
17.1.1 What You Can Do in this Chapter	210
17.2 Voice Mode	210
17.3 SIP	210
17.3.1 SIP Account	211
17.3.2 SIP Account Entry Edit	211
17.3.3 SIP Service Provider	212
17.3.4 Provider Entry Edit	
17.5.4 Horider Enry Edit	
17.5 Call Rule	217
17.5 Call History	
17.61 Call History Screen	220
17.6.7 Call Summary Screen	
Chapter 18	
Log	
18.1 Log Overview	
18.1.1 What You Can Do in this Chapter	
18.1.2 What You Need To Know	
18.2 System Log	
18.3 Security Log	
Chapter 10	
Tha flie Sta tus	

19.1 Traffic Status Overview	
19.1.1 What You Can Do in this Chapter	
19.2 WAN Status	
19.3 LAN Status	
Chapter 20	
ARP Table	
20.1 ARP Table Overview	
20.1.1 How ARP Works	
20.2 ARP Table	
Chapter 21	
Routing Table	231
21.1 Routing Table Overview	
21.2 Routing Table	
Chapter 22	
WIAN Station Status	234
22.1 WLAN Station Status Overview	
Chapter 23	
VoIP Status	236
23.1 VoIP Status Screen	
Chapter 24	
Cellular WAN Status	
24.1 Cellular WAN Status Overview	
24.2 Cellular WAN Status	
Chapter 25	
Syste m	
25.1 System Overview	
25.2 System	
Chapter 26	
Use r Ac c o unt	
26.1 User Account Overview	
26.2 User Account	
26.2.1 User Account Add/Edit	
Chapter 27	
Remote Management	
27.1 Overview	

27.2 MGMT Services	
27.3 MGMT Services for IP Passthrough	
27.4 Trust Domain	
27.5 Add Trust Domain	
27.6 Trust Domain for IP Passthrough	
27.7 Add Trust Domain	
Chapter 28	
TR-069 Client	253
28.1 Overview	
28.2 TR-069 Client	253
Chapter 29	
Time Settings	255
29.1 Time Settings Overview	
29.2 Time	255
Chapter 30	
E-mail Notific ation	258
30.1 E-mail Notification Overview	
30.2 E-mail Notification	
30.2.1 E-mail Notification Edit	
Chapter 31	
Log Setting	261
31.1 Log Setting Overview	
31.2 Log Setting	
Chapter 32	
Firm ware Upgrade	264
32.1 Overview	
32.2 Firmware Upgrade	
Chapter 33	
Backup/Restore	
33.1 Backup/Restore Overview	
33.2 Backup/Restore	
33.3 Reboot	
Chapter 34	
Dia g no stic	
34.1 Diagnostic Overview	
34.2 Ping/TraceRoute/Nslookup Test	

C ha pter 35 Trouble shoo

ου	ib le sho o ting	
	35.1 Overview	
	35.2 Power and Hardware Connections	
	35.3 Zyxel Device Access and Login	
	35.4 Internet Access	
	35.5 USB Device Connection	
	35.6 UPnP	
	35.7 SIM Card	
	35.8 Cellular Signal	

Part III: Appendices	
Appendix A Customer Support	
Appendix B IPv6	285
Appendix C Legal Information	
Index	

PART I User's Guide

C HAPTER 1 Introduction

1.1 Overview

Zyxel Device refers to these models as outlined below.

- LTE3301-PLUS • LTE7480-M804 • LTE5388-M804 • LTE7240-M403 • LTE7480-S905
- LTE7461-M602
- LTE7490-M904
- LTE5398-M904

- LTE3316-M604

The following table describes the feature differences of the Zyxel Device by model.

	LIE3301-PLUS	LIE7240-M403	LIE7461-M602	LIE7480-M804	
2.4G WLAN	V	V	V	V	
5G WLAN	V	-	-	-	
LTE Speed	300/50 Mbps	150/50 Mbps (FDD-LTE) 400/150 Mbps (FDD-LTE)		600/100 Mbps	
	Note: These are the theoretical downlink/uplink rates. LTE speed is affected by strength of signal, network congestion, LTE band(s) or frequency(-ies) to which your Zyxel Device is connected, and so forth.				
Gigabit Ethernet Port	V	V	V	V	
Ethernet WAN	Convert the fourth LAN port to work as a WAN port.	-	-	-	
IP Passthrough	Available when the fourth LAN port doesn't act as an Ethernet WAN port.	V	V	V	
USB for File Sharing	V	V	V	-	
External V Antennas		-	-	-	
PoE Injector	-	V	V	-	
Wall Mount	Wall Mount -		V	V	
Pole Mount	-	-	V	V	
Firmware 1.00 Version		2.00	2.00	1.00	

Table 1 Zyxel Device Comparison Table

	LIE7480-S905	LIE7490-M904	LIE5388-M804	LIE5398-M904	LTE3316-M604
2.4G WLAN	V	V	V	V	V
5G WLAN	-	-	V	V	V
LTE Speed 573/15.1 Mbps (TDD-LTE config. #2)		1200/150 Mbps	600/100 Mbps	1200/150 Mbps	300/50 Mbps
	Note: These are the theoretical downlink/uplink rates. LTE speed is affected by strength of signal, network congestion, LTE band(s) or frequency(-ies) to which your Zyxel Device is connected, and so forth.				affected by ency(-ies) to
Gigabit Ethernet Port	V	V	V	V	V
Ethernet WAN	-	-	Convert the first LAN port to work as a WAN port.	Convert the first LAN port to work as a WAN port.	Convert the first LAN port to work as a WAN port.
IP Passthrough	V	V	Available when the first LAN port doesn't act as an Ethernet WAN port.	Available when the first LAN port doesn't act as an Ethernet WAN port.	Available when the first LAN port doesn't act as an Ethernet WAN port.
USB for File Sharing	V	-	V	V	-
External Antennas	-	-	-	-	-
PoE Injector	V	-	-	-	-
Wall Mount	V	V	-	-	V
Pole Mount	V	V	-	-	-
Firmware Version	2.00	1.00	1.00	1.00	2.00

Table 2 Zyxel Device Comparison Table

The Zyxel Device is an LTE (Long Term Evolution) router that supports (but not limited to) the following:

- WAN Backup (LTE3301-PLUS / LTE5388-M804 / LTE5398-M904 / LTE3316-M604)
- Gigabit Ethernet connection
- DHCP (Dynamic Host Configuration Protocol) server
- NAT (Network Address Translation)
- DMZ (Demilitarized Zone)
- Port Forwarding/Triggering
- ALG (Application Layer Gateway)
- Embedded Bridge/Router mode
- Dynamic DNS (Domain Name System) for the first APN (Access Point Name)
- Static/Dynamic Route setting for RIP (Routing Information Protocol)
- Remote Management under Bridge mode
- Address Resolution Protocol (ARP)
- Firewall that uses Stateful Packet Inspection (SPI) technology
- Protects against Denial of Service (DoS) attacks
- Filter of LAN MAC address, LAN IP address and URLs
- Local and remote device management

• Firmware upgrade via TR-069 and Web Configurator

The embedded Web-based Configurator enables straightforward management and maintenance. Just insert the SIM card (with an active data plan) and make the hardware connections. See the Quick Start Guide for how to do the hardware installation, wall/pole mounting, and Internet setup.

1.2 Application for the Zyxel Device

Wire less WAN

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

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

You can install two external antennas to improve your wireless WAN signal strength. See Table 1 on page 16 for the feature differences.

Wire less IAN (WiFi)

Wireless clients can connect to the LTE Device to access network resources and the Internet. Your LTE Device supports WiFi Protected Setup (WPS), which allows you to quickly set up a wireless network with strong security.



Internet Access

Your Zyxel Device provides shared Internet access by connecting to an LTE network. A computer can connect to the Zyxel Device's PoE injector or a **LAN** port for configuration via the Web Configurator. See Table 1 on page 16 for the feature differences.





Carrier Aggregation (LIE7480-M804 / LIE7490-M904 / LIE5388-M804 / LIE5398-M904 / LIE5316-M604)

Carrier Aggregation (CA) is a technology to deliver high downlink data rates by combining more than one carrier in the same or different bands together.



Figure 2 Zyxel Device's CA Application

Ethe met WAN (LIE3301-PLUS / LIE5388-M804 / LIE5398-M904 / LIE3316-M604)

If you have another broadband modem or router available, you can use the Ethernet WAN port and then connect it to the broadband modem or router. This way, you can access the Internet via an Ethernet connection and still use the Firewall function on the Zyxel Device.

- Note: For LTE3301-PLUS, convert LAN port number four as a WAN port first. See Section 6.4 on page 90 for more information about the **Network Setting** > **Broadband** > **Ethemet WAN** screen.
- Note: For LTE5388-M804 / LTE5398-M904 / LTE3316-M604, convert LAN port number one as a WAN port first. See Section 6.4 on page 90 for more information about the **Network** Setting > Broadband > Ethe met WAN screen.



1.2.1 WAN Priority (LTE3301-PLUS / LTE5388-M804 / LTE5398-M904 / LTE3316-M604)

The WAN connection priority is as follows:

- 1 Ethernet WAN
- 2 Cellular WAN (3G/4G)

1.3 Manage the Zyxel Device

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

1.4 Good Habits for Managing the Zyxel 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 33.2 on page 266. Restoring an earlier working configuration may be useful if the Zyxel 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. Write down any information your ISP provides you.

1.5 Front and Bottom Panels

The LED indicators are located on the front (LTE7240-M403 / LTE3301-PLUS / LTE5388-M804 / LTE5398-M904 / LTE3316-M604)/ the bottom panel (LTE7461-M602 / LTE7480-M804 / LTE7480-S905 / LTE7490-M904)/ the rear panels (LTE5388-M804 / LTE5398-M904 / LTE5316-M604).

Front & Top Panels

Figure 4 Front Panel (LTE3301-PLUS)



Figure 5 Front Panel (LTE7240-M403)















Figure 12 Bottom Panel (LTE7461-M602 / LTE7480-M804 / LTE7480-S905 / LTE7490-M904)



Figure 13 Rear Panel (LTE5388-M804 / LTE5398-M904)







Figure 15 Rear Panel (LTE3316-M604)



Figure 16 Side Panel (LTE3316-M604)



1.5.1 IEDs (Lights)

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

LED	COLOR	STATUS	DESC RIPTIO N
POWER	White	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.
Internet	White	On	There is Internet connection.
		Blinking	The Zyxel Device is sending or receiving IP traffic.
		Off	There is no Internet connection.

Table 3 LTE3301-PLUS LED Descriptions

LTE Series User's Guide

24

IED	COLOR	STATUS	DESC RIPTIO N
LTE/3G	White	On	The Zyxel Device is registered and successfully connected to a 4G network.
		Blinking (slow)	The Zyxel Device is connected to a 3G network.
		Blinking (fast)	The Zyxel Device is trying to connect to a 3G/4G network.
		Off	There is no service.
	Green	On	The Zyxel Device has an Ethernet connection on the WAN.
		Off	There is no Ethernet connection on the WAN.
Signal	Green	On	The signal strength is excellent.
Strength	Amber	On	The signal strength is fair.
	Red	On	The signal strength is poor.
		Blinking	There is no SIM card inserted, no signal, or the signal strength is below the poor level.
		Off	The SIM card is invalid, or the PIN code is not correct.
WLAN	Green	On	The 2.4 GHz wireless network is activated.
		Blinking (slow)	The Zyxel Device is setting up a WPS connection with a 2.4 GHz wireless client.
		Blinking (fast)	The Zyxel Device is communicating with 2.4 GHz wireless clients.
	White	On	The 5 GHz wireless network is activated.
		Blinking (slow)	The Zyxel Device is setting up a WPS connection with a 5 GHz wireless client.
		Blinking (fast)	The Zyxel Device is communicating with 2.4 GHz and 5 GHz wireless clients.
		Off	The wireless network is not activated.
USB	White	On	The Zyxel Device recognizes a USB connection through the USB port.
		Blinking	The Zyxel Device is sending/receiving data to/from the USB device connected to it.
		Off	The Zyxel Device does not detect a USB connection through the USB port.

Table 3 LTE3301-PLUS LED Descriptions (continued)

Note: Blinking (slow) means the LED blinks once per second. Blinking (fast) means the LED blinks once per 0.5 second.

LED	COLOR	STATUS	DESC RIPTIO N	
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.	

Table 4 LTE7240-M403 LED Descriptions

IED	COLOR	STATUS	DESC RIPTIO N
LTE/3G/2G Green On		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	Green	On	The signal strength is excellent.
Strength	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.

Table 4 LTE7240-M403 LED Descriptions (continued)

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

Table 5	$/ TF7/80_N/80/$	1 TE7/80_905	/ITE7/90-M90/IED Descriptions
	/ LIL/ 400-10004	1 L L + 00 - 3703	

COLOR	STATUS	DESC RIPTIO N
Red	Red Blinking The Zyxel Device is booting or self-testi	
	On	The Zyxel Device encountered an error.
Green	Blinking	The Zyxel Device is trying to connect to the Internet.
	On	The Zyxel Device is connected to the Internet.
Amber	Blinking	The Zyxel Device WiFi is on.

Table 6 LTE5388-M804 / LTE5398-M904 LED Descriptions

IED	COLOR	STATUS	DESC RIPTIO N
Power/System or USB	Green	On	The Zyxel Device is receiving power and ready for use.
		Blinking	The Zyxel Device is booting.
		Off	The Zyxel Device is not receiving power.
	Blue	On	The Zyxel Device is sending/receiving data to/from the USB device connected to it.
		Off	The Zyxel Device does not detect a USB connection through the USB port.
Internet/SMS	Green	On	There is Internet connection.
		Blinking	There is a new SMS message.
		Off	There is no Internet connection.
LTE/3G 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 LTE/3G signal or the signal strength is below the poor level.

Table 6 L	.TE5388-M804 /	' LTE5398-M904 LED	Descriptions	(continued)
-----------	----------------	--------------------	--------------	-------------

LED	COLOR	STATUS	DESC RIPTIO N
WiFi/WPS	Green	On	The WiFi AP is activated.
		Blinking (fast)	Data is being transmitted and received.
		Blinking (slow)	The WPS is activated.
Voice	Green	On	A telephone connected to the PHO NE port has its receiver off the hook.
		Blinking	The Zyxel Device is receiving an incoming call.
		Off	A telephone connected to the PHO NE port has its receiver on the hook.
LAN Green On Blinking		On	The Zyxel Device recognizes an Ethernet cable through the LAN port.
		Blinking	The Zyxel Device is sending/receiving data through the LAN.
		Off	The wireless network is not activated.

Table 7	LTE3316-M604 LED	Descriptions
100107		Doscriptions

LED COLOR		STATUS	DESC RIPTIO N	
Power	White	On	The Zyxel Device is receiving power and functioning properly.	
		Blinking	The Zyxel Device is in the process of starting up or default restoring.	
		Off	The Zyxel Device is not receiving power.	
Internet	White	On	The Zyxel Device's WAN connection is ready, but there is no traffic.	
		Blinking	The Zyxel Device is transmitting and receiving data through the WAN.	
		Off	The WAN connection is not ready, or has failed.	
LTE/3G Signal Strength	White	On	The Zyxel Device is successfully connected to a 4G network.	
		Blinking	The Zyxel Device is successfully connected to a 3G network.	
	Green	On	The Zyxel Device is successfully connected to an Ethernet WAN network.	
Signal Strength	Green	On	The signal strength is good.	
	Orange	On	The signal strength is fair.	
	Red	On	The signal strength is poor.	
		Blinking	A valid SIM card is inserted, but no signal is detected.	
WLAN/WPS	White	On	This indicates either 5G and 2.4G wireless LAN are both on or the 5G wireless LAN is on.	
		Blinking	This indicates either 5G and 2.4G WPS are both on or the 5G WPS is on.	
	Green	On	The 2.4G wireless LAN is on, but the Zyxel Device is not sending/receiving data through the wireless LAN.	
		Blinking	The Zyxel Device is ready and the 2.4G WPS is on.	

LED	COLOR	STATUS DESCRIPTION		
Voice	White	On	A telephone connected to the PHONE port has its receiver on the hook.	
		Blinking	The Zyxel Device is receiving an incoming call.	
		Off	A telephone connected to the PHONE port has its receiver off the hook.	
LAN	Green	On	A 10/100 Mbps LAN connection is ready.	
		Blinking	The Zyxel Device is sending/receiving data at 10/100 Mbps through a LAN port.	
		Off	The wireless network is not activated.	
	Orange	On	A 1000 Mbps LAN connection is ready.	
		Blinking	The Zyxel Device is sending/receiving data at 1000 Mbps through a LAN port.	
		Off	The wireless network is not activated.	

Table 7 LTE3316-M604 LED Descriptions (continued)

1.5.2 Panel Ports & Buttons

The connection ports are located on the bottom/rear panels.

The following table describes the items on the bottom panel.

IABELS	DESC RIPTIO N
ANT1-ANT2	Install the external antennas to strengthen the cellular signal.
USB	The USB port of the Zyxel Device is used for file sharing.
LAN/Ethernet	Connect a computer via the PoE injector for configuration.
	Connect the PoE injector to a power outlet to start the device.
LAN/WAN	For LTE5388-M804 / LTE5398-M904 / LTE3316-M604, connect an RJ45 cable to a modem to connect to the Internet when using a LAN port as a WAN port.
LAN	For LTE5388-M804 / LTE5398-M904 / LTE3316-M604, connect an RJ45 cable to a computer to connect to the internal network In using a LAN port.
WiFi	Press the WLAN (WiFi) button for more than five seconds to enable the wireless function. To set up a WiFi connection between the Zyxel Device and a wireless client, press the WPS button for longer than five seconds for LTE5388-M804 / LTE5398-M904, and press the WPS button for two seconds for LTE3316-M604.
WPS	After the wireless function is enabled, press the WLAN button for more than one second but less than five seconds to quickly set up a secure wireless connection between the Zyxel Device and a WPS-compatible client. To enable WPS, press the WPS button for less than five seconds for LTE5388-M804 / LTE5398-M904, and press the WPS button for more than five seconds for LTE3316-M604.
RESET	Press the button for more than five seconds to return the Zyxel Device to the factory defaults.
POWER Button	Press the POWER button after the power adapter is connected to start the Zyxel Device.
POWER /DC IN	Connect the power adapter and press the POWER button to start the Zyxel Device.
Reboot	Press the RESET button for more than 2 seconds but less than 5 seconds, it will cause the system to reboot.

Table 8 Panel Ports and Buttons

LABELS	DESC RIPTIO N
SIM card	Insert a micro-SIM card into the slot with the chip facing down and the beveled corner in the top left corner.
PHONE	For LTE5388-M804 / LTE5398-M904 / LTE3316-M604, the phone port is used for VoIP and VoLTE.
INT/EXT	For LTE5388-M804 / LTE5398-M904, the internal/external switch is used for selecting between the internal or external LTE antenna.

Table 8 Panel Ports and Buttons (continued)

1.5.3 Turning On/Off WiFi

Use the **WPS** or **WiF/WPS** button on the Zyxel Device to turn on or turn off the wireless network.

Note: Use the WiFi function of the LTE7461-M602 / LTE7480-M804 / LTE7480-S905 / LTE7490-M904 for configuration (for example, connect to the LTE Ally app of your mobile device to find the optimal LTE signal strength and manage your LTE7461-M602 / LTE7480-M804 / LTE7480-S905 / LTE7490-M904).

Figure 17 LTE3301-PLUS WiFI/WPS Button

ZYXEL	٢	0	ů.	cf)	÷	ч р	
-	_	_					

Figure 18 LTE7240-M403 WiFi Button



Figure 19 LTE7461-M602 / LTE7480-M804 / LTE7480-S905 / LTE7490-M904 WiFi Button



LTE Series User's Guide





Figure 21 LTE3316-M604 WPS button



To turn on WiFi:

• Make sure the **POWER** LED is on and not blinking. Press the **WiFi** or **WiFi**/**WPS** button for more than 5 seconds and release it.

For LTE3301-PLUS: Once WiFi is turned on, the **WIAN** LED turns green/white.

For LTE7240-M403: Once WiFi is turned on, the **WIAN** LED shines green.

For LTE7461-M602 / LTE7480-M804 / LTE7480-S905 / LTE7490-M904: Once WiFi is turned on, the LED blinks amber.

For LTE5388-M804 / LTE5398-M904: Once WiFi is turned on, the LED turns green.

• Make sure the **POWER** LED is on and not blinking. Press the **WiFi** or **WiFi**/**WPS** button for 2 seconds.

For LTE3316-M604: Once WiFi is turned on, the **WIAN** LED turns green/white.

To activate WPS (WiFimust be already on):

You can also quickly set up a secure wireless connection between the Zyxel Device and a WPScompatible client by adding one device at a time.

• Press the **WiFi** or **WiFi**/ **WPS** button for more than 1 second but less than 5 seconds and release it (pressing more than 5 seconds will turn off WiFi). Press the WPS button on another WPS-enabled device within range of the Zyxel Device.

For LTE3301-PLUS: Once a wireless connection is ready, the **WIAN** LED turns green/white.

For LTE7240-M403: Once a wireless connection is ready, the **WIAN** LED shines green.

For LTE7461-M602 / LTE7480-M804 / LTE7480-S905 / LTE7490-M904: Once a wireless connection is ready, the LED blinks amber.

For LTE5388-M804 / LTE5398-M904: Once a wireless connection is ready, the **WPS** LED blinks green.

• Press the **WiFi** or **WiFi**/**WPS** button for more than 5 second of the Zyxel Device and release it. Press the WPS button on another WPS-enabled device within range of the Zyxel Device.

For LTE3316-M604:

Once a wireless connection is ready, the **WPS** LED blinks green/white.

To turn off the wire less network:

• Press the WiFi or WiFi/WPS button for more than 5 seconds.

For LTE3301-PLUS: The **WIAN** LED turns off when the wireless network is off.

For LTE7240-M403: The **WIAN** LED turns off when the wireless network is off.

For LTE7461-M602 / LTE7480-M804 / LTE7480-S905 / LTE7490-M904: The amber LED turns off when the wireless network is off.

For LTE5388-M804 / LTE5398-M904 / LTE3316-M604: The **WIAN** LED turns off when the wireless network is off.

• Press the WiFi or WiFi/ WPS button for 2 seconds.

For LTE3316-M604: The **WIAN** LED turns off when the wireless network is off.

1.5.4 The RESET Button

If you forget your password or cannot access the Web Configurator, you will need to use the **RESET** button of the Zyxel 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 the default (see the Zyxel Device label) and the IP address will be reset to **192.168.1.1**.





Figure 23 Reset Button (LTE7240-M403)



Figure 24 Reset Button (LTE7461-M602 / LTE7480-M804 / LTE7480-S905 / LTE7490-M904)





Figure 25 Reset Button (LTE5388-M804 / LTE5398-M904)

Figure 26 Reset Button (LTE3316-M604)

PRAFT PCARE DC N	LINEWAN LAND	-240 LACE	N+048E
	$\triangle \triangle$	$\triangle \triangle$] 🖸

- 1 Make sure the Zyxel Device is connected to power and **POWER** LED is on.
- 2 To set the Zyxel 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.

1.6 Wall Mounting

Please refer to the installation guide below for the wall mounting procedures of the LTE3316-M604. You may need screw anchors if mounting on a concrete or brick wall.

Table 9 Wall Mounting Information	
Distance between holes	100 mm
M4 Screws	Two
Screw anchors (optional)	Two

Do the following to attach your Zyxel Device to a wall.

- 1 Select a position free of obstructions on a wall strong enough to hold the weight of the device.
- 2 Mark two holes on the wall at the appropriate distance apart for the screws.

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

Do not wall mount the Zyxel Device over a height of 2 m.

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

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

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

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







C HAPTER 2 The Web Configurator

2.1 Overview

The Web Configurator is an HTML-based management interface that allows easy system setup and management via Internet browser. Use a browser that supports HTML5, such as Internet Explorer 11, Mozilla Firefox, or Google Chrome. 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 Zyxel Device.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

2.1.1 Access the Web Configurator

- 1 Make sure your Zyxel Device hardware is properly connected (refer to the Quick Start Guide).
- 2 Launch your web browser. If the Zyxel Device does not automatically re-direct you to the login screen, go to http://192.168.1.1.
- 3 A password screen displays. Select the language you prefer (upper right).
- 4 To access the Web Configurator and manage the Zyxel Device, type the default username **admin** and the randomly assigned default password (see the Zyxel Device label) in the **Login** screen and click **Login**. If you have changed the password, enter your password and click **Login**.

Figure 29 Password Screen

ZYXEL UT349-MIC	We w
Login	
ne l'ere	
a segured	
	<u> </u>
by a	

- Note: The first time you enter the password, you will be asked to change it. Make sure the new password must contain at least one uppercase letter, one lowercase letter and one number.
- 5 The Connection Status screen appears. Use this screen to configure basic Internet access and wireless settings.



Figure 30 Connection Status
2.2 Web Configurator Layout



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

- A Settings Icon (Navigation Panel & Side Bar)
- **B** Widget Icon
- C Main Window

2.2.1 Settings Icon

2.2.1.1 Side Bar

The side bar provides some icons on the right hand side.





The icons provide the following functions.

ICON	DESC RIPTIO N
Without	Wizand: Click this icon to open screens where you can configure the Zyxel Device's time zone and wireless settings. See Chapter 3 on page 44 for more information about the Wizand screens.
	Theme: Click this icon to select a color that you prefer and apply it to the Web Configurator.
liter a	Theme
	Ianguage: Select the language you prefer.
	Restart: Click this icon to reboot the Zyxel Device without turning the power off.
	Logout: Click this icon to log out of the Web Configurator.

2.2.1.2 Navigation Panel

Use the menu items on the navigation panel to open screens to configure Zyxel Device features. The following tables describe each menu item.

Table 11 Navigation Panel Summary

LINK	ТАВ	FUNCTION	
Home		Use this screen to configure basic Internet access and wireless settings. This screen also shows the network status of the Zyxel Device and computers/devices connected to it.	
Network Setting			
Broadband	Broadband	Use this screen to view and configure ISP parameters, WAN IP address assignment, and other advanced properties.	
	WAN Backup	Use this screen to configure your Zyxel Device's Internet settings if the cellular connection is down.	
	Ethernet WAN	Use this screen to convert the LAN port as WAN port, or restore the WAN port to LAN port.	
	Cellular WAN	Use this screen to configure an LTE WAN connection that includes the Access Point Name (APN) provided by your service provider.	
	Cellular SIM	Use this screen to enter a PIN for your SIM card to prevent others from using it.	
	Cellular Band	Use this screen to configure the LTE frequency bands that can be used for Internet access as provided by your service provider.	
	Cellular PLMN	Use this screen to view available PLMNs and select your preferred network.	
	Cellular IP Passthrough	Use this screen to enable IP Passthrough mode (bridge mode). Note: This screen is not available when the fourth LAN port acts as an Ethernet WAN port. See Table 1 on page 16 for the feature differences of the Zyxel Devices.	
Wireless	General	Use this screen to configure the wireless LAN settings and WLAN authentication/security settings.	
	Guest/More AP	Use this screen to configure multiple BSSs on the Zyxel Device.	
	MAC Authentication	Use this screen to block or allow wireless traffic from wireless devices of certain SSIDs and MAC addresses to the Zyxel Device.	
	WPS	Use this screen to configure and view your WPS (WiFi Protected Setup) settings.	
	WMM	Use this screen to enable or disable WiFi MultiMedia (WMM).	
	Others	Use this screen to configure advanced wireless settings.	
	WLAN Scheduler	Use this screen to create rules to schedule the times to permit Internet traffic from each wireless network interfaces.	
	Channel Status	Use this screen to scan wireless LAN channel noises and view the results.	
Home Networking	LAN Setup	Use this screen to configure LAN TCP/IP settings, and other advanced properties.	
	Static DHCP	Use this screen to assign specific IP addresses to individual MAC addresses.	
	UPnP	Use this screen to turn UPnP and UPnP NAT-T on or off.	

LINK	ТАВ	FUNCTION
Routing	Static Route	Use this screen to view and set up static routes on the Zyxel Device.
	DNS Route	Use this screen to forward DNS queries for certain domain names through a specific WAN interface to its DNS server(s).
	Policy Route	Use this screen to configure policy routing on the Zyxel Device.
	RIP	Use this screen to configure Routing Information Protocol to exchange routing information with other routers.
NAT	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	Port Triggering	Use this screen to change your Zyxel Device's port triggering settings.
	DMZ	Use this screen to configure a default server which receives packets from ports that are not specified in the Port Forwarding screen.
	ALG	Use this screen to enable or disable SIP ALG.
	Address Mapping	Use this screen to change your Zyxel Device's IP address mapping settings.
	Sessions	Use this screen to limit the number of NAT sessions each client can use.
DNS	DNS Entry	Use this screen to view and configure DNS routes.
	Dynamic DNS	Use this screen to allow a static hostname alias for a dynamic IP address.
USB	USB Service	Use this screen to enable file sharing via the Zyxel Device.
Security		
Firewall	General	Use this screen to configure the security level of your firewall.
	Protocol	Use this screen to add Internet services and configure firewall rules.
	Access Control	Use this screen to enable specific traffic directions for network services.
	DoS	Use this screen to activate protection against Denial of Service (DoS) attacks.
MAC Filter	MAC Filter	Use this screen to block or allow traffic from devices of certain MAC addresses to the Zyxel Device.
Parental Control	Parental Control	Use this screen to define time periods and days during which the Zyxel Device performs parental control and/or block web sites with the specific URL.
Certificates	Local Certificates	Use this screen to view a summary list of certificates and manage certificates and certification requests.
	Trusted CA	Use this screen to view and manage the list of the trusted CAs.
Voice	Voice Mode	Use this screen to enable the Voice Mode on the Zyxel Device.
	SIP	Use this screen to set up information about your SIP account.
	Phone	Use this screen to change settings that depend on the country you are in.
	Call Rule	Use this screen to add, edit, or remove speed-dial numbers for outgoing calls.
	Call History	Use this screen to view a call history list.
System Monitor		

 Table 11
 Navigation Panel Summary (continued)

LINK	ТАВ	FUNCTION	
Log	System Log	Use this screen to view the status of events that occurred to the Zyxel Device. You can export or email the logs.	
	Security Log	Use this screen to view all security related events. You can select the level and category of the security events in their proper drop-down list window.	
		Levels include:	
		 Emergency Alert Critical Error Warning Notice Informational Debugging Categories include: Account Attack 	
		Allock Firewall MAC Filter	
Traffic Status	WAN	Use this screen to view the status of all network traffic going through the WAN port of the Zyxel Device.	
	LAN	Use this screen to view the status of all network traffic going through the LAN ports of the Zyxel Device.	
VoIP Status	VoIP Status	Use this screen to view VoIP registration, current call status and phone numbers.	
ARP table	ARP table	Use this screen to view the ARP table. It displays the IP and MAC address of each DHCP connection.	
Routing Table	Routing Table	Use this screen to view the routing table on the Zyxel Device.	
WAN Station Status	WAN Station Status	Use this screen to view the wireless stations that are currently associated to the Zyxel Device's wireless LAN.	
Cellular WAN Status	Cellular Statistics	Use this screen to look at the cellular Internet connection status.	
Maintenance			
System	System	Use this screen to set the Zyxel Device name and Domain name.	
User Account	User Account	Use this screen to change the user password on the Zyxel Device.	
Remote Management	MGMT Services	Use this screen to enable specific traffic directions for network services.	
	MGMT Services for IP Passthrough	Use this screen to enable various approaches to access this Zyxel Device remotely from a WAN and/or LAN connection.	
	Trust Domain	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 screen.	
	Trust Domain for IP Passthrough	Use this screen to enable public IP addresses to access this Zyxel Device remotely from a WAN and/or LAN connection.	
TR-069 Client	TR-069 Client	Use this screen to configure your Zyxel Device to be managed remotely by an Auto Configuration Server (ACS) using TR-069.	
Time	Time	Use this screen to change your Zyxel Device's time and date.	
Email Notification	Email Notification	Use this screen to configure up to two mail servers and sender addresses on the Zyxel Device.	

 Table 11
 Navigation Panel Summary (continued)

LINK	ТАВ	FUNCTION	
Log Setting	Log Setting	Use this screen to change your Zyxel Device's log settings.	
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your Zyxel Device.	
Backup/Restore	Backup/Restore	Use this screen to backup and restore your Zyxel Device's configuration (settings) or reset the factory default settings.	
Reboot	Reboot	Use this screen to reboot the Zyxel Device without turning the power off.	
Diagnostic	Ping&Traceroute &Nslookup	Use this screen to identify problems with the DSL connection. You can use Ping, TraceRoute, or Nslookup to help you identify problems.	

Table 11 Navigation Panel Summary (continued)

2.2.1.3 Dashboard

Use the menu items in the navigation panel on the right to open screens to configure the Zyxel Device's features.



Figure 33 Navigation Panel

2.2.2 WidgetIcon

Click this icon (**H**) in the lower left corner to arrange the screen order.

Connecti	vity	System Info
23	~ ~	Analie Marie 1783801-MUS
(£)		Herbycon Marken 1.00(ABGU.0)63
S		Sector Listone
		WALLAN Connection down
_		<u>*</u>
Cellular li	nto	Wifi Selfings
	IP Painthrough Made	🛣 mentioner 🖷 Inexes
3345300		
Status Status	Connection down	2yzol_9919

Select a block and hold it to move around. Click the Check icon (2010) in the lower left corner to save the changes.



Pacija, Lame		
- Name -		ł
10.144	1 Marian	- 4 <mark>6</mark>
	141	*
al address and	100 Mar 1994	

C HA PTER 3 Quic k Start

3.1 Overview

Use the Wizard screens to configure the Zyxel Device's time zone and wireless settings.

Note: See the technical reference chapters (starting on Chapter 5 on page 71) for background information on the features in this chapter.

3.2 Quick Start Setup

You can click the **Wizard** icon in the side bar to open the **Wizard** screens. See Section 2.2.1.1 on page 37 for more information about the side bar. After you click the **Wizard** icon, the following screen appears. Click **Let's Go** to proceed with settings on time zone and wireless networks. It will take you a few minutes to complete the settings on the **Wizard** screens. You can click **Skip** to leave the **Wizard** screens.



3.3 Time Zone

Select the time zone of your location. Click Next.

tel's gu ani

Figure 37 Wizard - Time Zone

1 > Time sone	$\left< \frac{1}{2} \right>$	N	(3) 300
HT# Inne			
(CAST+08:00)	talpat		
Back	Ne	ext.	

3.4 The Internet Connection Setup

Select the Internet connection mode of the Zyxel Device. Click Next to continue.

Figure 38 Wizard - Internet



3.4.1 Successful Internet Connection

The Zyxel Device has Internet access.



Figure 39 Wizard - Successful Internet Connection

3.4.2 Unsuccessful Internet Connection

The Zyxel Device didn't detect a WAN connection.

Figure 40 Wizard - Internet Connection is down



3.5 Quick Start Setup-Wireless

Turn WiFi on or off. If you keep it on, record the **WiFi Name** and **Password** in this screen so you can configure your wireless clients to connect to the Zyxel Device. If you want to show or hide your WiFi password, click the Eye icon ()).

Figure 41 Wizard - Wireless	
O > Those rooms	Vensi Will
2.415 Wi 1 👘	sGWFT 👝
ATLATE	with one
2000_0003	20204(J1023)_982
A Trendent	GT Spectrat
Zwegli Forg	weigh Purp
19	900

Note: You can also enable the wireless service using any of the following methods: Click **Network Setting** > **Wire less** to open the **General** screen. Then select **Enable** in the **Wire less** field. Or, Press the **WiFi** button located under the **RESET** button (see Section 1.5.4 on page 31 for the location and for how long the wireless function is turned on) for one second.

3.6 Quick Start Setup-Finish

Your Zyxel Device saves your settings and attempts to connect to the Internet.

C HA PTER 4 Tuto ria ls

4.1 Overview

This chapter provides tutorials for setting up your Zyxel Device.

- Set Up a Wireless Network Using WPS
- Connect to the Zyxel Device's WiFi Network
- Use Multiple SSIDs on the Zyxel Device
- Make a VoIP/VoLTE Phone Call
- Configure a Firewall Rule
- Configure MAC Filter
- Upgrade Firmware on the Zyxel Device
- Back up a Configuration File
- Restore Configuration
- Connect to the Internet
- Configure DHCP
- Configure Static Route for Routing to Another Network
- Access the Zyxel Device Using DDNS

4.2 Set Up a Wireless Network Using WPS

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

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

- Push Button Configuration (PBC) create a secure wireless network simply by pressing a button. See Section 4.2.1 on page 49. This is the easier method.
- **PIN Configuration** create a secure wireless network simply by entering a wireless client's PIN (Personal Identification Number) in the Zyxel Device's interface. See Section 4.2.2 on page 50. This is the more secure method, since one device can authenticate the other.

4.2.1 Push Button Configuration (PBC)

- 1 Make sure that your Zyxel Device is turned on. Make sure the wireless LAN is turned on by pressing the WiF/WPS button for two seconds, and that the device is placed within range of your notebook (for LTE3316-M604). For more information about WiFi/WPS settings, see Section 1.5.3 on page 29.
- 2 WPS is enabled by default on the Zyxel Device. If not, log into the Zyxel Device's Web Configurator and press the **Push Button** in the **Configuration > Network Setting > Wire less > WPS** screen. You can either press the WPS button on the Zyxel Device's top/side panel or press **WPS** in the screen.
- 3 Go to your phone settings and turn on WiFi. Open the WiFi networks list and tap WPS Push Button or the WPS icon (
 - Note: It doesn't matter which button is pressed first. You must press the second button within two minutes of pressing the first one.

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

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





4.2.2 PIN Configuration

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

- 1 Go to your phone settings and turn on WiFi. Open the WiFi networks list and tap WPS PIN Entry to get a PIN number.
- 2 Enter the client's PIN number in the **PIN** field in the **Configuration > Network Setting > Broardband > Cellular SIM** screen on the Zyxel Device.
- 3 Click Start button (or the button next to the PIN field) on the Zyxel Device's Cellular SIM screen within two minutes.

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

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



Figure 43 Example WPS Process: PIN Method

4.3 Connect to the Zyxel Device's WiFi Network

In this example, you've configured the Zyxel Device's WiFi Network to the following settings.

SSID SSID_Example

Channel	6
Se c urity	WPA2-PSK
	(Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)

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

- 1 The Zyxel Device supports IEEE 802.11b, IEEE 802.11g, and IEEE 802.11n wireless clients. Make sure that your notebook or computer's wireless adapter supports one of these standards.
- 2 Click the WiFi icon in your computer's system tray.



- 3 The Wireless Network Connection screen displays. Click the refresh button to update the list of the available wireless APs within range.
- 4 Select SSID_Example and click Connect.

Not connected	69.00
Connections are available	the second
Window Matwork Commercies	100
Umrya_VILAN	.eff
ZyaEL_CSO	-ett
Zykel, CSO, 240	All
Unizya_MANAGER	A
705DF	M
ISID_Exemple	
Connect automatically	nect .
ZysEL Wi-Fi Open Network and Sharing Ce	,atl .: nter

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

-	Connect to a Nativork
	Type the 8-digit PIN from the router display
	9ht
	Connect using a security key initial
	Back Ree Conce

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

Connect to a Net	wait
Type the netwo	irk security key
Security key:	ThisismyWPA-PSKpre-sharedkey
	📰 Hide characters
	OK Cince

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

Currently connected to ZyXEL.com Internet access		49	1
Winites Network Corne	naitan	1	T
SSID_Example	Connected	at	
Unices WLAN		aff	
2yxEL_CSO		att	
2yXEL_CS0_246		A	
Unings_MANAGER		M	
8475		al	
ZyxEL_WA-Fi		M	
Amplifi		.M	-
Open Network and	t Sharing Care	D	

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

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

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

4.4 Use Multiple SSIDs on the Zyxel Device

You can configure more than one SSID on a Zyxel Device. See Section 7.3 on page 104.

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

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

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



4.4.1 Configure Security Settings of Multiple SSIDs

The Zyxel Device is in router mode by default.

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

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

- 1 Connect your computer to the LAN port of the Zyxel Device using an Ethernet cable.
- 2 The default IP address of the Zyxel Device is "192.168.1.1". In this case, your computer must have an IP address in the range between "192.168.1.2" and "192.168.1.254".
- 3 Click Start > Run on your computer in Windows. Type "cmd" in the dialog box. Enter "ipconfig" to show your computer's IP address. If your computer's IP address is not in the correct range then see Section 7.3 on page 104 for information on changing your computer's IP address.
- 4 After you've set your computer's IP address, open a web browser such as Internet Explorer and type "http://192.168.1.1" as the web address in your web browser.
- 5 Use "admin" as the user name and "1234" (default) as the password and click Login.
- 6 Go to Configuration > Network Setting > Wire less > Guest/More AP. Click the Modify/Edit icon of the first entry to configure wireless and security settings for SSID_Worker.

This the	Constituent Af	<mark>en en source de la constance de</mark>	a a deligen et leger e viere. Resonert met Adéptioneme et	d averativity in a Transfer	(malar ta
1	Sister	sun	Seculity	General Marca	Roam
	7	27%6 5653 gued	WHO America	1-04	
¢	4	7/10/10/02/21/10/02	White Priorient	1.0	12
1	7	200 983.793	and a second	6.22	67
		1100000 U.S. 120			

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

in any torus Drang Oren Brank M 422 and Rank M 422 and Rank M 422 and	an an only all a state of only the state of the state of the state of the state the state of the state of	Augus Housen (Province centre)
leary Deen Barb H-121 and Paren	er an offer get - 1 Mg was a de tradición manages de l'ana de activitada y - 317 - 1117.	Auto Broom (Broom control)
landy Lond Trans y Veen Starts Writti and Starts Writti and	e an an An - Pac an An - Andre Manager - An - Ang - The Andre	function of provincement of
ang tanal tenerytene	e antes partes	Name de com Jecomercente d
a Py tand Tanany Unio		kan keon Jacobi caled
iðg tænd		Santa Frances (Pravolationality)
ning kanad		has been
Sector de		
A STATE STATE 1991	-	
line r	8m	
	And the second	
Radi Antonia Reven	en eta destrucción endescadora	calculation of works
a ann an a	en staat wel operation op to dat het witten welde te naam internet op operation internet operationen operation	a la facta analis de traditionador Art. Analis de Antonio atom et la anciente Maria
1000		Dev
 Description 	0	1003
You Build		
ALC: N		
and the server print.	CID A day	
C REPORTED A CONCEPT OF		
a francisco d		

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

initia :	GestlyNeve vt.	Later and in the	1. Ores Coursellers		
+ +++++++++++++++++++++++++++++++++++++	and the second			and the second second	
4	i i an		9 m l	· · · · · · · · ·	1887 I
	4.		10.00 / 1000	¥ 5.	
	¥.	10 20m	The second product	44	
	27	1997 - 1990 -	10.3.3.9 million	25	100

9 Configure the screen as follows. In this example, you do not enable Intra-BSS Thaffic for SSID_VoIP. Click OK.

Versition Security Severi Weak Network Addres Valle Versition Free Station L. Separation Versition Security Versition	
Security Invest When Period Alama Free Sill Security 200 Security 20	
Whee Revolution III we we we III we	
C Perro Mar La Second Mondale Second Spontement Mar Alexante	
L_ General Ander Des Applement Restants	
bey Spolener Bestante	
	(con-
ViceEcontractor	a farmer and a second
here.	
 Mod Valleon Sort Act to This Set: Store you to confiden the modifully po- 	REPORT OF THE SOCIES WARE
Statistics - conditions of the children set of the providence of the set	In the International Advances of the
Children in a stand has also been submitted by a standard and the submitted by the submitte	un en la des
A Line Meridian Constraint Science A. Line House have	near performance
40 T 547 T 64 B 14 W	
untranet 🕒 J	
Security Sevel	
	de terres
Photos units pr	a a second at the
4	

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

nd ÷	h web on the hydrogram	n naiseachta naiseachta an a-chan le GMGC1	sue Lene Maggiorences constraine	or a subscription of the subscription of the	Harver Set.
<u>.</u>	Status	390	Secury	GaastWilde	Halls
1		S.D. Home	m22/#re-++1	F. 118	R
2	1	320,950F	MTA3-Percela	1/74	20
2	(Q)	Direct 0880 clients	MPAG/Nepcho	104	C 71

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

Areleas Hertwork Setup	Filler States	
Miletary.		
keeping bever		
Version for Annu for an	0.01_27_00++-	
do-do		
Devenue		
Inter Apartment Terrar Add in	0.5	8. p.
Prior Contra Jonato 1 (1997-1997		w.u
(Marchashan dia Ada) (Marchashan dia Harda (Marchashan dia Harda) (Marchashan dia Sector (Hara, Marchashan dia Sec	To the design rate is consigned as more all of scherolic constants is designed for more any hostical difference (a) is inclusion. It is not the sound is the optimal distance of a state of the sound is the optimal distance of a state.	e doe na di na 18 a 190 a 200 a 19 an Conde VII a 1999 a 19 190 tale a di walio dy Charactella y Notes et
(Martakar Hardon) 2 Martakar Harde 2 Martakar Harde 2 Martakar Hardon 2 Martakar 2 Martakar 20 Martakar 2 Martakar	 To the decision was to consequent that many parts to the consequence of the	e doe mee al a se fa a filo in 2000. e na founder al na 1900 a fina 1900. estas a de realitador da estada a perfecta en est
(Marchanton Hardon) 2 Marchanton Hardon 2 Marchanton Harver 2 Marchanton Harver 2 Marchanton 2	 To the decision on the contributed for many solution of the decision of the decis	e staar mee uit ee 19 - 1110 in 2004. e na Kaandee uit ee 1904 op ee 1000 water ee de realite dy District alles werke to et al. Manganiser parameter jater aandee
(Marchanica - Bar And Charles and Harden Charles and Andreas Charles A	 To the devices were be contracted as more year. To the device on a contract to device the new set of the best devices at the device the best devices at the device to the contract of the device the device at the device to the device the device at the device to the device	en hoemaan di na 19 a 19 bi 20 bi 20 bi man Kanaka di na 19 bi 20 bi 20 bi balan an di matika di Chamanalika di kata da Matikaka di Matikaka di
(Marchaelen - Bardela 2 Marchaelen - Robert 2 Marchaelen - Robert 2 Marchaelen - Robert 2 Marchaelen - Robert 2011 (2010) 2011 (2010) 2011 (2010) 2011 (2010) 2011 (2010)	 To the devices were to consigned the merry of the devices one can be consigned from the constraint the devices the device of the	e doe na di na 19 4 19 5 19 0 10 10 10 00 na di Andrea di na 19 00 na 19 00 na di Andrea di Angli Danga di Angli Patro da na 1 Nationale di Angli Patro da na 1
(Marchaelen Hardelle 2 Marchaelen Hardel 2 Marchaelen Hardel 2 Marchaelen Hardel 2 Marchaelen Hardel 2 Marchaelen 2 March	 To the denominant is contributed from the contributed from	e nice na ul na 19 4 110 in 2004. e na foca de vil na 1904 a na 1905 volar a de velle de la restalación de la de la restalación de la de la restalación de la de
(Marchanica - Bardel Adul) 2 Marchanis - Marcha 2 Marchanis - Marcha 2 Marchanis - Marcha 2 Marchanis - Marchan 2 Marchanis - Marchan 2 Marchanis - Marchan 2 Marchanis - Marchan 2 Marchan - Marchan 2 March	To the devices we do contract the merity of the test of tes	e Norman di su 19 4 110 in 2004. r un Condex di su 19 4 10 10 in 2004. subar auto-maille dege (Contra subar auto-dege (Contra subar auto-dege)
(Marchanica - Bar Ashi 2 Marchanis - Marchan 2	To the device year is contributed as more than the contributed contributed in the contributed of the result of the contributed in the contribut	e i General VII na 19 a 19 bi 2004. In de l'Andrée VII na 19 20 de la 19 20 International de la 19 20
(Marchanica - Bar And Charles and Barden Charles and Charles Charles and Charles	To the devices you be contributed as more that the contributed by the market of the the contributed by the c	e doe na ul na 19 a 19 a 19 de Jose na e doe na de valla de la resulta a de valla de la resulta de la resulta de la resulta de l
(Marchanica - Bar John) (Marchanica - Bar Harder (Marchanica - Barder (Marchanich - Barder (Marchanica -	To the devices you be contributed to many soft of the test of t	e doe mar of no 19 a 19 b Alexa non doe doe of the 19 b Alexa take of the well-off the second off proceedings proceedings (D

4.5 Make a VoIP/VoLTE Phone Call

You can make phone calls over the VoIP/VoLTE via the Zyxel Device.

- 1 For VoIP, make sure a SIM card is installed on the Zyxel Device to have Internet access. For VoLTE (Vo3G), contact your ISP to make sure that your SIM card supports VoLTE (Vo3G).
- 2 Log into the Web Configurator.
- **3** Go to the **Configuration > Voice > Voice Mode** screen.
- 4 Select Enable in the Voice Mode screen to activate the VoIP/VoLTE service. Click Apply.

m	
New and American and American and American and American and American and American Am	
Vace Lenice a shranged, autem wit rebook.	

5 Connect an analog telephone to a **PHONE** port to make phone calls over the VoIP/VoLTE.

4.6 Configure a Fire wall Rule

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

- 1 Click Configuration > Security > Fire wall to open the General screen.
- 2 Select IPv4 Fne wall/ IPv6 Fne wall to enable the firewall, and click Apply.

Por Pressel		ana a la pa			
1.101.2014		Low.	Nodam (Roomaanso)	Uzi	
	.) richtweit	160		10	
	- WOR (0/241	8	0	0	
olu e					
I) LAN IS WAS ARRY S 2) WAS INCOMENDARY SHOWN 2) WAS IN THE SHOWN IN THE STREET	obere to officiented avec cours from a free company efficient to Might incoment pres in Am Point Symmetry	va astan tabi o Ito Asla o Ito Asla	nlaria Wing senitric inclusio	ca.	
	Ca	aciet.	Apply		

- 3 Open the Access Control screen to create a rule.
- 4 Click Add New ACL Rule to set up a rule.

- Filter Name: Enter a name to identify the firewall rule.
- Source IP Address: Enter the IP address of the computer that initializes traffic for the application or service.
- Select Destination IP Address: Enter the IP address of the computer to which traffic for the application or service is entering.
- Protocol: Select the protocol (TCP, UDP or ICMP) used to transport the packets.
- Custom Source Port: Enter the port number/range of the source that define the traffic type.
- Custom Destination Port: Enter the port number/range of the destination that define the traffic type.
- 5 Select Enable Rate Limit to activate the rules you created. Click OK.

	000 000 X.1 KUP	
-		
teet water wither	Sec 1 P Actives	
accessivation of		Josephores.
and dating of the call	special Packet	
New York Concerns		(heteloge)
f sta-	1.82	
Sector and	Special Sector	
Nation -	AL.	
Galer Parate	3.04	
Agendicionalen.	19.1	
1	Access	
	Mr.: 6 08	
No. A local distance of the		
	i (teleficier Second	16990
hi sekki ka s	a Subburba	

4.7 Configure MAC Filter

You can block certain web features and specific website addresses.

- 1 Go to the Configuration > Security > MAC Filter screen. Click Add New Rule.
- 2 Type the Host Name and the corresponding MAC Address that you want to block in the MAC Filter screen.
- 3 Select the Active check box and click Apply.

		MAC	2 Filter				
ender wel Besondodit etchologie etchologie ender all genore well	e des addres Seconder 1	n di kisi cin Vati alavid	el inscuri Succession	na ha chudh Rhach canai	n outwool decod sure	terne folgeving Benthe Vereni	na <mark>hin P</mark> eri Nothe
encatena inte	★++++ <	6 6 06(\$.0	0 005	uption in a	2001. 1		
CALL SEPTICE COME	New Co	400				G	acht dans Lu
Sel Active Host New	er .			MAC Addre			Delete
1 🔳		27	142		25	121	n h
2 🛛				- 54	10		E E
No o Only devices lated here are gran	ned access to the	e newors miciel	A	upply			

4.8 Upgrade Firmware on the Zyxel Device

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

- 1 Download the firmware file at <u>www.zyxel.com</u> in a compressed file. Decompress the file.
- 2 Go to the Maintenance > Firm ware Upgrade screen.
- 3 Click Browse and select a .bin file to upload. Click Upload.

Firn	nware Upgrade
Remains a promitie is where you can appeare the d You can consticut the takes armous the form the	indice with newly weaved features by upper date the blest firmware. In the slop one watche of thy due on
Upgrade Firmware	
Rentere Octuel Self- gs Alter Finiwere Opgroep	7
Current Timwore Version: 2 00(ADM 7,1100	
Ne Poly	Laterate Light Date
Do Online Firmware Upgrode	
Check lot Lotest Percenter Now	

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

4.9 Back up a Configuration File

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

- 1 Go to the Maintenance > Backup/Restore screen.
- 2 Click **Backup** in the **Backup Configuration** section, and a configuration file will be saved to your computer.

Backup/Restore	
The constructive cover failing monotopic to book to be on your construction previous allings, you o book to be, for any number of the device book to it there a reliant order.	
Backup Configuration	
ediction de la la servicie de la configuration of sour systematic part computer	
Errivat	
Restore Configuration	
re colors a provincity star distantly ratios for in your system, prives to the location of the configuration fin and all k Upped	
Re Ports Arrew place	
Back to Factory Default Settings	
Click Seren to clean all user-entered configuration, nicrostaniand return to topromice but settings. After reporting, the	
Powerval webser 1234	
LAR Prederess will be 182-182 11	
neos sã bravara dobat satiog	
Waning, decrements are enternet cable connected to wire on well before writing.	
laon	

4.10 Restore Configuration

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

- 1 Go to the Maintenance > Backup/Restore screen.
- 2 Click **Browse** in **Restore Configuration** section, and select the configuration file that you want to upload. Click **Upload**.

Backup/Restore	
Too consuming commission of bodies is a criterio consumer of nation-previous-linger on a bodies is. The new new first criterio body to it factory online color	
Backup Contiguration	
: Seconds planets for a second construction of unersystem to your computer.	
Erztuar	
Restore Configuration	
 a make a providuary second spacing and as fits to you system, between to the location of the nonling antical fits ward shall. Up block 	
Re Pyth	
Back to Factory Default Settings	
ClickReter to deci bit user-entered configuration, notworkon and return to toprovi debut settings. After recenting, the	
Permand without 123+	
LAR Products will be ring ridd in 1	
u este est ha macht dalaut kontraj	
Warning, diagram moves the enternet cable concepted to whici on tabil perfore resulting.	
Tacer	

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

4.11 Connect to the Internet

This section gives you an example on how to connect to the Internet.

- 1 Insert the SIM Card into your Zyxel Device SIM slot. Make sure this SIM has an active data plan with your Internet Service Provider (ISP).
- 2 Connect your Zyxel Device to your computer, and log into the Web Configurator.
- 3 If your SIM has a PIN Code, enter this code in the Broardband > Cellular SIM screen.
- 4 Use the Home screen to check the Internet Status (IPv4) or Internet Status (IPv6). If it shows Connected this means your Internet connection is up.



4.12 Configure DHCP

You can enable the DHCP (Dynamic Host Configuration Protocol) in your Zyxel Device to assign IP addresses and DNS servers to systems that support DHCP client capability. DHCP allows clients to obtain TCP/IP configuration at start-up from a server.

The following figure shows how **Client A** uses DHCP to join the Zyxel Device's network. First Client A searches for an available DHCP, and sends a **DHCP Disc over** broadcast message asking for an IP address to connect to. Then the DHCP selects an IP address from its pool of IP addresses for Client A. The DHCP sends a **DHCP Offer** including the IP address selected and a lease time, which is the period of time Client A will be able to use this IP address, After Client A has received DHCP offers for an IP address, it chooses one and sends out a **DHCP Request** including the IP address it chose. Finally the DHCP confirms through a **DHCP Ack (Acknowledge)** message that the host can use the IP address for the previously specified lease time.



To configure the DHCP in your Zyxel Device:

- 1 Log into the Zyxel Device's Web Configurator.
- 2 Click Network Setting > Home Networking > IAN Setup.
- 3 Select Enable DHCP Server State.
- 4 Enter a range of addresses from which your DHCP will assign to devices in your network.

Note: Do not include the Zyxel Device's LAN IP address in your range of addresses.

5 Type the DHCP Server Lease Time, the period of time (in minutes) a device can use one of the IP addresses from the DHCP pool. The lease time helps recycle unused IP addresses so that other can use them again. Click Apply.

4.12.1 Add Devices to Your Static DHCP List

IP addresses from the DHCP pool can be reused after they have completed their lease time. Add your devices to your Static DHCP List so they have the same IP address everytime they connect to your network.

To add a device to your Static DHCP List:

- 1 Log into the Zyxel Device's Web Configurator.
- 2 Go to Network Setting > Home Networking > Static DHCP screen.

- 3 Click Static DHCPConfiguration in the Static DHCP Configuration screen.
- 4 Select Active and type the IP address you want to assign to your device.
- 5 Type the MAC Address of your device to which the LTE7460 assigns the IP address and click OK.

	Static DHCP Configuration	
Allon		
Group Home	Cefe(/1	
/* type	1994	
to investigate with	We want does not	
N/XC28detth		
P* General	(a) (a) (b)	

4.13 Configure Static Route for Routing to Another Network

In order to extend your Intranet and control traffic flowing directions, you may connect a router to the Zyxel Device's LAN. The router may be used to separate two area networks. This tutorial shows how to configure a static routing rule for two network routings.

In the following figure, router **R** is connected to the Zyxel Device's LAN. **R** connects to two networks, **N1** (192.168.1.x/24) and **N2** (192.168.10.x/24). If you want to send traffic from computer **A** (in **N1** network) to

computer **B** (in **N2** network), the traffic is sent to the Zyxel Device's WAN default gateway by default. In this case, **B** will never receive the traffic.



You need to specify a static routing rule on the Zyxel Device to specify **R** as the router in charge of forwarding traffic to **N2**. In this case, the Zyxel Device routes traffic from **A** to **R** and then **R** routes the traffic to **B**.



This tutorial uses the following example IP settings:

DEVICE/ COMPUTER	IP ADDRESS
The Zyxel Device's LAN	192.168.1.1
A	192.168.1.34
R's N1	192.168.1.253
R's N2	192.168.10.2
В	192.168.10.33

Table 12 IP Settings in this Tutorial



To configure a static route to route traffic from $\mathbf{N1}$ to $\mathbf{N2}$:

- 1 Log into the Zyxel Device's Web Configurator.
- 2 Go to Network Setting > Routing > Static Route screen.
- 3 Click Add New Static Route in the Static Route screen.
- 4 Configure the Static Route Setup screen using the following settings:
 - **4a** Type 192.168.10.2 and subnet mask 255.255.255.0 for the destination, N2.
 - 4b Type 192.168.1.253 (R's N1 address) in the Gateway IP Address field.
 - 4c Click OK.

Now **B** should be able to receive traffic from **A**. You may need to additionally configure **B**'s firewall settings to allow specific traffic to pass through.

	HUU	reere around n	0010	
Ashee				
15045 M3440	L			
Karr.	and .			34
David and Sections			-	
Industry of the second				
Die Golewiczi? Adolesi	-			
Care-roy P'Address	21			
(Selected)	Gelein			
laike				
to most report that Colore	avit Adamstration	io nato zario ien	ab state Day j	tutses.

4.14 Access the Zyxel Device Using DDNS

If you connect your Zyxel Device to the Internet and it uses a dynamic WAN IP address, it is inconvenient for you to manage the device from the Internet. The Zyxel Device's WAN IP address changes dynamically. Dynamic DNS (DDNS) allows you to access the Zyxel Device using a domain name.



To use this feature, you have to apply for DDNS service at www.dyndns.org.

This tutorial covers:

- Registering a DDNS Account on www.dyndns.org
- Configuring DDNS on Your Zyxel Device
- Testing the DDNS Setting

Note: If you have a private WAN IP address, then you cannot use DDNS.

4.14.1 Register a DDNS Account on www.dyndns.org

- 1 Open a browser and type http://www.dyndns.org.
- 2 Apply for a user account. This tutorial uses UserName1 and 12345 as the username and password.
- **3** Log into www.dyndns.org using your account.
- 4 Add a new DDNS host name. This tutorial uses the following settings as an example.
 - Hostname: zyxe lrouter.dyndns.org
 - Service Type: Host with IP address
 - IP Address: Enter the WAN IP address that your Zyxel Device is currently using. You can find the IP address on the Zyxel Device's Web Configurator **Home** page.
- 5 Then you will need to configure the same account and host name on the Zyxel Device later.

4.14.2 Configure DDNS on Your Zyxel Device

Configure the following settings in the Network Setting > DNS > Dynamic DNS screen.

- Select Enable Dynamic DNS.
- Select www.DynDNS.com as Service Provider.
- Type zyxelrouter.dyndns.org in the Host Name field.

• Type the user name (UserName1) and password (12345).

DHI Information		
ynamic DNS Solu;	ř.	
Commercial	😸 Distrie (-) Danie destrop die	radio alfred diazone
tévés forsís	unia Div SKA sem	3. • S
Read Contract		
University		
Fictorice:		
_ total 7/thereof	aken	
- Provide Contractions	Bar Steven and a strange of Mag	
ynamic ONS Statu	L	
ynamic ONS Statu	L	
ynamic DNS Statu Ver Aufter/ color Seul	E	
ynamic DNS Statu Var Artienicolor Secil	E .	
ynamic DNS Statu Ver Autori color Seul Lasi Godolad I me	E .	

Click Apply.

4.14.3 Test the DDNS Settings

Now you should be able to access the Zyxel Device from the Internet. To test this:

- 1 Open a web browser on the computer (using the IP address a.b.c.d) that is connected to the Internet.
- 2 Type http://zyxe houter.dyndns.org and press [Enter].
- 3 The Zyxel Device's login page should appear. You can then log into the Zyxel Device and manage it.



PART II Te c hnic a l Re fe re nc e

C HAPTER 5 Connection Status

5.1 Connection Status Overview

After you log into the Web Configurator, the **Connection Status** screen appears. You can configure basic Internet access and wireless settings in this screen. It also shows the network status of the Zyxel Device and computers/devices connected to it.

5.1.1 Connectivity

Use this screen to view the network connection status of the Zyxel Device and its clients.



Figure 44 Connectivity

Click the Arrow icon () to view IP addresses and MAC addresses of the wireless and wired devices connected to the Zyxel Device.

Figure 45 Connectivity: Connected Devices



You can change the icon and name of a connected device. Place your mouse within the device block, and an Edit icon () will appear. Click the Edit icon, and you'll see there are several icon choices for you to select. Enter a name in the **Device Name** field for a connected device. Click to enable () i **Internet Blocking** for a connected device. Click **Save** to save your changes.

Figure 46 Connectivity: Edit

<		~~ 0	Conne	ctivity		
	45-3)			?	And a second second	tore
and to	, j	181		R.,	inscend	Canael
	nikodown 1920-1931 (Al Iair 7 - 1937 (Al Iair Mir Filonda) Herret Blockh	- M 				

5.1.2 System Info

Use this screen to view the basic system information of the Zyxel Device.



System Info		
Vodel Harris	1197240-0448	
Terretorian Manifest	a my energia para	
Symmetric Liptics	Oldays 2 been 28 mins 11 and	
AA AMA Address	0404A:2000863.65	
1997 - N. W.	Connection down	×

Click the Arrow icon () to view more information on the status of your firewall and interfaces (WAN, LAN, and WLAN).
<		System Into		
Rock Name 25 Rocket Carlos 25 Series 72/02 31 Rocket Carlos 31 Norther Carlos 32	0536549604 0536549604 9072-006906 00(48862000) 00(48862000)	Interface Status		
WAN Information (No WAN)		WLANInformation	2.4698	55Hr
LAN Information		MAC Adotem	10:00:47:77:45:55	96000:37:57:36:55
NACOUR	112.165.1.1	Addt.m.	Ön.	0s
LOWINGE	255,255,255.0	500	ayout_abak	37201,4355,555
CVS ASSESS		schemmel	Auto(caneet 0)	auto(current of)
CALCULARIE ASSAG		scouty	WPA2-Personal	WPAS-Perronal
Associated a William Science		603.11 Mode	662.11b/g/n Mixed	662 11d/h/dd Mixed
SECK)	Server	24.25	Q.	Os.
ieoutty.				
CIWARI	Okobia			

Figure 48 System Info: Detailed Information

Each field is described in the following table.

LABEL	DESC RIPIIO N
Host Name	This field displays the Zyxel Device system name. It is used for identification.
Model Name	This shows the model number of your Zyxel Device.
Serial Number	This field displays the serial number of the Zyxel Device.
Firmware Version	This is the current version of the firmware inside the Zyxel Device.
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, when you restart it (Maintenance > Reboot), or when you reset it.
Interface Status	
Virtual ports are show	n here. You can see the ports in use and their transmission rate.
WAN Information (These fields display when you have a WAN connection.)	
Mode	This field displays the current mode of your Zyxel Device.
IP Address	This field displays the current IP address of the Zyxel Device in the WAN.
IP Subnet Mask	This field displays the current subnet mask in the WAN.
IPv6 Address	This field displays the current IPv6 address of the Zyxel Device in the WAN.
Primary DNS server	This field displays the first DNS server address assigned by the ISP.
Secondary DNS server	This field displays the second DNS server address assigned by the ISP.
Primary DNSv6 server	This field displays the first DNS server IPv6 address assigned by the ISP.

IABEL	DESC RIPIIO N
Secondary DNSv6 server	This field displays the second DNS server IPv6 address assigned by the ISP.
LAN Information	
IP Address	This is the current IP address of the Zyxel Device in the LAN.
Subnet Mask	This is the current subnet mask in the LAN.
DHCP	This field displays what DHCP services the Zyxel Device is providing to the LAN. The possible values are:
	Server - The Zyxel Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN.
	${f Re} {f la} {f y}$ - The Zyxel Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients.
	None - The Zyxel Device is not providing any DHCP services to the LAN.
Security	•
Firewall	This displays the firewall's current security level.
WLAN Information	
MAC Address	This shows the wireless adapter MAC (Media Access Control) Address of the wireless interface.
Status	This displays whether the WLAN is activated.
SSID	This is the descriptive name used to identify the Zyxel Device in a wireless LAN.
Channel	This is the channel number currently used by the wireless interface.
Security	This displays the type of security mode the wireless interface is using in the wireless LAN.
802.11 Mode	This displays the type of 802.11 mode the wireless interface is using in the wireless LAN.
WPS	This displays whether WPS is activated on the wireless interface.

 Table 13
 System Info: Detailed Information (continued)

5.1.3 Cellular Info

Use this screen to view the LTE connection details and LTE signal strength value that you can use as reference for positioning the Zyxel Device, as well as SIM card and module information.

Figure 49 Cellular Info

Cellular Info		
Mede	IP Passthrough Mode	
Status	Up	
IP Acidmete	10.204.58.202	
Primary ONE center	210.241.208.1,139.175.1.1	
Access lechnology	LTE	
Signal Strength	-71	5

Click the Arrow icon (>) to view the more information on the LTE connection.

<	< Cellular info		
wadels internation		Service information	
146	3518wit00000145	Carine of Period continger-	175
thesis By Vinter	AG1SEARARELAGEMAG	Ser.J	15.672
SIM Status		411	a
And Care Spin 1	Wollable	Der E Regime Dakte	56411660 ⁰ 23
	452011001081092	U. Arrente B. (1994)	29
cash.	84064018152706845379	Differentiation Mark	20
Park excercises of the second	3	001	3230
Conceptions of the Directory	- E	600 F	-01
le Potennosgn sicres		exci	.9
1 Francisco de Texador	Describe	- 6329	N-A
the shakes		1. Bull at	8-A
Collection	die .	tec.	57242
See Second and	Thursdaler	25	N/A
Springer	fen Festeau	4.94	N-A
P(2) 4	44401	- enc	8-8
		016	17

Figure 50 Cellular Info: Detailed Information

Table 14	Cellular Info: Detailed Information

IABEL	DESC RIPTIO N	
Module Information		
IMEI	This shows the International Mobile Equipment Identity of the Zyxel Device.	
Module SW Version	This shows the software version of the LTE module.	
SIM Status		
SIM Card Status	This displays the SIM card status:	
	\mathbf{None} - the Zyxel Device does not detect that there is a SIM card inserted.	
	Available - the SIM card could either have or doesn't have PIN code security.	
	\mathbf{Locked} - the SIM card has PIN code security, but you did not enter the PIN code yet.	
	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.	
	$\mathbf{Erro}\mathbf{r}$ - the Zyxel Device detected that the SIM card has errors.	
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 Protection	A PIN (Personal Identification Number) code is a key to a SIM card. Without the PIN code, you cannot use the SIM card.	
	Shows \mathbf{Enable} if the service provider requires you to enter a PIN to use the SIM card.	
	Shows Disa ble if the service provider lets you use the SIM without inputting a PIN.	
PIN Remaining Attempts	This is how many more times you can try to enter the PIN code before the ISP blocks your SIM card.	
IP Passthrough Sta	atus	

IABEL	DESC RIPTIO N	
IP Passthrough	This displays if IP Passthrough is enabled on the Zyxel Device.	
Enable	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.	
IP Passthrough	This displays the IP Passthrough mode.	
Mode	This displays Dynamic and the Zyxel Device will allow traffic to be forwarded to the first LAN computer requesting an IP address from the Zyxel Device.	
	This displays \mathbf{Fixed} and the Zyxel Device will allow traffic to be forwarded to a specific LAN computer on the local network of the Zyxel Device.	
Cellular Status		
Cellular Status	This displays the status of the cellular Internet connection.	
Data Roaming	This displays if data roaming is enabled on the Zyxel Device.	
	4G roaming is to use your Zyxel 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.	
Operator	This displays the name of the service provider.	
PLMN	This displays the PLMN number.	
Service Information		
Access Technology	This displays the type of the mobile network (such as LTE, UMTS, GSM) to which the Zyxel Device is connecting.	
Band	This displays the current LTE band of your Zyxel Device (WCDMA2100).	
RSSI	This displays the strength of the 3G/LTE signal strength between an associated cellular station and the Zyxel Device.	
Cell ID	This shows the cell ID, which is a unique number used to identify the Base Transceiver Station to which the Zyxel Device is connecting.	
	The value depends on the Current Access Technology:	
	 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. 	
	The value is '0' (zero) or 'N/A' if there is no network connection.	
Physical Cell ID	This shows the Physical Cell ID (PCI), which are queries and replies between the Zyxel Device and the mobile network it is connecting to. The normal range is 1 to 504.	
UL Bandwidth (MHz)	This shows the LTE channel bandwidth from device to base station. According to 3GPP specifications, the bandwidths defined by the standard are 1.4, 3, 5, 10, 15, and 20 MHz. The wider the bandwidth the higher the throughput.	
DL Bandwidth (MHz)	This shows the LTE channel bandwidth from base station to LTE device. According to 3GPP specifications, the bandwidths defined by the standard are 1.4, 3, 5, 10, 15, and 20 MHz. The wider the bandwidth the higher the throughput.	

Table 14 Cellular Info: Detailed Information

Table 14	Cellular Info: Detailed Information

IABEL	DESC RIPTIO N
RFCN	This displays the Radio Frequency Channel Number of DL carrier frequency used by the mobile network to which the Zyxel Device is connecting.
	The value depends on the Current Access Technology:
	• 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.
	The value is '0' (zero) or 'N/A' if there is no network connection.
RSRP	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.
	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.
	An undetectable signal is indicated by the lower limit, example -140 dBm.
	This parameter is for LTE only. The normal range is -30 to -140. The value is -140 if the Current Access Technology is not LTE. The value is 'N/A' if there is no network connection.
RSRQ	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.
	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.
	This parameter is for LTE only. The normal range is -30 to -240. The value is -240 if the Current Access Technology is not LTE. The value is 'N/A' if there is no network connection.
RSCP	This displays the Received Signal Code Power, which measures the power of channel used by the Zyxel Device.
	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.
	This parameter is for UMTS only. The normal range is -30 to -120. The value is -120 if the Current Access Technology is not UMTS. The value is 'N/A' if there is no network connection.
EcNo	This displays the ratio (in dB) of the received energy per chip and the interference level.
	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.
	This parameter is for UMTS only. The normal range is -30 to -240. The value is -240 if the Current Access Technology is not UMTS or there is no network connection.
TAC	This displays the Tracking Area Code (TAC), which is used to identify the country of a mobile subscriber.
	The physical cell ID of the connected E-UTRAN cell, is as specified in 3GPP-TS.36.101.
	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.
LAC	This displays the 2-octet Location Area Code (LAC), which is used to identify a location area within a PLMN.
	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].
	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.

IABEL	DESC RIPIIO N
RAC	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.
	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.
	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].
	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.
BSIC	The Base Station Identity Code (BSIC), which is a code used in GSM to uniquely identify a base station.
	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.
SINR	This displays the Signal to Interference plus Noise Ratio (SINR) in dB. This is also a measure of signal quality and used by the UE (User Equipment) to calculate the Channel Quality Indicator (CQI) that it reports to the network. A negative value means more noise than signal.
CQI	This displays the Channel Quality Indicator (CQI). It is an indicator carrying the information on how good/bad the communication channel quality is.
MCS	MCS stands for modulation coding scheme. The base station selects MCS based on current radio conditions. The higher the MCS the more bits can be transmitted per time unit.
RI	This displays the Rank Indication, one of the control information that a UE will report to eNodeB (Evolved Node-B) on either PUCCH (Physical Uplink Control Channel) or PUSCH (Physical Uplink Shared Channel) based on uplink scheduling.
PMI	This displays the Precoding Matrix Indicator (PMI).
	PMI is for transmission modes 4 (closed loop spatial multiplexing), 5 (multi-user MIMO), and 6 (closed loop spatial multiplexing using a single layer).
	PMI determines how cellular data are encoded for the antennas to improve downlink rate.

Table 14 Cellular Info: Detailed Information

5.1.4 WiFi Settings

Use this screen to enable or disable the main wireless network. When the switch turns blue (, the function is enabled. Otherwise, it's not. You can use this screen or the QR code on the upper right corner to check the SSIDs (WiFi network name) and passwords of the main wireless networks. If you want to show or hide your WiFi passwords, click the Eye icon ().





Click the Arrow icon () to configure the SSIDs and/or passwords for your main wireless networks. Click the Eye icon (**) to display the characters as you enter the WiFi Password.

Figure 52 WiFi Settings: Configuration



Each field is described in the following table.

Table 15	WiFi Settings: Configuration
----------	------------------------------

LABEL	DESC RIPTIO N	
2.4G / 5G WiFi	Click this switch to enable or disable the 2.4 GHz / 5 GHz wireless network. When the switch turns blue 🔁, the function is enabled. Otherwise, it's not.	
WiFi Name	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID.	
	Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.	
WiFi Password	If you selected Random Password , this field displays a pre-shared key generated by the Zyx Device.	
	If you did not select Random Password , you can manually type a pre-shared key from 8 to 64 case-sensitive keyboard characters.	
	Click the Eye icon to show or hide the password for your wireless network. When the Eye icon is slashed 🛐, you'll see the password in plain text. Otherwise, it's hidden.	
Random Password	Select this option to have the Zyxel Device automatically generate a password. The WiFi Password field will not be configurable when you select this option.	
Hide WiFi network name	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.	
	Note: Disable WPS in the Network Setting > Wire less > WPS screen to hide the SSID.	
Save	Click Save to save your changes.	

5.1.5 Guest WiFi Settings

Use this screen to enable or disable the guest wireless network. When the switch turns blue (,), the function is enabled. Otherwise, it's not. You can use this screen or the QR code on the upper right corner to check the SSIDs (WiFi network name) and passwords of the guest wireless networks. If you want to show or hide your WiFi passwords, click the Eye icon ().

Figure 53 Guest WiFi Settings



Click the Arrow icon () to configure the SSIDs and/or passwords for the guest wireless networks. Click the Eye icon () to display the characters as you enter the WiFi Password.



0G Wifi	•			5/5 WiFi	00	
الموري بشائل			WEIGHT	$(p_{1}, p_{2}, p_{3}) \in \mathcal{M}(\mathcal{M}_{1}, p_{3}, p_{3})$	1.00	18
		ø	3071Conference	and the second s		
neour				785	en.	
S Stark in Stream		🔄 🖬 🖬 mainte Process	ee			
🖩 138 Milahan 1378 🕕		E Gen A 11 PRA	(K. 54574) 🖳			
	es wiki Normani Neor Ot		es wiki 🛥 🕫	45 WiFi C/Lingurell Colorn	CS WIFI CS WIF	ACS WIFE CONTRACTOR OF A CONTRACT OF A CONTR

Each field is described in the following table.

LABEL	DESC RIPTIO N		
2.4G / 5G WiFi	Click this switch to enable or disable the 2.4 GHz / 5 GHz wireless network. When the switch turns blue [1] , the function is enabled. Otherwise, it's not.		
WiFi Name	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID.		
	Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.		
WiFi Password	If you selected Random Password , this field displays a pre-shared key generated by the Zyxel Device.		
	If you did not select Random Password , you can manually type a pre-shared key from 8 to 64 case-sensitive keyboard characters.		
	Click the Eye icon to show or hide the password for your wireless network. When the Eye icon is slashed 🛐, you'll see the password in plain text. Otherwise, it's hidden.		
Random Password	Select this option to have the Zyxel Device automatically generate a password. The WiFi Password field will not be configurable when you select this option.		
Hide WiFi network name	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.		
	Note: Disable WPS in the Network Setting > Wire less > WPS screen to hide the SSID.		
Save	Click Save to save your changes.		

5.1.6 LAN

Use this screen to view the LAN IP address, subnet mask, and DHCP settings of your Zyxel Device.

Figure 55 LAN		
LAN		
P Adv Av	192.148.1.1	
5.0004 (MOV)	255.255.255.0	
P.Alares Rorge	192,168,1.2 - 192,168,1.254	
0F12-		
lecte Inve	Idays Ohours Omins	>

Click the Arrow icon () to configure the LAN IP settings and DHCP setting for your Zyxel Device.

Figure 56 LAN Setup

		LAN	
	LAN Fiselup		P Addressing Values
Extern.	95 974 1	logisting f. Takes a	- 1/s
statel level	28 . 29 . 29 . 1	no sing - Pako sa	S. 100 (197) 198
		DHCP Server State	
	E CELLANDATION	1 deje v	tion d. shota
		Sava	

Each field is described in the following table.

able 17 Status Screen			
LABEL	DESC RIPTIO N		
LAN IP Setup			
IP Address	Enter the LAN IPv4 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 255.255.2. (factory default). Your Zyxel Device automatically computes the subnet mask based on IP Address you enter, so do not change this field unless you are instructed to do so.		

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.
IP Addressing Values	
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.
DHCP Server State	

LABEL	DESC RIPTIO N
DHCP Server Lease Time	This is the period of time DHCP-assigned addresses is used. DHCP automatically assigns IP addresses to clients when they log in. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses, for a period of time, which means that past addresses are "recycled" and made available for future reassignment to other systems.
Days/Hours/ Minutes	Enter the lease time of the DHCP server.
Save	Click Save to save your changes.

 Table 17
 Status Screen (continued)

C HAPTER 6 Broadband

6.1 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.



6.1.1 What You Can Do in this Chapter

- Use the **Broadband** screen to view a WAN interface. You can also configure the WAN settings on the Zyxel Device for Internet access (Section 6.2 on page 84).
- Use the **WAN Backup** screen to configure your Zyxel Device's WAN backup settings (Section 6.3 on page 89).
- Use the **Ethemet WAN** screen to convert LAN port number four as a WAN port or restore the Ethernet WAN port to a LAN port (Section 6.4 on page 90).
- Use the Cellular WAN screen to configure an LTE WAN connection (Section 6.5 on page 91).
- Use the Cellular SIM screen to enter the PIN of your SIM card (Section 6.6 on page 92).
- Use the **CellularBand** screen to view or edit an LTE WAN interface. You can also configure the WAN settings on the Zyxel Device for Internet access (Section 6.2 on page 84).
- Use the **Cellular PIMN** screen to display available Public Land Mobile Networks (Section 6.8 on page 94).

• Use the Cellular IP Passthrough screen to configure an LTE WAN connection (Section 6.9 on page 97). Table 18 WAN Setup Overview

LAYER-2 INTERFACE		INTERNET C O NNEC TIO N			
CONNECTION	DSLUNK TYPE	MODE	ENCAPSULATION	CONNECTION SETTINGS	
Ethernet	N/A	Routing	IPoE	WAN IPv4/IPv6 IP address, NAT, DNS server and routing feature.	

6.1.2 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.

6.1.3 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.

6.2 Broadband

Use this screen to change your Zyxel Device's Internet access settings. The summary table shows you the configured WAN services (connections) on the Zyxel Device. Use information provided by your ISP to configure WAN settings.

Click **Network Setting > Broadband** to access this screen.

Figure 58	Network Setting > Broadband
-----------	-----------------------------

					В	roadb	and					
Lipa	dbond (in 1	(Jost -	a Uneri	19.44 Tabler	tini ti	alyes an	Sec. or l	ano iCe	a en facen			
Ye	, concorte	Cie tre in	terner seit	ings of this cardo	e Conect	i configural	lari boʻda	Jocestul)	memet connec	tion.		
										1 1 1 1	illione Mari	a sa ta
4	None	Тура	Node	Incoprulation	002.1p	602.10	IGWP Procey	841	Defoult Crateway	1946	MID Procey	Nodity
Ť	Contact 1992	eni	Routing	t at	164	108	- M	29	- 24	- 19	-34	(2)
2	COMAN-	0.070	Reafing	10.05	11126	10/86	17	17	5.5	1.0	1.0	1.07

IABEL	DESC RIPTIO N			
#	This is the index number of the entry.			
Name	This is the service name of the connection.			
Туре	This shows whether it is a cellular or Ethernet connection.			
Mode	This shows the connection is in routing mode.			
Encapsulation	This is the method of encapsulation used by this connection.			
802.1p	This indicates the 802.1p priority level assigned to traffic sent through this connection. This displays N/A when there is no priority level assigned.			
802.1q	This indicates the VLAN ID number assigned to traffic sent through this connection. This displays N/A when there is no VLAN ID number assigned.			
IGMP Proxy	This shows whether the Zyxel Device act as an IGMP proxy on this connection.			
NAT	This shows whether NAT is activated or not for this connection.			
Default Gateway	This shows whether the Zyxel Device use the WAN interface of this connection as the system default gateway.			
IPv6	This shows whether IPv6 is activated or not for this connection. IPv6 is not available when the connection uses the bridging service.			
MLD Proxy	This shows whether Multicast Listener Discovery (MLD) is activated or not for this connection. MLD is not available when the connection uses the bridging service.			
Modify	Click the Edit or Modify icon to configure the WAN connection.			
	Click the Delete icon to remove the WAN connection.			

Table 19 Network Setting > Broadband

6.2.1 Add/Edit Internet Connection

Click the \mathbf{Edit} or \mathbf{Modify} icon to open the following screen. Use this screen to configure a WAN connection.

Gennell I Yeak I<	ξ	Edit	WAN Interface		
IP Address State of Thema area area area State of Thema area area State of Thema area <th>luma Ter Music Interneticien Internetic Histori</th> <th>General () Methodale</th> <th>nor ta Ror ta Ma</th> <th>VLAN () 3 · · · · · · · · · · · · · · · · · · ·</th> <th>(-0)</th>	luma Ter Music Interneticien Internetic Histori	General () Methodale	nor ta Ror ta Ma	VLAN () 3 · · · · · · · · · · · · · · · · · · ·	(-0)
DHOPO Options Proposed Options Proceeding Proceedin	 California # California # Anno California (California # California (California # California # Californi# Californi# California # California # Califo	IP Address Address Ann DNS Server Notectorstation (2014 CRI Address	awa Apple wa Schwał Octawał	Routing Feature	
IPve Routing Feature	Rogoni Option Topico () Ret (Splan) Topico () Splan () Splan () Splan () Splan () Splan () Splan () Splan () Splan () Splan ()	DHOPO Options	 Description Mark Rep Corps Part Corps Part Corps Part 	IPvé Address exclose Actor IPvé DNS Server Chi dis Adsoration Agresier in chi Adone	
Aliz Inay (Apple to Exclusion) (Apple to E	ALE Pears	Pos Buying Fealure	•		

Figure 59 Network Setting > Broadband > Add/Edit New WAN Interface

	Table 20	Network Setting >	> Broadband >	Add/Edit N	ew WAN Interface
--	----------	-------------------	---------------	------------	------------------

IABEL	DESC RIPTIO N
General	Click this switch to enable or disable the interface. When the switch goes to the right enabled , the function is enabled. Otherwise, it is not.
Name	This is the service name of the connection.
Туре	This shows the type of the connection the Zyxel Device is currently associated with.
Mode	This shows the connection is in Routing or Bridge mode. If the Zyxel Device is in routing mode, your ISP gives you one IP address only and you want multiple computers to share an Internet account.

LTE Series User's Guide

IABEL	DESC RIPTIO N
Encapsulation	This is the method of encapsulation used by this connection.
IPv4/IPv6 Mode	This shows IPv4 IPv6 DualStack .
	IPv4 IPv6 DualStack allows the Zyxel Device to run IPv4 and IPv6 at the same time.
VLAN	Click this switch to enable or disable VLAN on this WAN interface. When the switch goes to the right <i>i</i> , the function is enabled. Otherwise, it is not.
802.1p	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service.
	Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.
802.1q	Type the VLAN ID number (from 1 to 4094) for traffic through this connection.
MTU	
MTU	Enter the MTU (Maximum Transfer Unit) size for this traffic.
IP Address	
Obtain an IP Address Automatically	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you have a dynamic IP address.
Static IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter the static IP address provided by your ISP.
Subnet Mask	Enter the subnet mask provided by your ISP.
Gateway IP Address	Enter the gateway IP address provided by your ISP.
DNS Server	
	Select Obtain DNS Info Automatically if you want the Zyxel Device to use the DNS server addresses assigned by your ISP.
	Select Use Following Static DNS Address if you want the Zyxel Device to use the DNS server addresses you configure manually.
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.
Routing Feature	
NAT	Click this switch to activate or deactivate NAT on this connection. When the switch goes to the right <i>i</i> , the function is enabled. Otherwise, it is not.
IGMP Proxy	Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.
	Click this switch to have the Zyxel Device act as an IGMP proxy on this connection. When the switch goes to the right con , the function is enabled. Otherwise, it is not.
	This allows the Zyxel Device to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Apply as Default Gateway	Click this switch to have the Zyxel Device use the WAN interface of this connection as the system default gateway. When the switch goes to the right the function is enabled. Otherwise, it is not.

Table 20	Network Setting >	· Broadband >	Add/Fdit New	WAN Interface	(continued)
10010 20	rion work oonling -	biodabana -			

IABEL	DESC RIPIIO N			
Fullcone NAT	Click this switch to enable or disable fullcone NAT on this connection. When the switch goes to the right a , the function is enabled. Otherwise, it is not.			
	This field is available only when you activate NAT			
	In fullcone NAT, the Zyxel Device maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. The Zyxel Device also maps packets coming to that external IP address and port to the internal IP address and port.			
DHCPC Options				
Request Options	Select Option 43 to have the Zyxel Device automatically add vendor specific information in the DHCP packets to request the vendor specific options from the DHCP server.			
	Select Option 120 to have the Zyxel Device get the IP address or a fully-qualified domain name of SIP server from DHCP.			
	Select Option 121 to have the Zyxel Device push static routes to clients.			
Sent Options				
option 60	Select this and enter the device identity you want the Zyxel Device to add in the DHCP discovery packets that go to the DHCP server.			
Vendor ID	Enter the Vendor Class Identifier, such as the type of the hardware or firmware.			
option 61	Select this and enter any string that identifies the device.			
IAID	Enter the Identity Association Identifier (IAID) of the device, for example, the WAN connection index number.			
DUID	Enter the hardware type, a time value and the MAC address of the device.			
option 125	Select this to have the Zyxel Device automatically generate and add vendor specific parameters in the DHCP discovery packets that go to the DHCP server.			
IPv6 Address				
Obtain an IPv6 Address Automatically	Select Obtain an IPv6 Address Automatically if you want to have the Zyxel Device use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address.			
Static IPv6 Address	Select Static IPv6 Address if you have a fixed IPv6 address assigned by your ISP. When you select this, the following fields appear.			
IPv6 Address	Enter an IPv6 IP address that your ISP gave to you for this WAN interface.			
Prefix Length	Enter the address prefix length to specify how many most significant bits in an IPv6 address compose the network address.			
IPv6 Default Gateway	Enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your Zyxel Device's interface(s). The gateway helps forward packets to their destinations.			
IPv6 DNS Server				
Obtain IPv6 DNS Info Automatically	Select Obtain IPv6 DNS Info Automatically to have the Zyxel Device get the IPv6 DNS server addresses from the ISP automatically.			
Use Following Static IPv6 DNS Address	Select Use Following Static IPv6 DNS Address to have the Zyxel Device use the IPv6 DNS server addresses you configure manually.			
Primary DNS Server	Enter the first IPv6 DNS server address assigned by the ISP.			
Secondary DNS Server	Enter the second IPv6 DNS server address assigned by the ISP.			
IPv6 Routing Feat	ure			

Table 20 Network Setting > Broadband > Add/Edit New WAN Interface (continued)

IABEL	DESC RIPIIO N
MLD Proxy Enable	Select this check box/option to have the Zyxel Device act as an MLD proxy on this connection. This allows the Zyxel Device to get subscription information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Apply as Default Gateway	Select this option to have the Zyxel Device use the WAN interface of this connection as the system default gateway.
Cancel	Click Cancel to exit this screen without saving.
Apply	Click Apply to save your changes.

Table 20 Network Setting > Broadband > Add/Edit New WAN Interface (continued)

6.3 WAN Backup

Use this screen to configure your Zyxel Device's Internet settings if the wired connection is down. You can use an alternative network, and assign an IP address to verify the accessibility of the Internet and the time interval allowed between each connection check.

Click Network Setting > Broadband > WAN Backup to display the following screen.

	Broad	band	
WAN BOOKUD	There we call the o	N CARACTA CARTE	iani isali an 20
Manager Int MAN a second	o Antony, MASS Built op Antonias	eiller, diamieken spaar offer	é
APR Tex you Teacher			
Comp (et a)	Elas est		
Tra Dartinorior for . Sonreoßin Enleck	250000 (\$55	1.+1. and	3
	10		(00-s00 men)
Connection Checkshreival			

The following table describes the fields in this screen.

TODIE ZT INETWORK SETTING > DIOGODONO > WAIN DOCKUL	Table 21	Network Setting >	Broadband >	WAN Backup
---	----------	-------------------	-------------	------------

LABEL	DESC RIPIIO N
WAN Backup Enable	Select Enable to have the Zyxel Device use the cellular connection as your WAN or a backup when the wired WAN connection fails.
Primary WAN	This field displays the connection the Zyxel Device would use first when the wired WAN connection fails. You can choose Ethemet or Cellular as the primary WAN connection for your Zyxel Device.

LABEL	DESC RIPHO N
The Destination for Connection Check	Configure this field to test your Zyxel Device's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address).
	Note: If you activate either traffic redirect or dial backup, you must configure at least one IP address here. When using a WAN backup connection, the Zyxel Device periodically pings the addresses configured here and uses the other WAN backup connection (if configured) if there is no response.
Connection Check Interval	When the Zyxel Device is using a lower priority connection (usually a WAN backup connection), it periodically checks to whether or not it can use a higher priority connection. Type the number of seconds (30 recommended) for the Zyxel Device to wait between checks. Allow more time if your destination IP address handles lots of traffic.
Check Fail Limit	Type the number of times (2 recommended) that your Zyxel Device may ping the IP addresses configured in the WAN Backup Enable field without getting a response before switching to a WAN backup connection (or a different WAN backup connection).
Cancel	Click Cancel to exit this screen without saving.
Apply	Click Apply to save your changes.

Table 21 Network Setting > Broadband > WAN Backup (continued)

6.4 Ethernet WAN

Use this screen to have a LAN port act as an Ethernet WAN port. You can restore it back from a WAN port to a LAN port. Click the switch to set up the configuration. When the switch goes to the right, the LAN port acts as an Ethernet WAN port. Otherwise, the LAN port remains as a LAN port. The Ethernet WAN connection has priority over the DSL connection. Click **Apply** to save your changes back to the Zyxel Device.

Click Network Setting > Broadband > Ethemet WAN to display the following screen.

Figure 61 Network Setting > Broadband > Ethernet WAN

6.5 CellularWAN

Click **Network Setting > Broadband > Cellular WAN** to display the following screen. Use this screen to enable data roaming and network monitoring when the Zyxel Device cannot ping a base station.

Note: APN information can be obtained from the service provider.

Roaming charges may apply when **Data Roaming** is enabled.

Automatic APN Mode is not supported when operating in 3G only mode.

secondor -		
enna		
rhorand Solic of	blord	
nterno select Automotic	-Tolemalfreens	
aming		
4-9000 g		
E.		
mine of secondrey delay	when Data Koawing a chebled	
4 Settings		
Production and Providents	(a)	
1		
enone		giant
et al a state	(5)	(galars)
eter solar team	745	
in † ₁ 104	entre	
é –		

The following table describes the fields in this screen.

Table 22 Network Setting > Broadband > Cellular WAN

IABEL	DESC RIPHO N	
Antenna		
Antenna Select	Select between External or Internal Antenna for your Zyxel Device.	
Roaming		
Data Roaming	Click this to enable (
	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.	

IABEL	DESC RIPTIO N
APN Settings	
APN Manual Mode	Disable this to have the Zyxel Device configure the APN (Access Point Name) of an LTE network automatically. Otherwise, Click this to enable (
APN	This field allows you to display 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 allows you to display 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 allows you to set 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 .
PDP Type	Select $\mathbf{IPv4}$ if you want the Zyxel Device to run IPv4 (Internet Protocol version 4 addressing system) only.
	Select IPv4 / IPv6 if you want the Zyxel Device to run both IPv4 and IPv6 (Internet Protocol version 4 and 6 addressing system) at the same time.
Apply	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

 Table 22
 Network Setting > Broadband > Cellular WAN (continued)

6.6 Cellular SIM Configuration

Enter a PIN for your SIM card to prevent others from using it.

Entering the wrong PIN code 3 consecutive times locks the SIM card after which you need a PUK (Personal Unlocking Key) from the service provider to unlock it.

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

Figure 63	Network Setting >	Broadband >	Cellular SIM
ng uie 00	riorition John g	biodabana -	

PIN Management		
Nonector's		
τ _P .		Ø
	eteroprovens sing. I	
2004		
1) The PDH is purposed by	y marching the Topel Device	

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.

LABEL	DESC RIPIIO N	
PIN Manageme	PIN Management	
PIN Protection	A PIN (Personal Identification Number) code is a key to a SIM card. Without the PIN code, you cannot use the SIM card.	
	Click to enable () if the service provider requires you to enter a PIN to use the SIM card.	
	Click to disable if the service provider lets you use the SIM without inputting a PIN.	
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.	
Apply	Click Apply to save your changes.	
Cancel	Click Cancel to return to the previous screen without saving.	

Table 23 Network Setting > Broadband > Cellular SIM

6.7 Cellular Band Configuration

Either select Auto to have the Zyxel Device connect to an available network using the default settings on the SIM card or select the type of the network (4G, 3G, or 2G) to which you want the Zyxel Device to connect.

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

Figure 64	Network Setting >	Broadband >	Cellular Band
-----------	-------------------	-------------	---------------

acess Technology			
Detering waters Technology	Aim	T	
and Management			
energi Aleba anno Jon			

IABEL	DESC RIPTIO N	
Access Technology		
Preferred Access Technology	Select the type of the network $(4G, 3G, \text{ or } 2G)$ 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		
Band Auto Selection	Select the LTE bands to use for the Zyxel Device's WAN connection. Click to enable (automatic LTE frequency band selection as provided by your service provider. Otherwise, select disabled.	
Apply	Click this to save your changes.	
Cancel	Click this to exit this screen without saving.	

6.8 Cellular PIMN Configuration

Each service provider has its own unique Public Land Mobile Network (PLMN) number. Either select **PLMN Auto Selection** to have the Zyxel Device connect to the service provider using the default settings on the SIM card or manually view available PLMNs and select your service provider.

Click Network Setting > Broadband > Cellular PIMN. The screen appears as shown next.



Parth resiste provide car The Solel Sector Common and some your tradeback	b over unir Lw le live activates séden	Roale Leng Mobile In Roal der Groß Inersteil	meth (1944) is more the all set against the SM car	nar weed fund wats balaction to hove the manuality way to calcula (1909)
PLWN Management				
Fuch Arts Westin				
		Concel	Apply	

LTE Series User's Guide

94

LABEL	DESC RIPTIO N
PLMN Management	
PLMN Auto Selection	Click to enable (and have the Zyxel Device automatically connect to the first available mobile network.
	Select disabled 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.

Table 25	Network Setting >	Broadband > Cellular PLA	٨N
	Network Setting ~	DIOGUDUITU - CEIIUIUIT LI	/ II N

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

Figure 66	Network Setting >	Broadband >	Cellular PLMN >	Manual Scan Warning
-----------	-------------------	-------------	-----------------	---------------------



Click $\mathbf{Sc\,an}$ to check for available PLMNs in the area surrounding theZyxel Device, and then display them in the network list. Select from the network list and click \mathbf{Apply} .

n Managemeni Nahiriskesian M	0 12			
	Status	Nome	lypæ	PLMP
	Assistante	HT	itE	486.0
6	Consert	11 -	1055.2	2689
	Feibleden	19253	JP:575	46697
	/clase	Chunghwa	0.672	46692
102	Astributes	Guaghwa	105	4452
6	Lattice & deer	1316	111	16898
10	Forbiddon	1424	LTC.	46297
16	Feißicklon	466.00	GPR5	48600
	Figuradadee	est (G	ПF	466.20
	Louisideen	Ether	0558	- www.

Table 26 Network Setting > Broadband > Cellular PLMN > Manual Scan

LABEL	DESC RIPHO N
#	Click the radio button so the Zyxel Device connects to this ISP.
Status	This shows $\mathbf{Cune}\mathbf{nt}$ 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 $\mathbf{Available}$ to indicate an available ISP your Zyxel Device can connect to.
Name	This shows the ISP name.
Туре	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.

6.9 IP Passthrough

Enable **IP Passthrough** to allow Internet traffic to go to a LAN computer behind the Zyxel Device without going through NAT.

Click Network Setting > Broadband > IP Passthrough to display the following screen.

Note: This screen is not available when the fourth LAN port acts as an Ethernet WAN port. See Table 1 on page 16 for the feature differences of the Zyxel Devices.

Figure 68 Network Setting > Broadband > IP Passthrough

P Passthrough Managen	ient.		
1 posteriory, opt			
Paarteouph Mode	Tred		
-nothing to finished			
ante.			
honging the Presidential of	dings any other to actives orthop of closely	kwets	

Note: Changing the **IP Passthrough** settings may affect the network setting of client devices. After selecting to enable the following warning appears. Click **OK** to continue.

<	Warning
	Have to assonnet/connect the device or release/renew IF address after IF Fassthrough 's enabled/disabled.
	OK

Figure 69 Network Setting > Broadband > Cellular IP Passthrough > Enable Warning

The following table describes the fields in this screen.

Table 27 Network Setting > Broadband > IP Passthrough

LABEL	DESC RIPIIO N
IP Passthrough	Management
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.

IABEL	DESC RIPIIO N
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 Passthmugh 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 $\mathbf{Fixe} \mathbf{d}$ in the previous field.
Apply	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

 Table 27
 Network Setting > Broadband > IP Passthrough (continued)

C HA PTER 7 Wire le ss

7.1 Overview

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

7.1.1 What You Can Do in this Chapter

This section describes the Zyxel Device's **Wire less** 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 7.2 on page 100)
- Use the Guest/More AP screen to set up multiple wireless networks on your Zyxel Device (Section 7.3 on page 104).
- Use the **MAC Authentication** screen to allow or deny wireless clients based on their MAC addresses from connecting to the Zyxel Device (Section 7.5 on page 108).
- Use the **WPS** screen to enable or disable WPS, view or generate a security PIN (Personal Identification Number) (Section 7.6 on page 110).
- Use the **WMM** screen to enable WiFi MultiMedia (WMM) to ensure quality of service in WiFi networks for multimedia applications (Section 7.7 on page 112).
- Use the **O the rs** screen to configure WiFi advanced features, such as the RTS/CTS Threshold (Section 7.8 on page 113).
- Use the **WIAN Scheduler** screen to create rules to schedule the times to permit Internet traffic from each wireless network interfaces (Section 7.9 on page 115).
- Use the **Channel Status** screen to scan the number of accessing points and view the results(Section 7.10 on page 117).

7.1.2 What You Need to Know

Wire less 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 7.11 on page 118 for advanced technical information on WiFi networks.

7.2 General Settings

Use this screen to enable the Wireless LAN, enter the SSID and select the wireless security mode. We recommend that you select **More Secure** to enable **WPA2-PSK** data encryption.

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

Click Network Setting > Wire less to open the General screen.

Wholess Retwork :	Satep						
Barra		2,40,42					
(Section)							
Dared		failer :				Garan	
ferrights.		72,00					
Contra Palata au		the second					
Win Heiss Richard (Selence						
Selection of the	6	209-0002					
On them.		- 24					
E 107 0							
10 0 mm	Sq.						
The loss has all as	ordini -					Max	
Post for the filler Data for a more the sense (Delay Verbrace for Schim Generate and	ondin a unitar desclute fait al a		syde fan suit er s	endend the Back Main	ww. en.V.T	ulue Ulue	
Van bestern da er Den den er wer d une (Den Verbauer be Steller Ansenderen) alt det Alsen verb arter	onde a an de desche de take a Reseating Takes Generality Antis reflexagene fre		gara Dan sam on s nalg on to realist das se an realist das se an realist	underst na Bardina a Karana official Autor E Monarcian Marana fonomos	w #~V.5	ua ua	
Decide and decide of the Decidence of the new Other Sectors for Solar Counties of a Sector Sector Sector at the Sector Sector ACC	constru la sense dite indense dite inder at forwarden dite inder at forwarden at a sense regimente dite at the regimente dite at the	lass por la cott o des por la co des Jacobs Por des Jacobs Por Bino de der	ngen fan som en e relig er ter realen i der de af her rek frem i den er ter frem	emoral de Bastral e transmitte el Adria a de restantes a mara na Renances	₩ #n.v.1	u.a	
Dan bos har i da a Dan bos har i da a Dan bos a nave d Older Generale we Alta Santa Anter VI alta Santa Atta Atta Secol de Lovel	anda a an di des la fariada d Researches Tarles Researches Tarles Researches Tarles Researches Tarles	lana nay isang talang partiti a distang partiti a distang pang talang sagang Barang sagang	spore That source of the religion for the measure that can be the relation theory to state the form	enderst na Rastadi a e berezentek et Auto ko e talen da talen ko a hate na Konosene	**** *****	u.a	
Dan Joo Barrisland Dan Joo Barrisland (Den Joo Barrisland (Den Joo Barrisland) (Den Joo Barrisland (Den Joo Barrisland) (Den Joo Lovel)	ondo a un di descis de tales Researce de tales de tales de secondo restantes de secondo	lana a la cara di se per la c di se se se se di se se se se se di se se se se se se se di se se se se se se se se se di se se di se	gara Barrisan on A ndgo n to materia dariga an mandu dariga an mandu an	enderal no Banara i a consecutiva d'Adrian e devena devena de al mara na devena d	www. dow VI To jakaya kowan jakaya kowan jakaya kowan	U.a U.a	
Dani bos har i da a Dani bos an ever d Dani bos de ante d Dalar Contrata i la Stato Attato Attato Securito Lovel	ondin an ann dh' colmando. Ann anto a fean-antoire Tua Ann ann Tua agus an Ann an Tua agus an Ann	lang partition distribution distribution distribution distribution distribution distribution distribution	egoro Patri sono en la redigi en llo "enclara l device de la real cita llocare de la casa real de llocare	emderski ste Bastivick o te berezenski et Austrike a da orođenosti u majna na Romonanja	www. Bootton Danystroom (Fromes - Hell	U.a U.a	
Van bos hor i dan Dan bos new i Unite Vashara i ke Shine Gaarderen al deglasse i mass agen securitie Lovel	ondon an ann 201 Anna Chuilte an Anna Anna Chuilte Anna Anna Anna Anna Anna Anna Anna Anna Anna	lana na la ant di di anger (la ci di di anger	gan Dar van en e religier is name de orden en en e rec	ombrid in Bashkin Kongoridh di Abilin Solar tabun Shara na tararan Shara na tararan	www. energy to Data to com (Norman - com	u.a	
Decision model of a second sec	ondos a una dis electro de talo d ferenciales de talo d ferenciales de talo españa de talonas españa de talonas españa de talonas	lana na kaon dia pamba na dia pamba na dia pamba na dia pamba dia pamba dia pamba dia pamba dia pamba	ngen Dat von en en religion ter nomen dat da affrestelle dat da strandet nomen energi	enderal de Bastal e e Recenceration d'Antible E de rectores al rectores d'Antible al rectores d'Antible al rectores d'Antible	www. Worst T Days by on Days to out	U.a	
Data basi keun daran Data data senara di Yesi Utaka Nashara Keu Yakim Nashara Keu Yakim Nashara Keu Atta Keun Kin Lawal		lana positiva de de caracterita de de caracterita de de caracterita de de caracterita de de caracterita de de de caracterita de de de de caracterita de de de de de caracterita de de de de de de caracterita de de de de de de de de de de de de de d	agen Patrices en la religio de l'estre de la caracteria estre de la caracteria estre de la caracteria estre de la caracteria estre de la caracteria estre estre de la caracteria estre	endersi de Bastrid d terrerezité d'Adrik a de recentes a naga na Recentes a naga na Recentes	www. Bootton Dany toose Diaman too	U.a	
Van besiter i den Van besiter i den Van besiter i ver d Uten Van en ver d State Van en ver State Van en ver State Van Atten Recedie Lovel	ondin o uno di classica di cale a formatione di contra contra di contra contra di contra contra di contra contra di contra contra di contra di contra			n molecul est. Els a social a la conservation est Autor las la conservation est la marte esta fonccione p la marte esta fonccione p	www. Bootton Dawy Second Dawy Second Second Dawy Second Dawy Secon	0.a	
Van boo hor i dan Tour don a wor i Van Valen van de Older Valen van Alter Autor Attri Stan de Kovel				ondered to Basis Mile Consecutive Constants States on Networks	with Boo VI 5 Johan Jackson Ji Come - Land Boo - Land	0.a 0.a	
The balance days Decision and the Control of the second Children Control of the States Attraction of Attraction Second the Level	undin a un di desche de la si e leste de la si e regione de la si regione de la si leste de la si leste de la si leste de la si			nachrál na Bastrál a Isteración d'Atalia Starochartoru antes na fonorana Ingel	www. Wearston (Answer and (Answer and (Ans	0.a	

Figure 70 Network Setting > Wireless > General

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

LABEL	DESC RIPTIO N	
WiFi 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.	
WiFi	Click Enable to enable the wireless LAN in this field.	
Channel	Use $Auto$ to have the Zyxel Device automatically determine a channel to use.	

LABEL	DESC RIPTIO N
Bandwidth	Select whether the Zyxel Device uses a WiFi channel width of 20MHz, 40MHz or 20/40MHz.
	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.
	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.
	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.
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.
WiFi Network Sett	ings
WiFi Network Name	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.
	Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.
Max Clients	Specify the maximum number of clients that can connect to this network at the same time.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
	This check box is grayed out if the WPS function is enabled in the $Ne two tk > Wire less > WPS$ screen.
Multicast Forwarding	Select this check box to allow the Zyxel Device to convert wireless multicast traffic into wireless unicast traffic.
Max. Upstream Bandwidth	Specify the maximum rate for upstream wireless traffic to the WAN from this WLAN in kilobits per second (Kbps).
Max. Downstream Bandwidth	Specify the maximum rate for downstream wireless traffic to this WLAN from the WAN in kilobits per second (Kbps).
BSSID	This shows the MAC address of the wireless interface on the Zyxel Device when wireless LAN is enabled.
Security Level	
Security Mode	Select More Secure (WPA2-PSK) to add security on this WiFi network. The WiFi clients which want to associate to this network must have the same WiFi security settings as the Zyxel Device. When you select to use a security, additional options appears in this screen.
	Or you can select No Security to allow any client to associate with this network without any data encryption or authentication.
	See the following sections for more details about this field.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

Table 28 Network Setting > Wireless > General (continued)

7.2.1 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.





Table 29 Wireless > General: No Security

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

7.2.2 More Secure (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. Using a Pre-Shared Key (PSK), both the Zyxel Device and the connecting client share a common password in order to validate the connection.

Click Network Setting > Wireless to display the General screen. Select More Secure as the security level. WPA2-PSK is the default Security Mode.

Figure 72	Wireless >	General:	More Secure:	WPA2-PSK
-----------	------------	----------	--------------	----------

lecurity Leve	el No Secur	ttγ	More Sparre (Recommended)
	Security Mode	WPA2 DSK	-
	🔽 Ovierale pasword of	rematically	
	Enter 5-63 ASCII chorocter	n or 64 hexadecimal digits (1947, 1949).	
	Permente		۵
	Strength	modion	
	- ` —		
	energip Hom	Acc	-
	Tim er	2400	ne:

The following table describes the labels in this screen.

Table 30 Wireless > General: More Secure: WPA2-PSK

IABEL	DESC RIPTIO N
Security Level	Select More Secure to enable WPA2-PSK data encryption.
Security Mode	WPA2-PSK is the default security mode.

LTE Series User's Guide

LABEL	DESC RIPIIO N
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	Select Generate password automatically or enter a Password.
	The password has two uses.
	 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.
	Note: Enter 8-63 ASCII characters only. 64 hexadecimal characters are not accepted for WPS.
	Click the Eye icon to show or hide the password for your wireless network. When the Eye icon is slashed 🞆, you'll see the password in plain text. Otherwise, it's hidden.
more	Click this 🚹 to show more fields in this section. Click this 🐂 to hide them.
Encryption	AES is the default data encryption type, which uses a 128-bit key.
Timer	This is the rate at which the RADIUS server sends a new group key out to all clients.

Table 30 Wireless > General: More Secure: WPA2-PSK (continued)

7.3 Guest/More AP

Use this screen to configure a guest wireless network that allows access to the Internet through the Zyxel Device. Click **Network Setting > Wireless > Guest/More AP**. The screen appears as shown. This allows you to use one access point to provide several BSSs simultaneously. You can then assign varying security types to different SSIDs. Wireless clients can use different SSIDs to associate with the same access point. **Figure 73** Network Setting > Wireless > Guest/More AP

		WIF		
General Gu	nt Mans AB: 1742 X	Paristo, 075	(9/9) (01at /014	Colsebile 3
Fairmodon o Istel (Freed	cen proble up to 4 Win Act to start the Shal Dir	instaady to work stitte 5. and 8th Will setwork	, sano fire, Araunio na Ientres	re and a security
+	1	2	2	
No.	Ŷ	Ŧ	ίφ.	
380	General Strange and	Sud States 1	Trend States and St.	
Security	W140/Hendrol	WPASTerond	MTAG/THLODO	
Coort WLAS	*******	eren lant	*******	
Notiv	12	Z	<u>12</u>	

IABEL	DESC RIPTIO N
#	This is the index number of each SSID profile.
Status	This shows whether the SSID profile is active (a yellow bulb) or not (a gray bulb).
SSID	An SSID profile is the set of parameters relating to one of the Zyxel Device's BSSs. The SSID (Service Set IDentifier) identifies the Service Set with which a wireless device is associated. You can configure up to four SSIDs to enable multiple BSSs (Basic Service Sets) on the Zyxel Device. This field displays the name of the wireless profile on the network. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
Security	This field indicates the security mode of the SSID profile.
Guest WLAN	This field shows whether the SSID profile is an external or home guest.
Modify	Click Modify to change the SSID profile.

Table 31 Guest/More APNetwork Setting > Wireless >

7.4 More APEdit

Use this screen to create a guest wireless network and configure its security settings. Click the **Modify** icon in the **More AP** screen. The following screen displays. Click **Network Setting** > **Wire less** > **More AP Edit.**

	More AP Edit	
in the set of protect the set	a from uniquitariated access or damager via w	was helped to head a whereas helpeds normal
of above structure (200) so a	serves the wheles security	
Hindens Network Service		
Witness		
Security Level	- and	
wheel resident survey	Line sale place	
Dyamm		
The second second		
And and a second second	Telephone Concert	
The statement descents		1
Nex Obversteam		
sanateidet		tage .
-C18		
 Max Doursewer Scrawler I Isaa, spinkan (bounded) Ding Max, spinkan (bounded) 	 The field allows you to configure the matery, in standardon is enjoy, the device set the value neuro conductant value; 	un concreter of YAAN to Inte SEC. La outerfactioney a vitalass partementa.
- and a second s	- the second	
and realized		
and survey and survey		
and the name and rate support the first support		
ander Salle Taller Hell Saller Taller Heller Saller Taller Heller Saller Taller Heller		
anne 1990 Haarine 1990 Folde Aadree 1990 Folde Antonie 1990 Folde Antonie		
and and an		
and and an		
and and some order and Andreas and the Andreas and the Andreas and Andreas becaulty textel		Mare Securit (Reconstruction)
tana tana tanàn amin' nan-kaonen amin' aona amin' aona aona aona aona aona aona aona aona		Mare Secont Become and C
and and a second		Mar Jaco Berneredit (
anne Salat saarine Deitor saar Aaaree Secondry Sevel Secondry Sevel	Windowsky	Mare Sear Proceedings
Second Statement Second Statement Statement Statement Second Statement Second Statement Sec		stars Second
Second Se		Mart Seart (Reconcented)
Second Se		Mare Sear Processed (
Second Statement Second Statement Statement Statement Statement	Vitedorfic Vitedorfic Transfer Transfer Transfer	Marr Sour Merr Sour Merr Sour
Second Se		Marrison Marrison Marrison
teres Secondary Adapter Decor solar Adapter Secondary Level Teres P Adapter Percently Level Decondary Level	Wheth-face Wheth-	Her Star Brownstell

Figure 74 Network Setting > Wireless > More AP Edit

Table 32 Network Setting > Wireless > More AP Edit

IABEL	DESC RIPHO N	
WiFi Network Setup		
WiFi	Click Enable to enable the wireless LAN in this field.	
Security Level		

LTE Series User's Guide

IABEL	DESC RIPTIO N
WiFi Network Name	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.
	Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
	This check box is grayed out if the WPS function is enabled in the Network $>$ Wire less $>$ WPS screen.
Guest WLAN	Select the check box to enable Guest WLAN.
Access Scenario	If you select Home Guest, clients connecting to the same SSID can communicate with each other directly.
	If you select External Guest, clients are blocked from connecting to each other directly.
Max. Upstream Bandwidth	Specify the maximum rate for upstream wireless traffic to the WAN from this WLAN in kilobits per second (Kbps).
Max. downstream Bandwidth	Specify the maximum rate for downstream wireless traffic to this WLAN from the WAN in kilobits per second (Kbps).
BSSID	This shows the MAC address of the wireless interface on the Zyxel Device when wireless LAN is enabled.
BBSID Subnet	Select Enable to create an independent subnet for the SSID, which is separated from the LAN subnet(s).
DHCP Start Address	Enter the first of the contiguous addresses in the IP address pool for the SSID subnet. The Zyxel Device assigns IP addresses from this DHCP pool to wireless clients connecting to the SSID.
DHCP End Address	Enter the last of the contiguous addresses in the IP address pool for the SSID subnet.
SSID Subnet Mask	Enter the subnet mask of the Zyxel Device for the SSID subnet.
LAN IP Address	Enter the IP address of the Zyxel Device for the Guest SSID.
Security Level	
Security Mode	Select More Secure or WPA2-PSK to add security on this WiFi network. The WiFi clients which want to associate to this network must have the same WiFi security settings as the Zyxel Device. When you select to use a security, additional options appears in this screen.
	Or you can select No Security to allow any client to associate with this network without any data encryption or authentication.
	See the following sections for more details about this field.
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.

Table 32 Network Setting > Wireless > More AP Edit (continued)

LABEL	DESC RIPIIO N
Password	Select Generate password automatically or enter a Password.
	The password has two uses.
	 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.
	Note: Enter 8-63 ASCII characters only. 64 hexadecimal characters are not accepted for WPS.
	Click the Eye icon to show or hide the password for your wireless network. When the Eye icon is slashed j, you'll see the password in plain text. Otherwise, it's hidden.
more	Click this 🛧 to show more fields in this section. Click this 🐜 to hide them.
Encryption	AES is the default data encryption type, which uses a 128-bit key.
Timer	This is the rate at which the RADIUS server sends a new group key out to all clients.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

Table 32 Network Setting > Wireless > More AP Edit (continued)

7.5 MAC Authentication

Use this screen to give exclusive access to specific devices (Allow) or exclude specific devices from accessing the Zyxel Device (Deny), based on the MAC address of each device. Every Ethernet device has a unique factory-assigned MAC (Media Access Control) address, which 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 you want to allow/deny to configure this screen.
Use this screen to view your Zyxel Device's MAC filter settings and add new MAC filter rules. Click **Network Setting > Wire less > MAC Authentication**. The screen appears as shown.



1-001	-	
dete 🗆 deny 🖨 Maxi		
		🛨 Aldrice MAG police
WAC Address		Wedly
	MAC Address	MAC Addies

The following table describes the labels in this screen.

Table 33	Network Setting>	Wireless >	MAC	Authentication
----------	------------------	------------	-----	----------------

LABEL	DESC RIPTIO N
General	
SSID	Select the SSID for which you want to configure MAC filter settings.
MAC Restrict Mode	Define the filter action for the list of MAC addresses in the MAC Address table. Select Disa ble to turn off MAC filtering. Select Deny to block access to the Zyxel Device. MAC addresses not listed will be allowed to access the Zyxel Device. Select Allow to permit access to the Zyxel Device. MAC addresses not listed will be denied access to the Zyxel Device.
MAC address List	

IABEL	DESC RIPTIO N		
Add new MAC	This field is available when you select Deny or Allow in the MAC Restrict Mode field.		
address	Click this if you want to add a new MAC address entry to the MAC filter list below.		
	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.		
	Figure 76 Add New MAC Address		
	Add MAC address to list		
	To add a device, please enter device's MAC address		
#	This is the index number of the entry.		
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.		

Table 33 Network Setting> Wireless > MAC Authentication (continued)

7.6 WPS

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

WiFi Protected Setup (WPS) allows you to quickly set up a wireless 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. Your devices must support WPS to use this feature. We recommend using Push Button Configuration (**PBC**) if your device supports it. See Section 7.11.7.3 on page 126 for more information about WPS.

- Note: The Zyxel Device applies the security settings of the main SSID (SSID1) profile to the WPS wireless connection(see Section 7.2.2 on page 103).
- Note: The WPS switch is unavailable if the wireless LAN is disabled. If WPS is enabled, UPnP will automatically be turned on.

Click **Network Setting > Wire less > 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.





The following table describes the labels in this screen.

Table 34	Network Setting > W	vireless > '	WPS
	NOR JOINING - M		1113

LABEL	DESC RIPIIO N
General	
WPS	Click to enable () and have the Zyxel Device activate WPS. Otherwise, it is disabled.
Add a new device	with WPS Method
Method 1 PBC	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 PIN	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.

IABEL	DESC RIPIIO N
Register	Enter the PIN of the device that you are setting up a WPS connection with and click $\operatorname{Re} g$ ister 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.
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	The default WPS status is configured.
Configuration	Click this button to remove all configured WiFi and WiFi security settings for WPS connections on the Zyxel Device.
Generate New PIN	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.

Table 34 Network Setting > Wireless > WPS (continued)

7.7 WMM

Use this screen to enable WiFi MultiMedia (WMM) and WMM Automatic Power Save (APSD) in wireless networks for multimedia applications. WMM enhances data transmission quality, while APSD improves power management of wireless clients. This allows delay-sensitive applications, such as voice and videos, to run more smoothly.

Click Network Setting > Wire less > WMM to display the following screen.





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

The following table describes the labels in this screen.

IABEL	DESC RIPHO N
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 > O thers 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
Canaal	
Cuncer	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

Table 35 Network Setting > Wireless > WMM

7.8 Others Screen

Use this screen to configure advanced wireless settings, such as additional security settings, power saving, and data transmission settings. Click **Ne twork Setting > Wire less > O the rs**. The screen appears as shown.

See Section 7.11.2 on page 120 for detailed definitions of the terms listed here.

move to the work of a	1307		
Hoge challer freehold	3346		
e dest provine	1.056	÷	
Second Interval	(199)		
20Williago	1		
radio e procim	and simply in taking		
502.77 Protociau I	Aciu	÷	
m. and in	and generation of the second s		
Professie direct og ettert: Fruittill	Coocce	÷.	

Figure 79 Network Setting > Wireless > Others

The following table describes the labels in this screen.

Table 36	Network Setting > Wireless > Others
----------	-------------------------------------

IABEL	DESC RIPIIO N
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake.
	Enter a value between 0 and 2347.
Fragmentation Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2346.
Output Power	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% .
Beacon Interval	When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again.
	The interval tells receiving devices on the network how long they can wait in low power mode before waking up to handle the beacon. This value can be set from 50ms to 1000ms. A high value helps save current consumption of the access point.
DTIM Interval	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.
802.11 Mode	For 2.4GHz frequency WLAN devices:
	 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.
	For 5GHz frequency WLAN devices:
	 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	Enabling this feature can help prevent collisions in mixed-mode networks (networks with both IEEE 802.11b and IEEE 802.11g traffic).
	Select $Auto$ to have the wireless devices transmit data after a RTS/CTS handshake. This helps improve IEEE 802.11g performance.
	Select \mathbf{O} ff to disable 802.11 protection. The transmission rate of your Zyxel Device might be reduced in a mixed-mode network.
	This field displays Off and is not configurable when you set 802.11 Mode to 802.11b Only.

LTE Series User's Guide

LABEL	DESC RIPIIO N
Preamble	Select a preamble type from the drop-down list box. Choices are Long or Short . See Section 7.11.6 on page 123 for more information.
	This field is configurable only when you set 802.11 Mode to 802.11b.
Protected Management Frames	WiFi with Protected Management Frames (PMF) provides protection for unicast and multicast management action frames. Unicast management action frames are protected from both eavesdropping and forging, and multicast management action frames are protected from forging. Select Capable if the WiFi client supports PMF, then the management frames will be encrypted. Select Required to force the WiFi client to support PMF; otherwise the authentication cannot be performed by the Zyxel Device. Otherwise, select Disable d.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

Table 36 Network Setting > Wireless > Others (continued)

7.9 WIAN Scheduler

Use the **WIAN Scheduler** screen to create rules to schedule the times to permit Internet traffic from each wireless network interfaces. Select a specific time and day of a week for scheduling. You can also create a rule to automatically switch off all the WLAN together.

```
Click Ne two rk Setting > Wire less > WIAN Scheduler.
```

Figure 80 Network Setting > Wireless > WLAN Scheduler

				WiFi			
100 M	i (Madading)	ann stra	w Pro	WINHScher	1161		
MLA) Guild Gerli	Scheoolich olichai ye Maxee carloo - Mari Wolfo karanaci olid	ar le se null ri ler al lina pixed "activitti null-activ er le cullo meticulty sell	ille hemioest V All persistential chief fait benefi	Adhrofson Cole of check Athlogenes	neloca isr.		
Filst v							
Source	Tot no sea 1	the stars you do not a	de saterraa	The Borth	100% M		
rit Alt	When the second	07					
							1.11 West 10
- 34	Ad +4	Lotione	590	Dav	Tre	Description	Nocity
			Conce)		Apply.		

The following table describes the labels in this screen.

Table 37 Network Setting > Wireless > WLAN Scheduler

IABEL	DESC RIPTIO N
WLAN Scheduler Access	Click this switch to enable the WLAN scheduler function. This serves as the main switch to allow the individual rules to function. When the switch turns blue 2, the function is enabled. Otherwise, it's not.
Add New Rule	Click this to configure a new WLAN scheduler rule.
#	This is the index number of the entry.

LTE Series User's Guide

LABEL	DESC RIPTIO N		
Active	Click the check box to enable individual rules.		
	Note: Make sure to enable the WIAN SchedulerAccess switch for the individual rules to work.		
Rule Name	This field displays the name of the rule.		
SSID	This is the descriptive name used to identify the wireless network interface that this rule applies to. Will show AILWIAN if you select All wire less networks in the Add New Rule screen.		
Day	This field displays the day(s) of the week that you wish to apply this rule.		
Time	This field displays the time of the day that you wish to apply this rule.		
Description	This field shows a description of the rule, usually to help identify it.		
Modify	Click the Edit icon to configure the rule.		
	Click the Delete icon to remove the rule.		

Table 37 Network Setting > Wireless > WLAN Scheduler (continued)

Note: If you enable a rule for a specific SSID, you will not be able to connect to other wireless networks.

7.9.1 Add/Edit Rules

Click **Add New Rule** in the **WIAN Scheduler** screen, or click the **Edit** icon next to a scheduling rule, and the following screen displays.

Use this screen to create a scheduling rule to permit Internet traffic from each wireless network interface.

	Add New Rule						
Activ							
640	APWIC (White He	8					
Fully Highline							
(grain)							
@heres Select data and then for turned on	rier-of you want the specified WPI network will be dutance	fratty					
Qinena Select data and the in tured on	renatives want the specified With retwark will be subarro	fcaty Set Sur					
Break Select data and the in turned on The Decent Coulifornia	renotiyou ware the specified WP relevant will be automa	faats Sat San					
Qrease Select data and then to bared at. Dis Decent Data Konge Contation	renoch you warn the specified WP network will be outprop	ficany Set San Provi					

Figure 81 Network Setting > Wireless > WLAN Scheduler > Add New Rule

The following table describes the labels in this screen.

Table 38 Network Setting > Wireless > WLAN Schedule > Add New Rule

IABEL	DESC RIPTIO N
Active	Slide the switch to the right (
SSID	Select All wire less networks if you want the rule to apply to all wireless network interfaces or select a wireless network interface to apply the rule to.
Rule Name	Enter a descriptive name for the rule.
Day	Select the day(s) of the week that you wish to apply this rule.
Time of Day Range	Specify the time of the day that you wish to apply to this rule (format $hh:mm$). Note: Click the check box for All day if you wish to apply the rule for the whole day
	(24 hours).
Description	Enter a description of the rule, usually to help identify it (its purpose).
OK	Click OK to save the changes back to the Zyxel Device.
Cancel	Click Cancel to close the window with changes unsaved.

7.10 Channel Status

Use this screen to scan for wireless LAN channel noises and view the results. Click **Scan** to start, and then view the results in the **Channel Scan Result** section. The value on each channel number indicates the number of Access Points (AP) using that channel. The Auto-channel-selection algorithm does not always directly follow the AP count; other factors about the channels are also considered. Click **Network Setting > Wire less > Channel Status**. The screen appears as shown. Click **Scan** to scan wireless LAN channels. You can view the results in Channel Status screen.





7.11 Technical Reference

This section discusses wireless LANs in depth.

7.11.1 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.





The WiFi network is the part in the blue circle. In this WiFi network, devices \mathbf{A} and \mathbf{B} use the access point (\mathbf{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.

7.11.2 Additional Wire less Terms

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

TERM	DESC RIPIIO N
RTS/CTS Threshold	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.
	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.
	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.
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.

Table 39 Additional WiFi Terms

7.11.3 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.

7.11.3.1 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.

7.11.3.2 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.

7.11.3.3 UserAuthentication

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.

7.11.3.4 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 7.11.3.3 on page 121 for information about this.)

	NO A UTHENTICATION	RADIUS SERVER
Weakest	No Security	WPA
\$	WPA-PSK	
Strongest	WPA2-PSK	
		WPA2

Table 40 Types of Encryption for Each Type of Authentication

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.

7.11.4 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.

7.11.5 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.





7.11.6 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.

7.11.7 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.

7.11.7.1 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 7.6 on page 110).
- 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.

7.11.7.2 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 7.6 on page 110).
- 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.



7.11.7.3 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.



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.

7.11.7.4 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.





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 API 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.





CLIENT 2

In step 3, you add another access point (AP2) to your network. AP2 is out of range of AP1, so you cannot use API 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.



7.11.7.5 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.

C HAPTER 8 Home Networking

8.1 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.



8.1.1 What You Can Do in this Chapter

- Use the IAN Setup screen to set the LAN IP address, subnet mask, and DHCP settings (Section 8.2 on page 132).
- Use the Static DHCP screen to assign IP addresses on the LAN to specific individual computers based on their MAC addresses (Section 8.3 on page 136).
- Use the UPnP screen to enable UPnP (Section 8.4 on page 138).

8.1.2 What You Need To Know

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

8.1.2.1 About IAN

IPAddress

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 do not need to change the subnet mask computed by the Zyxel Device unless you are instructed to do otherwise.

DHC P

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.

8.1.2.2 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 8.6 on page 140 for examples on installing and using UPnP.

8.2 IAN Setup

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.

Use this screen to set the Local Area Network IP address and subnet mask of your Zyxel Device. Configure DHCP settings to have the Zyxel Device or a DHCP server assign IP addresses to devices. Click **Network Setting > Home Networking** to open the **LAN Setup** screen.

Figure 90	Network Setting > Home	Networking > LAN Setup
-----------	------------------------	------------------------

Manager - Strengt -						
maname	perior.					
8123eba					9.0	
	112	1.0			11	
				-		
and and a second	-000					
ICP Server Stole						
HT.	· Produce of the	15 BYO	Onia -			
Addressing Volues						
ingenig P. Liken	200		-			
inter Anna	10	1.18			1.00	
Weberg & Arriston State						
CP Server Lessie Time						
i ma		Nor:	1.	-		
ti Volum						
R	Denne II	ile San	1			
in Pvs Mode Setup						
	-					
III Local Address Proe-						
an ethnis at the other in such						
or Construction where						
4444,846,942						
al investments and up						
All and a second state of the second state of					- *	
100						
Willy's Address Assign Setup						
Patrice -			5 e -			
MITTY'S DNS Assign Letup						
Prov Fill (Sector Inter-			24			
CPV6 Configuration						
in the action	(The second second					
is four Advertureed Unle						
ment kika	and a					
vs 246 Volum						
Paris and	10-10 C					
Pri () Caren (Repection .					
No 24 (1999)	mpro de					

LTE Series User's Guide

The following table describes the fields in this screen.

Table 41 Network Setting > Home Networking > LAN Setup

LABEL	DESC RIPTIO N				
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	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.				
	If you select Disable , you need to manually configure the IP addresses of the computers and other devices on your LAN.				
	If you select DHCP Re lay , the Zyxel Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients.				
	When DHCP is used, the following fields need to be set:				
IP Addressing Values					
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 Tir	me				
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	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.				
	Select From ISP if your ISP dynamically assigns DNS server information (and the Zyxel Device's WAN IP address).				
	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.				
	Select $DNS Pro xy$ to have the DHCP clients use the Zyxel Device's own LAN IP address. The Zyxel Device works as a DNS relay.				
LAN IPv6 Mode Setup					
IPv6 Active	Use this field to Enable or Disable IPv6 activation on the Zyxel Device.				
	When IPv6 activation is used, the following fields need to be set:				

IABEL	DESC RIPIIO N						
Link Local Address Type	A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a "private IP address" in IPv6. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of fe80::/10. The link-local unicast address format is as follows. Select EUI64 to allow the Zyxel Device to generate an interface ID for the LAN interface's link-local address using the EUI-64 format. Otherwise, enter an interface ID for the LAN interface's link-local address if you select Manual .						
	Link-local Unicast Address Format						
	1111 1110 10 0 Interface ID						
	10 bits 54 bits 64 bits						
LAN Global Identifier Type	Select EUI64 to have the Zyxel Device generate an interface ID using the EUI-64 format for its global address. Select Manual to manually enter an interface ID for the LAN interface's global IPv6 address.						
LAN IPv6 Prefix Setup	Select Delegate prefix from WAN to automatically obtain an IPv6 network prefix from the service provider or an uplink router. Select Static to configure a fixed IPv6 address for the Zyxel Device's LAN IPv6 address.						
LAN IPv6 Address	Select how you want to obtain an IPv6 address:						
Assign Setup	State less: The Zyxel Device uses IPv6 stateless autoconfiguration. RADVD (Router Advertisement Daemon) is enabled to have the Zyxel Device send IPv6 prefix information in router advertisements periodically and in response to router solicitations. DHCPv6 server is disabled.						
	Sta te ful: The Zyxel Device uses IPv6 stateful autoconfiguration. The DHCPv6 server is enabled to have the Zyxel Device act as a DHCPv6 server and pass IPv6 addresses to DHCPv6 clients.						
LAN IPv6 DNS Assign Setup	Select how the Zyxel Device provide DNS server and domain name information to the clients:						
	From Router Advertisement: The Zyxel Device provides DNS information through router advertisements.						
	From DHCPv6 Server. The Zyxel Device provides DNS information through DHCPv6.						
	From RA & DHC Pv6 Server: The Zyxel Device provides DNS information through both router advertisements and DHCPv6.						
DHCPv6 Configuration	DHC Pv6 Active shows the status of the DHCPv6. DHC Pv6 Server displays if you configured the Zyxel Device to act as a DHCPv6 server which assigns IPv6 addresses and/or DNS information to clients.						
IPv6 Router Advertisement State	RADVD Ac tive shows whether RADVD is enabled or not.						
IPv6 DNS Values							
IPv6 DNS Server 1~3	Specify the IP addresses up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses.						
	Use r De fine d - Select this if you have the IPv6 address of a DNS server. Enter the DNS server IPv6 addresses the Zyxel Device passes to the DHCP clients.						
	From ISP - Select this if your ISP dynamically assigns IPv6 DNS server information.						
	$\mathbf{Pro} \mathbf{xy}$ - Select this if the DHCP clients use the IP address of this interface and the Zyxel Device works as a DNS relay.						
	Otherwise, select None if you do not want to configure IPv6 DNS servers.						

 Table 41
 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESC RIPTIO N
DNS Query Scenario	Select how the Zyxel Device handles clients' DNS information requests.
	IPv4/IPv6 DNS Server : The Zyxel Device forwards the requests to both the IPv4 and IPv6 DNS servers and sends clients the first DNS information it receives.
	IPv6 DNS Server Only : The Zyxel Device forwards the requests to the IPv6 DNS server and sends clients the DNS information it receives.
	IPv4 DNS Server Only : The Zyxel Device forwards the requests to the IPv4 DNS server and sends clients the DNS information it receives.
	IPv6 DNS Server First : The Zyxel Device forwards the requests to the IPv6 DNS server first and then the IPv4 DNS server. Then it sends clients the first DNS information it receives.
	IPv4 DNS Server First : The Zyxel Device forwards the requests to the IPv4 DNS server first and then the IPv6 DNS server. Then it sends clients the first DNS information it receives.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

Table 41 Network Setting > Home Networking > LAN Setup (continued)

8.3 Static DHCP

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 table allows you to assign IP addresses on the LAN to 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.

8.3.1 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 91 Network Setting > Home Networking > Static DHCP



The following table describes the labels in this screen.

LABEL	DESC RIPTIO N
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.
	Click the Delete icon to remove the connection.

Table 42 Network Setting > Home Networking > Static DHCP

If you click Static DHCPConfiguration in the Static DHCP screen, the following screen displays.

	and bird comgonator	
27.m		
Oldud Harry	Detaut	a .
et sine -	144	
and man W	Assistant a Set	•
anta constituta	8 28 28 291	-2
Protein 1		

Figure 92 Static DHCP: Static DHCP Configuration

The following table describes the labels in this screen.

Table 43	Static DHCP [•] Cc	onfiguration
	June Drier. Ce	ningoranori

LABEL	DESC RIPTIO N
Active	Select Enable to activate static DHCP in your Zyxel Device.
Group Name	This displays the Group Name, Usually Default.
IP Туре	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.

LABEL	DESC RIPIIO N
ОК	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

Table 43	Static DHCP: Configuration
	static brief . Cornigoration

8.4 UPnP

Universal Plug and Play (UPnP) is an open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between networking devices or software applications which have UPnP enabled. A UPnP device can dynamically join a network, obtain an IP address, advertise its services, and learn about other devices on the network. A device can also leave a network automatically when it is no longer in use.

See Section 8.6 on page 140 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 93 Network Setting > Home Networking > UPnP

- cive Uvter Tritos Teixo	eral Flug and Ride (19 aid hily between hele ok, and shi whier activ ok emperiek and auk	(a) can define the set of a period to a set of a realing demonstrated sufficient for a real control of control of the set of real can y offer that to control out off can y offer that to control out	g Mardon (1991), Martil No Trans (1717) endaled National Cathol (1994) N	NA for Crock paramis . A UNIT de cor cor o r the recent in de d	percetable (non-cultur) on c those believe
UPn7 S	tote				
1990		0			
JPnf N	IAT-T State				
Unit.	(ase	4			
t isin					
Pro 14	64 any ostal when i	Al elenitole			
	Dependent	Section IF Address	External Fort	Internal Port	Protocol
		Cancal	Apply		

The following table describes the labels in this screen.

Table 44 Network Settings > Home Networking > UPnP

IABEL	DESC RIPIIO N
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	

IABEL	DESC RIPIIO N
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. Choices are TCP or UDP .
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

Table 44 Network Settings > Home Networking > UPnP

8.5 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.



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."

8.6 Tum 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 by clicking **Network Setting > Home Networking > UPnP**.

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

-	Const. Marcon and the second s	takes -		111
	An Constantion An Constantion of Section And Constantion of Section And Andrew And	Communities Communities	El Janes Bi Visco Arco Bi Nacional Bi Naci	E commentante 2 par se o co E commença 2 par se prime 2 par se prim 2 par se prim 2 par se prime 2 par
	Contraction of			~

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

2 Click Change Advanced Sharing Settings.

Co. Di statut		ter:	-
Concernant of the second secon		<u>a</u>	
1	De 222. (222.)	Andreas Salarine	
	Y Contractor Contractor	an a	
Constant of the	4 (
Same Agent			

3 Select **Tum 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.



8.6.1 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 the LAN port of the Zyxel Device.

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

Figure 95 Network Connections

genide * Herviolitians Shalling Center	Add a printer And a winder party.
Formalies Disting Sourcease Sourcease I Looins	 Computer (1) Inverter on and Net the computer of the co
j Vocumente 1 Marco 1 Marco 1 Videba 2 Computer 1 Local Did (21) 2 Ford (201 21) 2 Ford (201 21) 2 Rom	Provi doproti vecinjego. Disobio Zobio: Creato sinovinat Yrodotneji
f ber I otr 1 Tecl Nøtsark	

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

Figure 96 Internet Connection Properties

and Chipple			
Gornal (Articulations)			
Lametra de meneturo			
🗯 internat Connector			
hu dan terdan elariar yanga teranakan prompole	conectic fieldon	net through a shared cor	veces)
		Les a	1000
		Charles and Charle	

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

Figure 97	Internet Connection	Properties:	Advanced	Settings
				0

there before				
Sector				
Solar Baranaa		Sector 1		
200 (201	64			
2.1				
		30.		Celes
			1. CC	1 Daniel
				1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

Figure 98 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 the system tray to see your Internet connection status.



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 100	Internet Connection Status
------------	----------------------------

	1000000	
érre x		
iner -		
To al Constanting	Q	Indexner
Pro Connection IN	Ş	No network access
Post Course		Fishers
Only Bend		11,26,27
Served 1		the slope
inek.		
	ser — 📕	
197.94	320.54	17,299,246
(Secondar)	rpunes []	agent
		Locen

8.7 Tum on UPnP in Windows 10 Example

This section shows you how to use the UPnP feature in Windows 10. UPnP server is installed in Windows 10. Activate UPnP on the Zyxel Device by clicking **Network Setting > Home Networking > UPnP**.

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

of up.				- 11 X
		Let exting	μ	
_	Ny Jeon Desky start, not saide a proce	i i i i i i i i i i i i i i i i i i i	La base Labyre for the Autor	He would be follow a Marka and an array (Marka
) – Peris di futuationen Reche, ne sel, fai fasse i si e des	Hardel, a dash a dash a dash Karata	Accessa Second construction accesses	Spinner Kittangunge Spinner segunde
~	Gaming Course cos, Brañ Introducentino Vener Mitche	Con Disa di Acreso Harrison accession hier No cost	💾 Ritary Transa, and a	Diplome 2 Security Values a lipture, interes, lipture
R) – Nora I. Language processes of story			

1 Click the start icon, Settings and then Network & Internet.

2 Click Network and Sharing Center.


3 Click Change advanced sharing settings.

📱 Network and Sharing Center				-	30
🔶 🔅 🔅 🕆 🙀 x Centrol Parte	I > All Control Panel Items > Network and Starling Cent	leg:	\times 0	Search Centrol Panel	,p
Control Panel Home	View your basic network information and a	et up connections			
Charles adjuster anti-	line year active selands				
Change advanced sharing settings	Nationark 2 Palvata: nativoli	Annex (pper Internet Connections: 🖉 Othernet 2			
	Changeyour returning settings				
	Set up a new connection or network. Det up a travellanet, status, or 2010 connection	ej ne sel qua essiler ne annesa pulei.			
	Toubledicat peoplems Disgross and repeit retwork problems, or get?	toubleshooting information.			
Secular					
Internet Options					
Windows Defender Fisovall					

4 Under **Domain**, select **Tum 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.

*4 Alexandred thering railings				1. 18
= - + + + Schollend - Al	Control Rahal Norm - Network and Shalong Casher - Advanced sharing settings	- 6	- Same Control Barg	-
	Charge sharing options for althous natively perfect to early observe the set of theme appeals relevely perfect to early observe the set of theme appeals relevely perfect to early observe the set of theme appeals relevely perfect to early observe theme appeals relevely perfect to early observe theme appeals relevely perfect to early observe theme appeals relevely to early observe the set of the set o			
	Standorm Court	11		

8.7.1 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 the LAN port of the Zyxel Device.

- 1 Open File Explorer and click Network.
- 2 Right-click the Zyxel Device icon and select Properties.

n Anti-anti-southe (Balancesepe- Metwork) nfrastructure (1) Introde-6600 Vice dedec activity
Althout to calle (Batannesses) V Network Infrastructure (1) Infrastructure Units for the sectors
Vice de la compar
Wine deskin and same
The PL Ward Proc. Planta West
Houtle international balg
Dalaria.
Createshorted
Protection

Figure 101 Network Connections

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

Figure 102 Internet Connection Properties

and a personal service					
Connect to the Droemet Lenge					
🛲 Information					
The connection allows you to p on another comparter.	ernet to h	as interne	an sign 6.	ine of cours	etton
				a fores	

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

Figure 103 Internet Connection Properties: Advanced Settings

Advanced India ye			2
Searce			
Meetile wave and	and so to possible	ah dan lawa	a na sa
Anna anna anna anna anna anna anna anna			
B			
All	H		D Inde
		а.	Grud

Figure 104 Internet Connection Properties: Advanced Settings: Add

Service Settings			?	×
Description of service:				
Name or IP address (or even computer hosting this service in	ple 192.168.0. on your netwo	12) of 1 fr	he	
				_
Edonal Pot number for the Internet Pot number for this a	anecc. 80 B	P	0 	
	OK		Des	4

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 the system tray to see your Internet connection status.



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



Figure 106 Internet Connection Status

8.8 Web Configurator Easy Access in Windows 7

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 107 Network Connections

apare Mensile and an approximation of	allegion	Valuated pleasables
 Industry 	 Computer : Mean and in 	(E taitavent firmoture (E) , intraviews

- 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.

igner in the second sec	Research and Subsequences	and been	dates and be
 Taxo tess De Ang Develop de Desert Placet Desert Placet	 Comparer (1) Wreczwerte Netware Infrastruct Entrast Max Entrast Max Entrast Entrast Entrast Entrast Entrast Entrast 	a: 110:51) 119:97 4	

Figure 108 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 109 Network Connections: My Network Places: Properties: Exc	ample
--	-------

- 1 : 10 4 M	4.5
Senier Selar	
Arista area	 (N)-4 (A) (N)-200 (PRODUCT)
N N	TEXT BACKED By We are compared at
Nodol number:	.TE72-8-4-463
Cesarie car queges	1012200.000.0
Trada cahoatana Jeria	πales
fer set and and	41-
HWC #ddraw	×
Unious Identifier	4.4
De la sec	- 41

8.9 Web Configurator Easy Access in Windows 10

Follow the steps below to access the Web Configurator.

- 1 Open File Explorer.
- 2 Click Network.

MASIC - M.	
Martin Frankling	Attraction Constants
letoket.	Schoold
	11 T
le sharing is to be full. Some of	rteants comparies and devices might part he veil de Olista or near p
	WhetworkInfrastructure (1
Consecutions	
🔏 OndQ it/s	1707240-14400
and the state of the	
Dasktop	
- Provensi	
📲 Douinica de	
A Mark	
an Falses	
E Vdag	
E Falare E Falare Sa Salaritan Ca	

Figure 110 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.

nter Bart Lawr with Small - 14 Friday President - 14	Alforer Transference		
	H 547-9		
- · · · · · · · · · · · · · · · · · · ·			
ning an <mark>arad</mark> of, acina navora carea	anen and devices ni ginines be els bis. Click to change.		
Culti scian	··· Network Infrastructure (%)		
Caclanic			
🕎 Bester 🎯 3D Glaers	Tana Brahmaningapa Saabbah terusti ana mataina		
Burgerand :	Contrological		
Downliceds	Arcure Set		
an internet			
Market 1			

Figure 111 Network Connections: Network Infrastructure

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

Figure 112 Network Connections: Network Infrastruct	ure: Properties: Example
---	--------------------------

D JINGAN	a:
evitor Cetato	
Annumferbarner:	2011
kodel	0127343-0403 9227/1/1-021704-0216
e lebrarden	3.4
enios neososge:	10015-001-001-0001
nalissiana, siki	ration -
Anie namber:	51001900.00810
C.F. alleren	4. A. 03. A. 22
the state	$(a_{1},a_{2},2) \in \mathcal{T}(\mathcal{T}_{2},a_{2},2) \cap \mathcal{T}(\mathcal{T}(\mathcal{T}_{2},a_{2},2) \cap \mathcal{T}(\mathcal{T}_{2},2)) \cap \mathcal{T}(\mathcal{T}(\mathcal{T}_{2},a_{2},2$
r s dareas	is a new lot

C HAPTER 9 Routing

9.1 Overview

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

For example, the next figure shows a computer (A) connected to the 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 113 Example of Static Routing Topology

9.2 Configure Static Route

Use this screen to view and configure static route rules on the Zyxel Device. A static route is used 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 in your home or office network. Click **Ne twork Setting > Routing** to open the **Static Route** screen.



V.2 Ale 207	erando sali na indeka naecionalia	generalista versalista versiones	when the same time Arrest states are to be a most trans- profiles narrowers.	How we have a second	lana ta kisa binan Kata ta kisa binang	ere i le ana ber lin ana basa basa s	1949 B
						<mark>le</mark> Aleitea	Alexa Sec. 4
	Media 4	Na me	Sedender P	Subsections by Teeffiel enotity	Converg	interfacer.	No.49y

The following table describes the labels in this screen.

LABEL	DESC RIPTIO N
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 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 Zyxel 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 De le te icon to remove a static route from the Zyxel Device.

Table 45 Network Setting > Routing > Static Route

9.2.1 Add/Edit Static Route

Click Add New Static Route in the Static Route screen, the following screen appears. 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.

Configure the required into	whether love a	referent.			
NT A					
ndere nation					
a light	1.9			2.4	
Cieff day Awayson			505		
Selar a Street		- 42	36		
Denter, Hereiter					
Convert Acons					
1	(teste a			100	

Figure 115 Network Setting > Routing > Static Route > Add New Static Route

The following table describes the labels in this screen.

Table 46	Network Setting >	Routing >	Static Route >	Add New S	static Route
----------	-------------------	-----------	----------------	-----------	--------------

IABEL	DESC RIPTIO N
Active	Select Enable to activate your static route.
Route Name	Assign a name for your static route (up to 15 characters). Special characters are allowed except the following: double quote (") back quote (`) apostrophe or single quote (') less than (<) greater than (>) caret or circumflex accent (^) dollar sign (\$) vertical bar () ampersand (&) semicolon (;)
ІР Туре	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	Select \mathbf{Enable} to enable forwarding packets to a gateway IP address or a bound interface.
Gateway IP	You can decide if you want to forward packets to a gateway IP address or a bound interface.
Address	If you want to configure Gateway IPAddress , enter the IP address of the next-hop gateway. The gateway is a router or switch on the same network segment as the Zyxel 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 (De fa ult) or a bound interface (Ce Ilula r 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.
ОК	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

LTE Series User's Guide

9.3 DNS Route

Use this screen to view and configure DNS routes on the Zyxel Device. A DNS route entry defines a policy for the Zyxel Device to forward a particular DNS query to a specific WAN interface. Click **Ne two rk Se tting** > **Routing** > **DNS Route** to open the **DNS Route** screen.

Figure 116 Network Setting > Routing > DNS Route

				+ 2	de New 2015 Roci
•	into tax	Sandir Nano	was defait	tabaci Mode	Notly

The following table describes the labels in this screen.

IABEL	DESC RIPTIO N
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 $\mathbf{De} \mathbf{le} \mathbf{te}$ icon to remove a DNS route from the Zyxel Device.

Table 47 Network Setting > Routing > DNS Route

9.3.1 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.

	Add New DNS Route	
ist-4	(* •)	
Songri Jane		
Const Wate	· · · · · · · · · · · · · · · · · · ·	
Westernethers	tr/s nowes	

Figure 117 Network Setting > Routing > DNS Route > Add New DNS Route

The following table describes the labels in this screen.

IABEL	DESC RIPTIO N
Active	Enable DNS route in your Zyxel Device.
Domain Name	Enter the domain name you want to resolve.
	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.

9.4 Policy Route

By default, the Zyxel Device routes packets based on the shortest path to the destination address. Policy routes allow you to override the default behavior and route packets based on other criteria, such as the source address. For example, you can use policy-based routing to direct traffic from specific users through specific connections or distribute traffic across multiple paths for load sharing. Policy-based routing is applied to outgoing packets before the default routing rules are applied.

The Policy Route screen let you view and configure routing policies on the Zyxel Device. Click Network Setting > Routing > Policy Route to open the following screen.





LABEL	DESC RIPTIO N
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 De le te icon to remove a policy from the Zyxel Device. A window displays asking you to confirm that you want to delete the policy.

Table 49 Network Setting > Routing > Policy Route

9.4.1 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 119 Policy Route: Add/Edit

ist et	1 10	
Soura Barna		
Course Cixiddiness	ti ti it it	
Course Solorier Analt		
entral.	NCM	
Status Tor	1	
Source Cost.		
$_{\rm CO}$ and with the last the $_{\rm CO}$, and $_{\rm CO}$	1	
Average and the second	Se(4.51/(42)	(e)

Table 50	Policy Route: Add/Edit
----------	------------------------

IABEL	DESC RIPHO N
Active	Click this to enable (turns blue) activation of the policy route. Otherwise, click to disable (turns gray).
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, UDP, or None).
Source Port	Enter the source port number.
Source MAC	Enter the source MAC address.
SourceInterface (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.
ОК	Click OK to save your changes.

9.5 RIP Overview

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

9.5.1 RIP

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.

Tigute 120 Retwork Setting & Rooting & Rit	Figure 120	Network Setting > Routing > R	IP
--	------------	-------------------------------	----

(10) (10)	terangeria				
6	-Interface	Varies	O deraiker	factile	Intelle Defauit Goleway
	Georgeowy)	m. 	A4826 🖤 🗉	11	11
10	-21,9669	80. 0	Active 🖤 .	1.1	L.I

IABEL	DESC RIPTIO N
#	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). RIPv1 is universally supported but RIPv2 carries more information. RIPv1 is probably adequate for most networks, unless you have an unusual network topology. When set to Both , the Zyxel Device will broadcast its routing table periodically and incorporate the RIP information that it receives
Operation	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. Select Active to have the Zyxel Device advertise its route information and also listen for routing updates from neighboring routers.
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.

Снартек 10 Network Address Translation (NAT)

10.1 Overview

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

10.1.1 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 10.2 on page 163).
- Use the **Port Thiggering** screen to add and configure the Zyxel Device's trigger port settings (Section 10.3 on page 166).
- Use the DMZ screen to configure a default server (Section 10.4 on page 169).
- Use the ALG screen to enable or disable the SIP ALG (Section 10.5 on page 170).
- Use the Address Mapping screen to enable and disable the NAT Address Mapping in the Zyxel Device (Section 10.6 on page 171).
- Use the Sessions screen to limit the number of concurrent NAT sessions each client can use(Section 10.7 on page 173).

10.1.2 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.

10.2 Port Forwarding Overview

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.

Configure 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.





10.2.1 Port Forwarding

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

Note: TCP port 7547 is reserved for system use.

Figure 122 Network Setting > NAT > Port Forwarding



The following table describes the fields in this screen.

LABEL	DESC RIPTIO N
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.
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 De le te icon to delete an existing port forwarding rule. Note that subsequent address mapping rules move up by one when you take this action.

Table 52	Network Setting > 1	NAT >	Port Forwardina

10.2.2 Add/Edit Port Forwarding

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.

Fig ure	123	Port Forwarding: Add/Edit	ł
I IS UIC	140	i on	1

	Add New	Role	
Action 1			
And control of the			
www.com	sider	× .	
Stat Par.			
Inc Part			
Trenk at on Gion Port			
contration services			
Server 7 Address	1 <u> </u>		
Contrains Orbitating #	📴 era i der		
usigenting =			
Parkes	16*		
(2 · v· s.			
r in theote on exit a part lower	ninan in upicity rither academan	ige of parts, a reverse address, and a polacia (
Strand and but paying	general terror terror sky	where a fire Shell Park Park Davidation Shell	Ref. and
 Translation End Red & da To scartigere switt Installate Translation End Part issist. 	n overheed to have different configur	die nam die Stanfert Englitiet Granskalien Stad P	at ord
	CONTRACTOR OF A DECIMARY OF A		

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.

Here is an example to configure port translation. Configure Start Port to 100, End Port to 120, Thanslation Start Port to 200, and Thanslation End Port to 220.

Note: TCP port 7547 is reserved for system use.

IABEL	DESC RIPTIO N
Active	Select or clear this field to turn the port forwarding rule on or off.
Service Name	Select a service to forward or select $Use r De fine d$ and enter a name in the field to the right.
WAN Interface	Select the WAN interface for which to configure NAT port forwarding rules.

Table 53 Port Forwarding: Add/Edit

LABEL	DESC RIPTIO N			
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.			
Configure Originating IP	Click the Enable check box to enter the originating IP in the next field.			
Originating IP	Enter the originating IP address here.			
Protocol	Select the protocol supported by this virtual server. Choices are TCP, UDP, or TCP/ UDP.			
ОК	Click this to save your changes.			
Cancel	Click this to exit this screen without saving.			

 Table 53
 Port Forwarding: Add/Edit (continued)

10.3 Port Triggering

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 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 that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

For 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 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.

Figure 125 Network Setting > NAT > Port Triggering



The following table describes the labels in this screen.

IABEL	DESC RIPTIO N				
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.				
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.				

Table 54 Network Setting > NAT > Port Triggering

10.3.1 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 126 Port Triggering: Add/Edit

	Add New I	tole
40%a		
Serios Totte		
10-21-5 (1-1-	191-1	•
(4)		
(Appendent) - and		
The per Protocol	10P	
Openador Part		
Open and Port		
Open/pitopat	702	*

The following table describes the labels in this screen.

Tabla 55	Port Triggoring:	Add/Edit
10016 22	Fon inggening.	AUU/EUII

IABEL	DESC RIPTIO N			
Active	Click to enable (blue switch) or disable (gray switch) 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.			
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.			

10.4 DMZ

Use this screen to specify the IP address of a default server to receive packets from ports not specified in the **Port Triggering** screen. The DMZ (DeMilitarized Zone) is a network between the WAN and the LAN that is accessible to devices on both the WAN and LAN with firewall protection. Devices on the WAN

can initiate connections to devices on the DMZ but not to those on the LAN.

You can put public servers, such as email, web, and FTP servers, on the DMZ to provide services on both the WAN and LAN. To use this feature, you first need to assign a DMZ host. Click **Network Setting > NAT> DMZ** to open the **DMZ** screen.

Note: Use an IPv4 address for the DMZ server.

Note: Enter the IP address of the default server in the **Default Server Address** field, and click **Apply** to activate the DMZ host. Otherwise, clear the IP address in the **Default Server Address** field, and click **Apply** to deactivate the DMZ host.

Figure 127 Network Setting > NAT > DMZ



The following table describes the fields in this screen.

Table 56	Network Setting > NAT > DMZ
----------	-----------------------------

LABEL	DESC RIPTIO N		
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.		

10.5 ALG

Click **Network Setting > NAT> AIG** to open the **AIG** 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 128 Network Setting > NAT > ALG



The following table describes the fields in this screen.

	Nist work Catting as NIATS ALC
aple 5/	Network Setting > NAT > ALG

IABEL	DESC RIPIIO N
SIP ALG	Click this (switch turns blue) to make sure SIP (VoIP) works correctly with port-forwarding and address-mapping rules. Otherwise, click this to turn off (switch turns gray) the SIP ALG.
PPTP ALG	Click this to turn on (switch turns blue) the PPTP ALG on the Zyxel Device to detect PPTP traffic and help build PPTP sessions through the Zyxel Device's NAT.
Apply	Click Apply to save your changes back to the Zyxel Device.
Cancel	Click Cancel to restore your previously saved settings.

10.6 Address Mapping

Use this screen to enable or disable the NAT Address Mapping in the Zyxel Device.

10.6.1 Address Mapping Screen

Click Network Setting > NAT> Address Mapping to open the Address Mapping screen.

Figure 129 Network Setting > NAT > Address Mapping

			NAT				
9.46 Concerner	Nothiggen)	162 AS A	hterne Mappings	area.			
Actional Maps	eng can nag tee	el IP Actoresses To	Crocci - Addresser			1222	
N (11		10000000000			-		
Rule Same	Local Start IF	Local End P	Olobel Start P	Clobal End IF	Sthe	WAN Interfuce	Modely

Table 58 Network Setting > NAT > Address Mapping				
LABEL	DESC RIPHO N			
Rule Name	This is the name of the rule.			
Local Start IP	This is the starting Inside Local IP Address (ILA).			

IABEL	DESC RIPIIO N
Local End IP	This is the ending Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is blank for One-to-One mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for the Many-to-One mapping type.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is blank for One-to-One and Many-to-One mapping types.
Туре	This is the address mapping type.
	One-to-One: This mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-One NAT mapping type.
	Many-to-One: This mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), the Device's Single User Account feature that previous routers supported only.
	Many-to-Many: This mode maps multiple local IP addresses to shared global IP addresses.
WAN Interface	This is the WAN interface to which the address mapping rule applies.
Modify	Click the Edit icon to go to the screen where you can edit the address mapping rule.
	Click the \mathbf{Delete} icon to delete an existing address mapping rule. Note that subsequent address mapping rules move up by one when you take this action.

Table 58 Network Setting > NAT > Address Mapping (continued)

10.6.2 Add New Rule Screen

To add or edit an address mapping rule, click **Add New Rule** or the **Modify** icon in the **Address Mapping** screen to display the screen shown next.

		Ad	a new fold	6	
The Horse					
105	1000				
Louis and R					
transis &					
1.0162.00		4.2	- 44	122	
Distances (Pro-					
908-1-104-1	23.00				

Figure 130 Network Setting > NAT > Address Mapping > Add New Rule

The following table describes the fields in this screen.

IABEL	DESC RIPTIO N
Rule Name	Type up to 20 alphanumeric characters for the name of this rule.
Туре	Choose the IP/port mapping type from one of the following.
	One-to-One: This mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-One NAT mapping type.
	Many-to-One: This mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), the Device's Single User Account feature that previous routers supported only.
	Many-to-Many: This mode maps multiple local IP addresses to shared global IP addresses.
Local Start IP	Enter the starting Inside Local IP Address (ILA).
Local End IP	Enter the ending Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is blank for One-to-One mapping types.
Global Start IP	Enter the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for the Many-to-One mapping type.
Global End IP	Enter the ending Inside Global IP Address (IGA). This field is blank for One-to-One and Many-to-One mapping types.
WAN Interface	Select a WAN interface to which the address mapping rule applies.
Cancel	Click Cancel to exit this screen without saving.
OK	Click OK to save your changes.

Table 59 Network Setting > NAT > Address Mapping > Add New Rule

10.7 Sessions

Use the Sessions screen to limit the number of concurrent NAT sessions each client can use. Click Ne twork Setting > NAT> Sessions to open the Sessions screen.

Figure 131 Network Setting > NAT > Sessions

	N.	AT .	
Performation and marging	Dot a consideration	n Saulon:	
The figure balance in the balance is a second or gradient with the second or gradient	subicipion a per rectificit.AN P foet of NAI sectors in proef to pe	Publicus) pusé Server doplications a geodra el o better uploading and downloading rol	(yillio P2PT). ■
MAARIAN Sectors Par Posi (S- - 70:00)	2048		
(+cre			
(1) one reason non-second citio (2) Electrine textion number field	Apply to do twole this leadure, and a low Apply to devocity the	the facture.	
	Concel	Apply	

IABEL	DESC RIPTIO N
MAX NAT Session Per Host (0~20480)	Use this field to set a common limit to the number of concurrent NAT sessions each client computer can have.
	If only a few clients use peer to peer applications, you can raise this number to improve their performance. With heavy peer to peer application use, lower this number to ensure no single client uses too many of the available NAT sessions.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

Table 60 Network Setting > NAT > Sessions

C HAPTER 11 Dynamic DNS Setup

11.1 DNS Overview

DNS

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

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

Dynamic DNS

Dynamic DNS allows you to use a dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). 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.

You first 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.

11.1.1 What You Can Do in this Chapter

- Use the DNS Entry screen to view, configure, or remove DNS routes (Section 11.2 on page 176).
- Use the **Dynamic DNS** screen to enable DDNS and configure the DDNS settings on the Zyxel Device (Section 11.3 on page 177).

11.1.2 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.

11.2 DNS Entry

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 routes on the Zyxel Device. Click **Ne twork 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 132 Network Setting > DNS > DNS Entry

	HotNorte	17 Address	Medity
No.			

The following table describes the fields in this screen.

LABEL	DESC RIPIIO N
Add New DNS Entry	Click this to create a new DNS entry.
#	This is the index number of the entry.
HostName	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.

Table 61 Network Setting > DNS > DNS Entry

11.2.1 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 133 DNS Entry: Add/Edit

<	Add New	DNS Entry	
of Nome			
$\mathcal{A}_{\mathcal{A}}$ is the formula $\mathcal{A}_{\mathcal{A}}$			
	Concel	OK.	

The following table describes the labels in this screen.

Table 62	DNS	Fntrv	Add	/Fdit
	0110		,	

IABEL	DESC RIPIIO N
Host Name	Enter the host name of the DNS entry.
IPv4 Address	Enter the IPv4 address of the DNS entry.
Cancel	Click Cancel to exit this screen without saving.
OK	Click OK to save your changes.

11.3 Dynamic DNS

Dynamic DNS can update your current dynamic IP address mapping to a hostname. Configure a DDNS service provider on your Zyxel Device. Click **Ne twork Setting > DNS > Dynamic DNS**. The screen appears as shown.

Figure 134	Network Setting > DNS > Dynamic DNS
------------	-------------------------------------

AND DOCUMENTS CARDING SCHOOL SCHOOL			
Germania datas	🔮 Dioble 🔅 Dioble (Setimorice and Diviser dioble)		
Det-up "stream	www.EgiptEuch	×	
Hold Photos			
10 million -			
Personant			•
📴 Drease in charact Syste			
Criscille Off Lave Color	u Only opposed to californi Dolly		
ynamic ONS Status			
(in a transferder Sec.)	*		
Last Goldsteid firme			

Table 63	Network Setting > DNS > Dynamic DNS	

IABEL	DESC RIPHO N	
Dynamic DNS Setup		
Dynamic DNS	Select Enable to use dynamic DNS.	
Service Provider	Select your Dynamic DNS service provider from the drop-down list box.	
Host Name	Type the domain name assigned to your Zyxel Device by your Dynamic DNS provider.	
	You can specify up to two host names in the field separated by a comma (",").	
Username	Type your user name.	
Password	Type the password assigned to you.	
Enable Wildcard Option	Select the check box to enable DynDNS Wildcard.	
Enable Off Line Option (Only applies to custom DNS)	Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.	
Dynamic DNS Status		
User Authentication Result	This shows $\mathbf{Success}$ if the account is correctly set up with the Dynamic DNS provider account.	
Last Updated Time	This shows the last time the IP address the Dynamic DNS provider has associated with the hostname was updated.	
Current Dynamic IP	This shows the IP address your Dynamic DNS provider has currently associated with the hostname.	
Cancel	Click Cancel to exit this screen without saving.	
Apply	Click Apply to save your changes.	

C HAPTER 12 USB Servic e

12.1 USB Service Overview

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

The following figure is an overview of the Zyxel Device's file server feature. Computers \mathbf{A} and \mathbf{B} can access files on a USB device (\mathbf{C}) which is connected to the Zyxel Device.





The Zyxel Device will not be able to join the workgroup if your local area network has restrictions set up that do not allow devices to join a workgroup. In this case, contact your network administrator.

12.1.1 What You Need To Know

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

12.1.1.1 About File Sharing

Workgroup Name

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

Shares

When settings are set to default, each USB device connected to the Zyxel Device is given a folder, called a "share". If a USB hard drive connected to the Zyxel Device has more than one partition, then each partition will be allocated a share. You can also configure a "share" to be a sub-folder or file on the USB device.

File Systems

A file system is a way of storing and organizing files on your hard drive and storage device. Often different operating systems such as Windows or Linux have different file systems. The file sharing feature on your Zyxel Device supports File Allocation Table (FAT) and FAT32.

Common Internet File System

The Zyxel Device uses Common Internet File System (CIFS) protocol for its file sharing functions. CIFS compatible computers can access the USB file storage devices connected to the Zyxel Device. CIFS protocol is supported on Microsoft Windows, Linux Samba and other operating systems (refer to your systems specifications for CIFS compatibility).

12.1.2 Before You Begin

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

- 1 Connect the USB device to one of the Zyxel Device's USB port. Make sure the Zyxel Device is connected to your network.
- 2 The Zyxel Device detects the USB device and makes its contents available for browsing. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.

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

12.2 USB Service

Use this screen to set up file sharing through the Zyxel Device. The Zyxel Device's LAN users can access the shared folder (or share) from the USB device inserted in the Zyxel Device. To access this screen, click **Ne twork Setting > USB Service**.


		US	B Service		
16. m. Ab. Deberath the	or, launus ("Richard Channa	yaan 200 kuu oo waxaa dago nii waxaa ahaa ahaa ahaa ahaa ahaa	den yaar oo ber intig t Gebeuruung Sister	n 1990). Al mar Mar Ka	0. "dog ologi
Information					
	Volument		Copies Iv	Seed Sc	cice.
	and the		NT VS	. 2.42	tais in
Server Config	uration				
Reference.	4:10	-			
Shore Directo	ry Lui				
					🛨 Ade Kulershare
Active	Shahuk	More Horse.	Shale Calif	Share Desctoton	Wodilly
Account Man	agameni				
	S				🙀 Ascilers itse
	varis			Hare Moune	
	2			Section .	
		12202303	20.0		
		Cancel	App	¥.	

Note: Share Directory List field appears when you connect a USB device to the USB port. Otherwise, it does not.

Each field is described in the following table.

IABEL	DESC RIPTIO N				
Information	Information				
Volume	This is the volume name the Zyxel Device gives to an inserted USB device.				
Capacity	This is the total available memory size (in megabytes) on the USB device.				
Used Space	This is the memory size (in megabytes) already used on the USB device.				
Server Configurat	Server Configuration				
File Sharing Services	Click this switch to enable or disable file sharing through the Zyxel Device. When the switch goes to the right 1 , the function is enabled. Otherwise, it is not.				
Share Directory Li	st				
Add New Share	Click this to set up a new share on the Zyxel Device.				
Active	Select this to allow the share to be accessed.				
Status	This field shows the status of the share				
	The share is not activated.				
	📅: The share is activated.				

Table 64 Network Setting > USB Service > File Sharing

LABEL	DESC RIPIIO N			
Share Name	This field displays the name of the file you shared.			
Share Path	This field displays the location in the USB of the file you shared.			
Share Description	This field displays a description of the file you shared.			
Modify	Click the Edit icon to change the settings of an existing share.			
Click the De le te icon to delete this share in the list.				
Account Management				
Add New User	Click this button to create a user account to access the secured shares. This button redirects you to Maintenance > UserAccount .			
Status	This field shows the status of the user.			
	: The user account is not activated for the share.			
	📽: The user account is activated for the share.			
User Name	This is the name of a user who is allowed to access the secured shares on the USB device.			
Cancel	Click this to restore your previously saved settings.			
Apply	Click this to save your changes to the Zyxel Device.			

Table 64 Network Setting > USB Service > File Sharing

12.2.1 Add New Share

Use this screen to set up a new share or edit an existing share on the Zyxel Device. Click Add New Share in the File Sharing screen or click the Edit/ Modify icon next to an existing share.

Please note that you need to set up your shares in the USB before enabling file sharing in the Zyxel Device. Also, spaces and the following special characters listed in the brackets ["`<> $^{|`}<>^{|}$ are not allowed for the USB share name.

veta2_ada)	
Public .	
	Asta2_adat) Public

Figure 137 Network Setting > USB Service > File Sharing > Add New Share

Table 65	Network Setting >	USB Service >	Media Server
----------	-------------------	---------------	--------------

IABEL	DESC RIPTIO N
Volume	Select the volume in the USB storage device that you want to add as a share in the Zyxel Device.
	This field is read-only when you are editing the share.
Share Path	Manually enter the file path for the share, or click the Browse button and select the folder that you want to add as a share.
	This field is read-only when you are editing the share.
Description	You can either enter a short description of the share, or leave this field blank.
Access Level	Select Public if you want the share to be accessed by users connecting to the Zyxel Device. Otherwise, select Security .
Allowed	If Security is selected in the Access Level field, select this check box to allow/prohibit access to the share.
User Name	This field specifies the user for which the Allowed setting applies. Users can be added or modified in Maintenance > UserAccount .
Cancel	Click Cancel to return to the previous screen.
OK	Click OK to save your changes.

12.2.2 The Add New User Screen

Once you click the **Add New User** button, you'll be directed to the **UserAccount** screen. To create a user account that can access the secured shares on the USB device, click the **Add New Account** button in the **Network Setting > USB Service > UserAccount** screen.

Please see Chapter 26 on page 245, for detailed information about User Account screen.

C HAPTER 13 Fire wall

13.1 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).





13.1.1 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.

ЮМР

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 Thre sholds

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.

13.2 Fire wall

13.2.1 What You Can Do in this Chapter

- Use the General screen to configure the security level of the firewall on the Zyxel Device (Section 13.3 on page 185).
- Use the **Protocol** screen to add or remove predefined Internet services and configure firewall rules (Section 13.4 on page 187).
- Use the Access Control screen to view and configure incoming/outgoing filtering rules (Section 13.5 on page 188).
- Use the **DoS** screen to activate protection against Denial of Service (DoS) attacks (Section 13.6 on page 191).

13.3 Fire wall General Settings

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. 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.



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**, Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3, SMTP, and/or IPv6 ICMPv6 (Ping) traffic from the LAN are still allowed.

The following table describes the labels in this screen.

LABEL	DESC RIPIIO N
IPv4 Firewall	Enable firewall protection when using ${f IPv4}$ (Internet Protocol version 4).
IPv6 Firewall	Enable firewall protection when using $\mathbf{IPv6}$ (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.

Table 66 Security > Firewall > General

13.4 Protocol (Customized Services)

You can configure customized services and port numbers in the **Protocol** screen. Each set of protocol rules listed in the table are reusable objects to be used in conjunction with ACL rules in the Access Control screen. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. Click **Security > Fire wall > Protocol** to display the following screen.

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

Figure	e 140 Secu	rity > Firewall > Protocol		
Ap Pr- Aut	entres konsta Laras, Case dares tertal Henty within	nantas nie witro define o entis sea Franz ar an Deine arronan anni eta o comprir reste. Mioto	e, Service for the Froil, Rephoner, owner The constraints for you want to only occurs a of nearbort and withing with the value (and	mewaging, Crites samev un chroke to in the Freed on heigh in namer
				E editions embour erroy
	Home	Cesciption	Rantz Protocci Number	Modity
Bay	v.			
Betry	ang ing ing second	de vellato remove avocaties 30	4 Max	

The following table describes the labels in this screen.

LABEL	DESC RIPIIO N
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 (TC P or UDP) that defines your customized service.
Modify	Click this to edit a customized service.

Table 67 Security > Firewall > Protocol

13.4.1 Add Customized Service

Add a customized rule or edit an existing rule by specifying the protocol and the port numbers. Click **Add New Protocol Entry** in the **Protocol** screen to display the following screen.

	Add New Prof	ocol Brity	
Acts or cultombed in mymound	u e criedrich aneologiju e c	vice chiro ne picio	KS 510 74 507
Serviziation			
Pethiolog		1	
Protocol	Otor		
Protocol - antoch		1	2-03

Figure 141 Security > Firewall > Protocol: Add New Protocol Entry

IABEL	DESC RIPIIO N
Service Name	Type a unique name for your custom port.
Description	Enter a description for your custom port.
Protocol	Choose the protocol (TCP, UDP, ICMP, ICMPv6 , or 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.
ОК	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

Table 68 Security > Firewall > Protocol: Add New Protocol Entry

13.5 Access Control (Rules)

An Access Control List (ACL) rule is a manually-defined rule that can accept, reject, or drop incoming or outgoing packets from 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 > Fire wall > Access Control to display the following screen.

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

 An encount (server) (1 (A.1.) score matrices, consist on the score of stage in 31 where a the one of god poors, some 	nde à closen spalo tratour crégains au cry courtai	, nën dethe dinsë Tra L'Ar seciritale gan V anling at avlgating Tr Gandar ara ganlad	n dan antwert mjent o of draktik swart wang t wang stiffs software o in fami	r dog kvorne nikr i Medog der Voerfek S	a senaren ingeryeurre in uniterieks	portivo ficir equit. Tra VCL
Rijavšto nga Socioa Usoba						
					<mark>1</mark> 6.	k si≑ XX. s. c
	Home	ara P	Ged ik	Service	Asten	Modily
11	211	1.464.260.01252	destruction angles		- topot	No e

Figure 142 Security > Firewall > Access Control

LABEL	DESC RIPIIO N
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 New ACLRule 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.
Dest IP	This field displays the destination IP addresses to which this rule applies.
Service	This field displays the protocol (All, TCP, UDP, TCP/UDP, ICMP, ICMPv6, 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.

Table 69 Security > Firewall > Rules

13.5.1 Add New ACLRule Screen

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

		Add New A	CL Rule	
Re. None				
Ome	<u> 1</u>			
Select Source I* Acidhem	Ipecitor Added			
Source In Address	Concern Concerne			7prets length
Select Deutection Device	ipector Ad	kirwa		
Ografication P Address				April 1997
P Type:	64			
Select Service	Specific Service			
10,000	345			
Cuttom Source Dod	Ronge	14		
Euritors Californiton Fort	Ranse	1		
Policy	ACCEPT			
Director	WANHALAN.			
Chapter Bate (Init	0			
		Conserva-	and Strong	(52.3
An Anna Ing Kalawa				
C 10 040 04-03 04 04 04		Add Ne.	villate.	

Figure 143	Security > Firewall > Access Control > Add New ACL Rule

LABEL	DESC RIPTIO N
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 IP Address	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 Spec ific 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.

Table 70 Security > Firewall > Access Control > Add New ACL Rule

LABEL	DESC RIPTIO N
IP Туре	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 (AIL, TC P/ UDP, TC P, UDP, IC MP, or IC MPv6) 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.
Custom Destination Port	This is a single port number or the ending port number of a range that defines your rule.
TCP Flag	Select the TCP Flag (SYN, ACK, URG, PSH, RST, FIN).
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 IAN to apply the rule to traffic from WAN to LAN. Select IAN 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 IAN to Router to apply the rule to traffic from LAN to router.
Enable Rate Limit	Click to enable (switch turns blue) the setting of maximum number of packets per maximum number of minute/second to limit the throughput of traffic that matches this rule. If not, the next item will be disabled.
Scheduler Rules	
packet(s) per (1-512)	Enter the maximum number of $packets$ (1-512) $perminute/second$.
Add New Rule	Select a schedule rule for this ACL rule from the drop-down list box. You can configure a new schedule rule by clicking Add New Rule .
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

Table 70 Security > Firewall > Access Control > Add New ACL Rule (continued)

13.6 DoS

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 the **DoS** screen to activate protection against DoS attacks.

Click Security > Fire wall > DoS to display the following screen.

Figure 144 Security > Firewall > DoS

- excitation and adding
Apply

IABEL	DESC RIPIIO N
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.

Table 71 Security > Firewall > DoS

13.7 Fire wall Technical Reference

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

13.7.1 Fire wall 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
 WAN to LAN
- LAN to WAN
 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.

13.7.2 Guidelines For Security Enhancement 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.

13.7.3 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.

C HAPTER 14 MAC Filter

14.1 MAC Filter Overview

You can configure the Zyxel Device to permit access to clients based on their MAC addresses in the **MAC Filter** screen. This applies to wired and wireless connections. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the LAN client to configure this screen.

14.2 MAC Filter

Enable **MAC Address Filter** and add the host name and MAC address of a LAN client to the table if you wish to allow or deny them access to your network. You can choose to enable or disable the filters per entry; make sure that the check box under **Active** is selected if you want to use a filter. Select **Sec unity** > **MAC Filter**. The screen appears as shown.

Yuu oonii oopiiwiin oddaalais ta sadwiit	onigure line aver wines and science everyned of the is electrocological	During la porrel accession d'un la compara de Roma Parent de de porrel d'actes à d'actes d'internet de actes e la complete d'actes de la actes e la complete de la porrel d'hac	concrete line MAX construction in a AND Note of chapter is with the Antonia Con- construction of chapters is a statistic is 10000 When	Criffer surch a His and Inscient. The solar's SCROOCC 22 You need
an ina	A	• Paper C Data party	ne sine and some	
ad then	e Mode	🖷 Kow 🗤 Keny		
Sel	Active	lict kione	MAC Address	told share Delete
-				

Figure 145 Security > MAC Filter

IABEL	DESC RIPIIO N
MAC Address Filter	Select Enable to activate the MAC filter function.
MAC Restrict Mode	Select Allow to only permit the listed MAC addresses access to the Zyxel Device. Select Deny to permit anyone access to the Zyxel Device except the listed MAC addresses.
Add New Rule	Click this button to create a new entry.
Set	This is the index number of the MAC address.
Active	Select $Active$ to enable the MAC filter rule. The rule will not be applied if $Allow$ is not selected under MAC Restrict Mode.
Host Name	Enter the host name of the wireless or LAN clients that are allowed access to the Zyxel Device.
MAC Address	Enter the MAC addresses of the wireless or LAN clients that are allowed 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.
Delete	Click the Delete icon to delete an existing rule.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

Table 72 Security > MAC Filter

14.2.1 Add New Rule

You can choose to enable or disable the filters per entry; make sure that the check box under Active is selected if you want to use a filter, as shown in the example below. Select Security > MAC Filter > Add New Rule. The screen appears as shown.

Figure 146	Security	/ > MAC Filte	er > Add	New Rule
------------	----------	---------------	----------	----------

5-1	Active	nos/ Name	WAC Address	C Gelete
7	2	ad i	1603. 127 all T. Aw AS	0
2		Teal	we mi twi to the 2	0

The following table describes the labels in this screen.

IABEL	DESC RIPIIO N
Set	This is the index number of the MAC address.
Active	Select Active to enable the MAC filter rule. The rule will not be applied if Allow is not selected under MAC Restrict Mode .
Host Name	Enter the host name of the wireless or LAN clients that are allowed access to the Zyxel Device.
MAC Address	Enter the MAC addresses of the wireless or LAN clients that are allowed 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.
Delete	Click the Delete icon to delete an existing rule.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

C HAPTER 15 Parental Control

15.1 Overview

Use this screen to enable parental control and view parental control rules and schedules. Parental control allows you to limit the time users can access the Internet, and prevent users from viewing inappropriate content or participating in unauthorized online activities. These rules are defined in a Parental Control Profile (PCP).

15.2 The Parental Control Screen

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

Click Security > Parental Control to open the following screen.

Figure 147	Security >	Parental	Control
	/		

periodan visu etc	nino ort. 1 Po Analati, dielfis	r Torre Forts Book of Farry e ToreMol Contro Ptoll e/10	, menders her wedige og Fjirste gewälle herre hel	el de storn of t var une Amaña	oriano activatios 1 en el 20 proviles s	o antes
Seneral						
Fridmont, is	in a start a st	📕 marcula 👘 Dorg	The state of a weather the	a salar		
Pareima Co	antrol First	16(PCP)			* *	Ja New Fic
			2422220000000	200000	22.0223	

The following table describes the fields in this screen.

LABEL	DESC RIPTIO N
Parental Control	Select Enable to activate parental control.
Add New PCP	Click this if you want to configure a new parental control rule.
#	This shows the index number of the rule.

 Table 74
 Parental Control > Parental Control

Table 74	Parental Control > Parental Control (continued)
----------	---------------------------------------	------------

LABEL	DESC RIPTIO N
Status	This 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.
PCP Name	This shows the name of the rule.
Home Network User (MAC)	This shows the MAC address of the LAN user's computer to which this rule applies.
Internet Access Schedule	This shows the day(s) and time on which parental control is enabled.
Network Service	This shows whether the network service is configured. If not, None will be shown.
Website Blocked	This shows whether the website block is configured. If not, None will be shown.
Modify	Click the Edit icon to go to the screen where you can edit the rule.
	Click the De le te icon to delete an existing rule.
Cancel	Click Cancel to exit this screen without saving.
Apply	Click Apply to save your changes back to the Zyxel Device.

15.2.1 Add New Parental Control Rule

Click Add New PCP in the Parental Control screen to add a new PCP rule. Use this screen to configure a restricted access schedule and/or URL filtering settings to block the users on your network from accessing certain websites.

			677. 		
lichona					
Alt de Research and the	dia norma	Charles & Smith	fa hay controlog and	1112.4 de	
President and		fatter 1	9. 9	* ***	
Nde Cal					
	Jan 2	912 Fabrica		Soleka	
100001006	ana.				
Contract Access 1	onegoe				
Des.	MADE.		in Mar (144)	9	
Sec.	(mex.)	La March Part	(n)(35)(3)	0	
Sec.		as (Mac) Ty) Minimuten	0/8/8		
Der. New (dert feet)		an (And) Ty /	(j) ((ar) (ar)	-	
Den Den (ant hat Telan da ben) - e	(me) + 2 	La II Mac II Ty /	9 (đ) (đ)		
Der. Der (der fan) Selaurik bergine 1000-100000 10		an (And) Ty ((j) ((de)) (de)		
Der- Pro (ann fuit) Islan - A born (an ann-ann anns an	~	La II Mac II Ty /			
Den Den (den hal) Geboork bestion Henroe (den hal)		44 (1 And 1 Ty) consumbras	() (ar) (ar)		
Den Den (son har) Indonek berei en Indonek berei en	ree.	44 (1 AMC) Ty /	() (45) (45)		
De- Per (an fait Indones and a anguer anno an anguer an anguer an an anguer an anguer an a		19 10 AME (1) Ty /	n ((ar)(ar)	1	
Des Des (ant hat Indones la Section Indones la Section Indones la Section Indones la Section	ingen	44 (1 AMC) Ty / cross.tra	() ((20)) (20)		erito y con sua tanta tanta
Der- Ter (an fait) Refer de Service Refer de Service Refer de Service Refer de Service	lance for	La CANCO Tra	(n) (der () (der) (new me		

Figure 148 Parental Control > Parental Control > Add New PCP

The following table describes the fields in this screen.

Table 75 Parental Control > Parental Control > Add New PCP

LABEL	DESCRIPTION
General	
Active	Select \mathbf{Enable} to activate this parental control rule.

LABEL	DESCRIPTION
Parental Control Profile Name	Enter a descriptive name for the rule.
Home Network User	Select the LAN user that you want to apply this rule to from the drop-down list box. If you select $Custom$, enter the LAN user's MAC address. If you select All, the rule applies to all LAN users.
Rule List	In Home Network User , select Custom , enter the LAN user's MAC address, then click the + sign to enter a computer MAC address for this PCP. Up to five are allowed. Click the - sign to remove one.
Internet Access Sche	dule
Day	Select the days that you want the Zyxel Device to perform parental control.
Time	Drag the time bar to define the time that the LAN user is allowed access.
Add New Time	Click this to add a new time bar. Up to three are allowed.
Network Service	
Network Service Setting	If you select \mathbf{Block} , the Zyxel Device prohibits the users from viewing the Web sites with the URLs listed below.
	If you select ${\bf Allow},$ the Zyxel Device blocks access to all URLs except the ones listed below.
Add New Service	Click this to show a screen in which you can add a new service rule. You can configure the Add New Service , Protocol , and Port of the new rule.
#	This shows the index number of the rule. Select the checkbox next to the rule to activate it.
Protocol	This shows the protocol of the rule. Choices are TCP , UDP , or TCP& UDP .
Port	This shows the port of the rule.
Modify	Click the Edit icon to go to the screen where you can edit the rule.
	Click the Delete icon to delete an existing rule.
Site/URL Keyword	
Block or Allow the Web Site	If you select Block the Web URLs , the Zyxel Device prohibits the users from viewing the Web sites with the URLs listed below.
	If you select Allow the Web URLs , the Zyxel Device blocks access to all URLs except the ones listed below.
#	This shows the index number of the rule.
Website	This shows the URL of web site or URL keyword to which the Zyxel Device blocks or allows access.
Modify	Click the Edit icon to go to the screen where you can edit the rule.
	Click the Delete icon to delete an existing rule.
Add	Click Add to show a screen to enter the URL of web site or URL keyword to which the Zyxel Device blocks or allows access.
ОК	Click \mathbf{OK} to save your settings back to the Zyxel Device.
Cancel	Click Cancel to return to the previous screen without saving any changes.

Table 75Parental Control > Parental Control > Add New PCP

C HA PTER 16 C e rtific a te s

16.1 Certificates 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.

16.1.1 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 16.2 on page 201).
- Use the **Thusted CA** screen to save the certificates of trusted CAs to the Zyxel Device. You can also export the certificates to a computer (Section 16.3 on page 205).

16.2 Local Certificates

Use this screen to view the Zyxel Device's summary list of certificates, generate certification requests, and import 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 149 Security > Certificates > Local Certificates

iadiona Pristaria, Spanito	analtia la PEN Isroa	n:			
 Provide station provide Oncovide Active Stations 	θφ.				
			ting Control	vi	dicch de Foole Skyled
manost etc.	-publicati	(Dates)	A called response	-9556 to:	w.odity

Table 76	Security >	Certificates >	Local	Certificates
1001070	000001119 -	Connicator	LOCOI	Connicatos

LABEL	DESC RIPTIO N		
Replace Private Key/Certificate file in PEM format			
Private Key is protected by 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 Expired! message if the certificate is about to expire or has already expired.		
Modify	Click the $View$ icon to open a screen with an in-depth list of information about the certificate.		
	For a certification request, click Load Signed to import the signed certificate.		
	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.		

16.2.1 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.



love the 2/14 Device gets for the came, or activity	este o certitoci on reguer. To o este o set e nome statuți o cleve nome, and the bea	hoote coning request you need to enter a write source you do the face coefficients
Every survive and		
and such Kennel	🗇 Auto 🐞 Guiromay	
Octorbeiller klavik		
COMPOSITION (CONTRACT)		
Contriviporon brame C	125 junied Sicher	

Table 77	Create	Certificate	Request
----------	--------	-------------	---------

IABEL	DESC RIPIIO N
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 email address in the field provided. The domain name or email address can be up to 63 ASCII characters. The domain name or email 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.
ОК	Click OK to save your changes.

16.2.2 View Certificate Request

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).

Click the View icon in the Local Certificates screen to open the following screen.

Figure 151	Certificate Request: View	v
------------	---------------------------	---

Continue datas	
11/14	Tec:
71	ЯХ,
HAT:	- Sector State Sector 2010 2122/2010/02/2017/2017/2017 1:00:00
e tracte	
1 - J V 8. 7	hts "Nord-Lei Limicherbook D.C. Hoszofi, C.C.B. (K. Hoszofi, C.C. Baskers Zoneslaft Salavatzekier, Horizofi, K. Basker, B. Salavatzekier, Status Zoneslaft Salavatzekier, Horizofi, K. Basker, B. Salavatzekier, S. Salavatzekier, Salavatzekier, Salavatzekier, Salavat
gn≻giavian	CONTRACTOR INVOLVED AND A CONTRACT A

	Table 78	Certificate Request: View
--	----------	---------------------------

LABEL	DESC RIPIIO N
Name	This field displays the identifying name of this certificate.
Туре	This field displays general information about the certificate. \mathbf{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 email 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.

IABEL	DESC RIPTIO N
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.

Table 78 Certificate Request: View (continued)

16.3 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, which means you do not need to import any certificate that is signed by one of these certification authorities.

Note: A maximum of 4 certificates can be added.

Figure 152	Security > Certificates > Trusted CA
------------	--------------------------------------

			💼 mileri Card
Nores	subject :	type	waddy

The following table describes the labels in this screen.

IABEL	DESC RIPTIO N
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 a unique subject information.
Туре	This field displays general information about the certificate. ${f c}{f a}$ 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.

Table 79 Security > Certificates > Trusted CA

16.4 Import Trusted CA Certificate

Click **Import Certificate** in the **Thusted 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.

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

Figure 153 Trusted CA > Import



The following table describes the labels in this screen.

LABEL	DESC RIPIIO N
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.
ОК	Click this to save the certificate on the Zyxel Device.
Cancel	Click this to exit this screen without saving.

Table 80 Security > Certificates > Trusted CA > Import

16.5 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 > Thusted CA to open the Thusted CA screen. Click the View icon to open the View Certificate screen.

Figure 154	Trusted CA: View
------------	------------------

Carlor and Long	et C.e.	
Saróy:	x0.405.73.261	
Barris - Marca A Estado Salación (A) estado	Constraints of the second state of the seco	I

Table 81	Trusted CA: View	

IABEL	DESC RIPIIO N
Name	This field displays the identifying name of this certificate.
	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form.
	You can copy and paste the certificate into an email 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).
Back	Click this to return to the previous screen.

16.6 Certificates Technical Reference

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

Certific a tion 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.

16.6.1 Verify 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 155 Certificates on Your Computer

<u> </u>	Landon-Office.or	
Certificates		

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.

Second (Malk Confiction	Path
Show (cxits Feel) Subject (see Pablic (s	Situa Stran Kisa (Hize Intel) Digital Signadure , Cartificate Signing) Situate Type=CA, Fain Length Core that BOAT 2286 7980 PP32 52P4 obtic A2 121
	gav to No

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.



C HAPTER 17 Voice

17.1 Overview

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

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

17.1.1 What You Can Do in this Chapter

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

- Use the **Voice Mode** screen to enable VoIP or VoLTE services on the Zyxel Device (Section 17.2 on page 210).
- Use the SIP Account screen to set up information about your SIP account, control which SIP accounts the phones connected to the LTE Device use and configure audio settings such as volume levels for the phones connected to the ZyXEL Device (Section 17.3.1 on page 211).
- Use the SIP Service Provider screen to configure the SIP server information, and the numbers for certain phone functions (Section 17.3.3 on page 215).
- Use the **Phone** screen to change settings that depend on which region of the world the Zyxel Device is in (Section 17.4 on page 219).
- Use the Call Rule screen to set up shortcuts for dialing frequently-used (VoIP) phone numbers (Section 17.5 on page 219).
- Use the Call History screen to view a call history list(Section 17.6 on page 220).

17.2 Voice Mode

Use this screen to enable VoIP or VoLTE services on the Zyxel Device. To access this screen, click **Voice > Voice Mode**.

Figure 157 Voice > Voice Mode

Voice Mode			
Places select cincide se	Preparatives to holds werkte of the SveriDers of		
-classica	🖶 bernen Obrennen		
-cHe			
Make S <mark>aM</mark> ae inchorged	i nydey Almosot.		
	Concel Apple		

able 82	Voice > Voice Moc	le

IABEL	DESC RIPTIO N
Configuration	
Voice Service	Select \mathbf{Enable} to activate VoIP or VoLTE on the Zyxel Device.
Apply	Click Apply to save the settings.
Cancel	Click Cancel to start configuring this screen again.

17.3 SIP

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

17.3.1 SIPAccount

You can make calls over the Internet using VoIP technology. For this, you first need to set up a SIP account with a SIP service provider. The Zyxel Device uses a SIP account to make outgoing VoIP calls, and to check if an incoming call's destination number matches your SIP account's VoIP number. In order to make and receive VoIP calls, you need to enable and configure a SIP account, and then map it to a phone port. The SIP account contains information that allows your Zyxel Device to connect to your VoIP service provider.

To access this screen, click Voice > SIP > SIP Account.

Figure 158	Voice > SIP > SIP Account.
------------	----------------------------

			SIP		
P Acc		Tokolar			
ir isida telitika	n to make non-ming 1. This for Routerton	nore call and d'Affecte Nove betwee Nacolumn	antis essential, four moy need to a be writt SP Service Provider	ons, how Siften to croker for	ne silver:
ir olda Self Se	e to more internery a Telador Rouxeron Costes	nore can a raid of acco Assue to total handbed Stractory	um 1 eller Fill, för mar nesa ta 1 be virt SF Sandas Freddas Sandas Freddas	onu hour XI ⁿ erices croiserte Anno 11 desemb	netikeet

IABEL	DESC RIPTIO N
#	This is the index number of the entry.
Enable	This shows whether the SIP account is activated or not. A yellow bulb signifies that this SIP account is activated. A gray bulb signifies that this SIP account is activated.
SIP Account	This shows the name of the SIP account.
Service Provider	This shows the name of the SIP service provider.
Account Number	This shows the SIP number.
Modify	Click the Modify icon to configure the SIP account.

Table 83 Voice > SIP > SIP Account

17.3.2 SIP Account Entry Edit

You can configure a SIP account. To access this screen, click the **Modify** icon.

	SIF Account Entry Edit		
Sif-Account Scieption			
20 Annual Develop			
SP Service Provider Association)		
Withous devotes a r	Margelle -		
General			
() how the second			
28 Printer Tracker	Charge and		
Avhenicotor			
- deriverse	Wisequille.		
Company .	(the second sec		
111 fype			
$T = T_{CD} +$	1992 ()	- 28	
Kinter Fridaers			
Henry Versenator (see	910.6	18	
NOTION CONTRACTOR	4-0		
time Machine Constraints	Will w		
Speaking Palmin Denied	efabr		
Lease graves the me	etada.		
📮 football (* 1991) "Here Constantion			
In the set of the proton service former	ent.		
Collfoolves			
📴 bern State 🗉			
🗖 krabis tost Oranag			
US Abreaktoww	23		Landstein
(The device for the use (244)			
Warning: Type of all of the proceeding of	d haladan dha arwana ad par		
Destroine the Second Sec	i		

Figure 159 Voice > SIP > SIP Account > SIP Account Entry Edit

|--|

IABEL	DESC RIPHO N	
SIP Service Provider Association	on	
SIP Service Provider Associated with	Select the check box to use this account. Clear it to not use this account.	
General		
SIP Account Number	Enter your SIP number. In the full SIP URI, this is the part before the @ symbol. You can use up to 127 printable ASCII characters.	
Authentication		
User Name	Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII characters.	

LABEL	DESC RIPTIO N		
Password	Enter the password for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII characters.		
URL Type			
URL Type	Select whether or not to include the SIP service domain name when the LTE Device sends the SIP number.		
	SIP - include the SIP service domain name.		
	TEL- do not include the SIP service domain name.		
Voice Features			
Primary Compression Type	Select the type of voice coder/decoder (codec) that you want the LTE Device to use.		
Туре	G.711 provides higher voice quality but requires more bandwidth (64 kbps).		
Third Compression Type	• G.729 provides good sound quality and reduces the required bandwidth to 8 kbps.		
	• G.711a is typically used in Europe.		
	• G.711u is typically used in North America and Japan.		
	• G.726-32 operates at 16, 24, 32 or 40 kbps.		
	• G.722 operates at 6.3 kbps or 5.3 kbps.		
	When two SIP devices start a SIP session, they must agree on a codec.		
	Select the LTE Device's first choice for voice coder/decoder.		
	Select the LTE Device's second choice for voice coder/decoder. Select None if you only want the LTE Device to accept the first choice.		
	Select the LTE Device's third choice for voice coder/decoder. Select None if you only want the LTE Device to accept the first or second choice.		
Speaking Volume Control	Select the loudness that the LTE Device uses for speech that it sends to the peer device. Choices are Minimum, Middle, and Maximum.		
Listening Volume Control	Select the loudness that the LTE Device uses for speech that it receives from the peer device. Choices are Minimum, Middle, and Maximum.		
Enable G. 168	Select this if you want to eliminate the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.		
Enable VAD	Select this if the LTE Device should stop transmitting when you are not speaking. This reduces the bandwidth the LTE Device uses.		
Call Features			
Send Caller ID	Select this if you want to send identification when you make VoIP phone calls. Clear this if you do not want to send identification.		
Enable Call Waiting	Select this to enable call waiting on the LTE Device. This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.		
Call Waiting Reject Timer	Specify a time of seconds that the LTE Device waits before rejecting the second call if you do not answer it.		
Enable Do Not Disturb (DND)	Select this to turn the do not disturb feature on. This has the Zyxel Device reject all calls destined to the phone line.		
Active Incoming Anonymous Call Block	Select this to have the phone not ring for incoming calls with caller ID deactivated.		
ОК	Click this to save your changes.		
Cancel	Click this to exit this screen without saving.		

Table 84	Voice > SIP > SIP	Account > SIF	Account Entry	/ Edit ((continued)
		/ 00000111 - 011	7.0000111 En Ini		

17.3.3 SIP Service Provider

Use this screen to view the SIP service provider information on the Zyxel Device. A SIP provider offers Internet call services using VoIP technology. You may need to consult your SIP service provider for the following settings. To access this screen, click **Voice > SIP > SIP Service Provider**.

Figure 160 Voice > SIP > SIP Service Provider

		SI	P		
4	nan af la <mark>f service fromber</mark>				
	larvoa irokoa presidender dir telepisetings finis contiguiertor p	oning meneropoising von e wuche van Procedurator with	e <mark>chinalo</mark> gy, hou may reed to con Wir Account	ne poer si niemice, novo	112-101
20	28 Severe Brocker Brow-	. SP Fray Serve Address	POWERses debry	NP Stroke Doctoba	Worth
	Concernant and	There are block			

The following table describes the labels in this screen.

IABEL	DESC RIPHO N
#	This is the index number of the entry.
SIP Service Provider Name	This shows the name of the SIP service provider.
SIP Proxy Server Address	This shows the IP address or domain name of the SIP server.
Register Server Address	This shows the IP address or domain name of the SIP register server.
SIP Service Domain	Enter the SIP service domain name. In the full SIP URI, this is the part after the @symbol. You can use up to 127 printable ASCII Extended set characters.
Modify	Click the Modify icon to configure the profile of SIP service provider settings.

Table 85 Voice > SIP > SIP Service Provider

17.3.4 Provider Entry Edit

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

Figure 161	Voice > SIP >	SIP Service	Provider: Edit
------------	---------------	-------------	----------------

	Provider Station 2019	
10 James Francisco Sales - 10		
and the first state of the second state of the	and a	
(and	0.03	
Margaren and		
an and a strategy s		
1100.00	1000	10.00
Witness in our water out	STRAIN L	
any management of the	1.41	100.00
In carding of free strength	CERTIFIC .	
of Manufacture and Party	14	144.144
Wirds Law	0.0000	
and Legend		
10.22 M 104 August Stat		
VOP IOP TOBS		
Bitte internet ogen i met att	and get	
Record Inter Story Reader		
	constant and a second	
Laffrance many		
and a state of the		
man and an and	4.04	Cash-Area
the Definition of the		
BYT CORPORE		
	100 m	
hate	122.4	1000
eter was		11.77
100 2444	1 million	
risson to e		
100.000	- Weiter - Contraction - Contr	
age and a desire		
BILLER COMPANY		
Pers Option		
and the book of the	interior in the second s	
ine (ng		
ALC: NAME OF TAXABLE PARTY.	14)	144
and the second second		3.90
Trans Series		
An and the Paperson of Andrea	10	(Protocore)
and the second states of all	101	107040-001
Set and a set	74.	101 Md annual
and the second second	14 C	100.000.0000
Dusting Informal Sales Ion		
and the second second second	* C	1.000
D/D SW-		
Second and Second		
	Carles A Carlos	

Table 86	Voice $> S$	SIP > SIF	Service	Provider:	Fdit
		JII / JII			LUII

IABEL	DESC RIPTIO N
General	
SIP Service Provider	Select this if you want the Zyxel Device to use this SIP provider. Clear it if you do not want the Zyxel Device to use this SIP provider.
SIP Service Provider Name	Enter the name of your SIP service provider.
SIP Local Port	Enter the Zyxel Device's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
SIP Proxy Server Address	Enter the IP address or domain name of the SIP server provided by your VoIP service provider. You can use up to 95 printable ASCII characters. It does not matter whether the SIP server is a proxy, redirect or register server.
LABEL	DESC RIPTIO N
---------------------------------	--
SIP Proxy Server Port	Enter the SIP server's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
SIP REGISTAR Server Address	Enter the IP address or domain name of the SIP register server, if your VoIP service provider gave you one. Otherwise, enter the same address you entered in the SIP Server Address field. You can use up to 95 printable ASCII characters.
SIP REGISTAR Server Port	Enter the SIP register server's listening port number, if your VoIP service provider gave you one. Otherwise, enter the same port number you entered in the SIP Server Port field.
SIP Service Domain	Enter the SIP service domain name. In the full SIP URI, this is the part after the @ symbol. You can use up to 127 printable ASCII Extended set characters.
RFC Support	
PRACK (RFC 3262)	RFC 3262 defines a mechanism to provide reliable transmission of SIP provisional response messages, which convey information on the processing progress of the request. This uses the option tag 100rel and the Provisional Response ACKnowledgement (PRACK) method.
	Select Supported or Required to have the Zyxel Device include a SIP Require/ Supported header field with the option tag 100rel in all INVITE requests. When the Zyxel Device receives a SIP response message indicating that the phone it called is ringing, the Zyxel Device sends a PRACK message to have both sides confirm the message is received.
	If you select $\mathbf{Supported}$, the peer device supports the option tag 100rel to send provisional responses reliably.
	If you select $\mathbf{Re} \mathbf{quine} \mathbf{d}$, the peer device requires the option tag 100rel to send provisional responses reliably.
	Select Disabled to turn off this function.
VoIP IOP Flags - Select VoIP ir	nter-operability settings.
	Replace dial digit '#' to '%23' in SIP messages.
	Remove ':5060' and 'transport=udp' from request-uri in SIP messages.
	Remove the 'Route' header in SIP messages.
	Don't send re-Invite to the remote party when there are multiple codecs answered in the Session Description Protocol (SDP).
	Remove the 'Authentication' header in SIP ACK messages.
Bound Interface Name	
Bound Interface Name	If you select AnyWAN , the Zyxel Device automatically activates the VoIP service when any WAN connection is up.
	If you select MultiWAN , you also need to select the pre-configured WAN connections. The VoIP service is activated only when one of the selected WAN connections is up.
Outbound Proxy	· · · · · · · · · · · · · · · · · · ·
Enable	Select this if your VoIP service provider has a SIP outbound server to handle voice calls. This allows the Zyxel Device to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off any SIP ALG on a NAT router in front of the Zyxel Device to keep it from re-translating the IP address (since this is already handled by the outbound proxy server).
Outbound Proxy Address	Enter the IP address or domain name of the SIP outbound proxy server.
Outbound Proxy Port	Enter the SIP outbound proxy server's listening port, if your VoIP service provider gave you one. Otherwise, keep the default value.
Use DHCP Option 120 first	Select this to have the Zyxel Device use DHCP Option 120 first.

 Table 86
 Voice > SIP > SIP Service Provider: Edit (continued)

Tailal a O/	1/-:> CID		• • · · · · • •	D	F -111	(
1 a Die 86	VOICE > SIP	> 215 S	service	Provider:	Ealt	(continuea)

LABEL	DESC RIPTIO N
RTP Port Range	·
Start Port	Enter the listening port number(s) for RTP traffic, if your VoIP service provider gave you this information. Otherwise, keep the default values.
End Port	To enter one port number, enter the port number in the Start Port and End Port fields.
	To enter a range of ports,
	 enter the port number at the beginning of the range in the Start Port field. enter the port number at the end of the range in the End Port field.
DTMF Mode	Control how the Zyxel Device handles the tones that your telephone makes when you push its buttons. You should use the same mode your VoIP service provider uses.
	RFC 2833 - send the DTMF tones in RTP packets.
	Inb and - send the DTMF tones in the voice data stream. This method works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.726) can distort the tones.
	SIPInfo - send the DTMF tones in SIP messages.
Transport Type	
Transport Type	Select the transport layer protocol \mathbf{UDP} or \mathbf{TCP} (usually UDP) used for SIP.
Ignore Direct IP	Select Enable to have the connected devices accept SIP requests only from the SIP proxy/register server specified above. SIP requests sent from other IP addresses will be ignored.
FAX Option	This field controls how the Zyxel Device handles fax messages.
QoS Tag	·
SIP DSCP Mark Setting	Enter the DSCP (DiffServ Code Point) number for SIP message transmissions. The Zyxel Device creates Class of Service (CoS) priority tags with this number to SIP traffic that it transmits.
RTP DSCP Mark Setting	Enter the DSCP (DiffServ Code Point) number for RTP voice transmissions. The Zyxel Device creates Class of Service (CoS) priority tags with this number to RTP traffic that it transmits.
Timer Setting	
SIP Register Expiration Duration	Enter the number of seconds your SIP account is registered with the SIP register server before it is deleted. The Zyxel Device automatically tries to re-register your SIP account when one-half of this time has passed (The SIP register server might have a different expiration).
SIP Register Fall Re-try timer	Enter the number of seconds the Zyxel Device waits before it tries again to register the SIP account, if the first try failed or if there is no response.
Session Expires [SE]	Enter the number of seconds the Zyxel Device lets a SIP session remain idle (without traffic) before it automatically disconnects the session.
Min-SE	Enter the minimum number of seconds the Zyxel Device lets a SIP session remain idle (without traffic) before it automatically disconnects the session. When two SIP devices start a SIP session, they must agree on an expiration time for idle sessions. This field is the shortest expiration time that the Zyxel Device accepts.
Dialing interval selection	
Dialing interval selection	Enter the number of seconds the Zyxel Device should wait after you stop dialing numbers before it makes the phone call. The value depends on how quickly you dial phone numbers.
Enable DNS SRV	Select this to have the Zyxel Device query your ISP's DNS server for a list of any available SIP servers that it maintains. This is useful if your static SIP server experiences difficulties, making it hard for your IP phone users to make SIP calls.

Table 86 Voice > SIP > SIP Service Provider: Edit (continued)

LABEL	DESC RIPTIO N
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

17.4 Phone

Use this screen to configure settings that depend on which region of the world the Zyxel Device is in. Selecting the region where the device is physically located improves the quality of phone calls. To access this screen, click **Voice > Phone**.

Figure 162 Voice > Phone

	Phone	
	е парел за слидови и обслед роком рате сирто и отога соо	
Region Colory	the firmed their editorial	
Diddorige Model	Bran Dec	1
Source, the reput tells p	echonged roomeed for wood comparies to take rational and	
	Council Apple	

The following table describes the labels in this screen.

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

Table 87 Voice > Phone

Note: You need to reboot the device after changing the region settings for it to take effect.

17.5 Call Rule

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

Figure 163	Voice > Call Rule
------------	-------------------

n verbangene in inder in Nationalise state	ere ore availed to be negative to use. Averand that succedies of Available	ar dala yan sana. Tarixiyo ng silan sana ila di Bary sana
		Star 10 Sec
-	1.000	1-colpitur
04		
131		
ue l		
(A)		
0.0		
16		
ώr.		
en i		
69.5		

Table 88 Voice > Call Rule	
IABEL	DESC RIPHO N
Keys	This field displays the speed-dial number you should dial to use this entry.
Number	Enter the SIP number you want the Zyxel Device to call when you dial the speed-dial number.
Description	Enter a short description to identify the party you call when you dial the speed-dial number. You can use up to 127 printable ASCII characters.
Clear All Speed Dials	Click this button to remove all speed dials saved.
Apply	Click this to save your changes and to apply them to the Zyxel Device.
Cancel	Click this to set every field in this screen to its last-saved value.

Table 88 Voice > Call Rule

17.6 Call History

The Zyxel Device logs calls from or to your SIP addresses. This screen allows you to view a summary of received, dialed and missed calls and a call history list. You can also view detailed information on each outgoing and incoming call.

17.6.1 Call History Screen

To access this screen, click Voice > Call History.

Figure 164 Voice > Call History

		Call	listory		
Cor Here	er Children (
(Cal. 14	ore page those the inform	after of pre-kout call,			
Coulde:	AL	•		Charitht, Rebeil	and the second
			369 C	inni, Yalaria 1	, Morris
Tess	Dale Horse Humb	e Those Device	Outgoing Sunster	Datafier (Hit series)	$\mathcal{H}od\mathbb{F}_{\mathbb{F}}$

The following table describes the labels in this screen.

IABEL	DESC RIPTIO N
Classify	Select the type of the calls. The call types are: Incoming, Outgoing and Missed.
Clear List	Click this button to remove all entries from the call history list.
Refresh	Click this button to renew the call history list.
Export	Click Export to download a call history list.
Туре	This displays the type of the calls.
Date	This displays the date when the calls were made.
Name	This displays the SIP account you called.
Number	This displays the SIP number you called.
Phone Device	This field displays the name of a phone port on the Zyxel Device.
Outgoing Number	This displays how many calls originated from you that day.
Duration	This displays how long the current call has lasted.
Modify	Click the Modify icon to make changes to the call history.

Table 89 Voice > Call History

17.6.2 Call Summary Screen

The Zyxel Device logs calls to or from your SIP addresses. This screen allows you to view the summary of received, dialed and missed calls. To access this screen, click **Voice > Call History > Call Summary**.

Figure 165 Voice > Call History > Call Summary

			Call Histor	Y	
	Coll larger	1			
		Server			
ina ing	p + žirnes				Tetted, Clored

LABEL	DESC RIPTIO N
Refresh	Click this button to renew the call history list.
Clear All	Click this button to remove all entries from the call history list.
Date	This is the date when the calls were made.
Total Calls	This displays the total number of calls from or to your SIP numbers that day.
Outgoing Calls	This displays how many calls originated from you that day.
Incoming Calls	This displays how many calls you received that day.
Missing Calls	This displays how many incoming calls were not answered that day.
Total Duration	This displays how long all calls lasted that day.

Table 90 Voice > Call History > Call Summary

C HAPTER 18 Log

18.1 Log Overview

These screens allow you to determine the categories of events and/or alerts that the Zyxel Device logs and then display these logs or have the Zyxel Device send them to an administrator (through email) or to a syslog server.

18.1.1 What You Can Do in this Chapter

- Use the System Log screen to see the system logs (Section 18.2 on page 224).
- Use the Security Log screen to see the security-related logs for the categories that you select (Section 18.3 on page 224).

18.1.2 What You Need To Know

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

Alerts and Logs

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

Syslog Overview

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

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

CODE	SEVERIIY
0	Emergency: The system is unusable.
1	Alert: Action must be taken immediately.
2	Critical: The system condition is critical.
3	Error: There is an error condition on the system.
4	Warning: There is a warning condition on the system.

Table 91 Syslog Severity Levels



CODE	SEVERITY
5	Notice: There is a normal but significant condition on the system.
6	Informational: The syslog contains an informational message.
7	Debugging: The message is intended for debug-level purposes.

Table 91 Syslog Severity Levels

18.2 System Log

Use the System Log screen to see the system logs. You can filter the entries by selecting a severity level and/or category. Click System Monitor > Log to open the System Log screen.





The following table describes the fields in this screen.

IABEL	DESC RIPTIO N
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).
Email Log Now	Click this to send the log file(s) to the email address you specify in the Maintenance > Logs 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.

Table 92 System Monitor > Log > System Log

18.3 Security Log

Use the Security Log screen to see the security-related logs for the categories that you select. You can filter the entries by selecting a severity level and/or category. Click System Monitor > Log > Security Log to open the following screen.



View to the parts	e aeisan (-rais) Neo Rittinam	ed og for the outlegories f	iel yskiewet. Yns is	ch the the entropy choicing	Invitevel on d/Critegery
1. Mar	20	· Langer AL	-	Cleariton, Neter	A experies freelieshee
	fime.	Focility	Lavai	Calegory	//emoger

IABEL	DESC RIPTIO N
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).
Email Log Now	Click this to send the log file(s) to the email address you specify in the Maintenance > Logs 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.

Table 93 System Monitor > Log > Security Log

C HAPTER 19 Traffic Status

19.1 Traffic Status Overview

Use the Thaffic Status screens to look at the network traffic status and statistics of the WAN/LAN interfaces.

19.1.1 What You Can Do in this Chapter

- Use the WAN screen to view the WAN traffic statistics (Section 19.2 on page 226).
- Use the IAN screen to view the LAN traffic statistics (Section 19.3 on page 227).

19.2 WAN Status

Click System Monitor> Thaffic Status to open the WAN screen. The figures in this screen show the number of bytes received and sent through the Zyxel Device's WAN interface. The table below shows packet statistics for each WAN interface.





LABEL	DESC RIPIIO N
Refresh Interval	Select how often you want the Zyxel Device to update this 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	d
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 disabled.
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	d
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.

Table 94 System Monitor > Traffic Status > WAN

19.3 IAN Status

Click System Monitor > Thaffic Status > IAN to open the following screen. This screen allows you to view packet statistics for each LAN or WLAN interface on the Zyxel Device.

Figure 169	System Monitor > Traffic Status > LAN
rigure 109	System MOLIIO - ITUNIC STUDS - LAN

Traffic Status								
International Contraction of Contrac								
Comessarias	frof home been een to and	received horn each La	e Ipor (rdud	ing viewed are shadyed in the	rb sydry kiele.			
Second second	winder:							
kierzce -		IAN		249 NUM	39.6268			
Byles lost		107414		175	and the second sec			
Pytra 1	e Revelued	0.611	and .		59 C			
	at the		1.66	Sec. 10 and	47. W 81			
	100000	. Units	202	the second second				
- 30	ant (ruckel)	610	0	F	9			
		Deop	10		1			
Galantial Sectors		Dele	4.9	- N.	<u>ii</u>			
		. Para	11	8	1			
		Canyo		1. S.	1			

IABEL	DESC RIPTIO N
Refresh Interval	Select how often you want the Zyxel Device to update this screen.
Interface	This shows the LAN or WLAN 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 or WLAN interfaces.
Sent (Packets)	
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	S)
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.

 Table 95
 System Monitor > Traffic Status > LAN

C HAPTER 20 ARP Table

20.1 ARP Table Overview

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

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

20.1.1 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.

20.2 ARP Table

Use the ARP table to view the IPv4-to-MAC address mappings for each device connected to the Zyxel Device. The neighbor table shows the IPv6-to-MAC address mappings of each IPv6 neighbor. To open this screen, click **System Monitor** > **ARP Table**.



	AR	IP Table	
Audolaan Kasu Anadoola Aksa Kasa Aksa Aksa Liio Kasa Aksa Magaalaa (Kasa	u Romme o poblijster, na pro vodil kom rapping Imaa han a kredit kones Charlen na Orthan Imaa han a kredit kones Charlen in Orthan Imaa han a kredit kones hataan Idal - a nuw Fruitter is Meta as drasme op Gener neistige	ran hier of Houselford Act, (Haddred) to o dens, an the local area network a whose antifer neurosciencing in actions gay for the LOFA the resignation lists above the	olyanali oa stên. Men ia west anto da
nia Atribu			
	i Fyli Address	MAC Address	-Device
•	(Pel Address 192-192-1929	WAC Address User work to be	-Device
•	(Pet Address (Ag. Iso 1.42# (Pet No.1.73	MAC Address durae accento bi 7436 (color) e7	Device Lett BrD
e E Bookstadet-set	Peri Address Trisched Little Trisched Little	Search Ad droot (durwy don Africa: El 7 #36 "colocit" 67	Dovice In V In D
s S Real Solatorian	Prof Address (Ag. 165 1919) (1923) 5631-75 (1925) (MAC Address	Device Int Int Device
I Even Monter	Pv6 Address P52-5401-75 P52-5401-75 Pv6 Address Pv6 Address Pv6 Address	MAC Address MAC Address MAC Address do so feedbe so	Device tri tri tri tri tri tri tri tri

Table 96	System	Monitor >	ARP	Table
	5,510111		7 \(\)	1 GDIC

IABEL	DESC RIPTIO N
#	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 the device type to go to its configuration screen.

C HAPTER 21 Routing Table

21.1 Routing Table Overview

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

21.2 Routing Table

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	171	System	Monitor >	Routina	Table
rig uic	111	59310111		Roomig	TUDIC

Routing Table							
Rooting a based on th	e desired on active only	end the Zoost Denice Julia	ote divisió pa	n eleviedes	ervert.		
tes tes tes tes for chief out review and for the fire down house. He get aver accluses when as "" (red)", reset once also Bogs on the Letter Line etc. De geteway, Celocobe He hout Selectorize. De departie edited, and e modeled redrec (. Welke ellipe de chief agel (Localy over edit hous), there are shown to worker for the root e with conti							
Part Covering Topole							
ordination	adoway	today of work	Plag	noble	relations		
0.0.0.0	10.00.02.158	0,0,0		2.1	Voltard		
- 1961-22-18 E	0000	-12012M2012	191-22	11 A.	www.		
107.000	1,00.0	120 220 2 0	3.9	20	114		
012.342.340	0.0.0.0	255,255,255,255,0	1.4	- E	-04		
>>====101	innis	evotian	17		-2941		
A rooting root							
D	extection	Gotewoy	Fing	Metric	Interface		
· · · · · · · · · · · · · · · · · · ·	Var (Ma		10	204	1997		
	1050 stur	133	10	250	100		
	In The state	33	11.	236	. COL		
1	191 194		10 C	234	Access 0		
	(0)(00)	10	22	0	344.5		
	ABC/001		10	10	100		
	4878 (T28	122	20	0			
6	A1027121		10	ň.	194		
6	otechica		- U.	0	110.0		
1+50:0005	42+5+8-11-6-21-26	-		6	100		
Pacietore	or the state set of		1	1.11	and the second		
Land Street	a - La città - attaina a						
MARCH MARKET	or the state of the	14	- 66	. 6	160		
	Terrariant.		12	11	1.1		
	Inter 2	14		and a			
	Bach		- 33	114			
	100-0		102	and a	1.12		
	Horacia.						
	d month if i			100	0.0001.04		

Table 97	System Monitor >	Routing Table
----------	------------------	----------------------

IABEL	DESC RIPIIO N
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.

Table 07	System Monitor	> Douting Table	(continued)
	system Monitor		(coninued)

IABEL	DESC RIPTIO N
Flag	This indicates the route status.
	U-Up: The route is up.
	$!-\operatorname{Reject}$ The route is blocked and will force a route lookup to fail.
	G-Gateway: The route uses a gateway to forward traffic.
	H-Host: The target of the route is a host.
	R Reinstate: The route is reinstated for dynamic routing.
	D-Dynamic (redirect): The route is dynamically installed by a routing daemon or redirect.
	M-Modified (redirect): The route is modified from a routing daemon or redirect.
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	This indicates the name of the interface through which the route is forwarded.

C HAPTER 22 WIAN Station Status

22.1 WLAN Station Status Overview

Use this screen to view information and status of the wireless stations (wireless clients) that are currently associated with the Zyxel Device. Being associated means that a wireless client (for example, your computer with a wireless network card installed) has connected successfully to an AP (or wireless router) using the same SSID, channel, and WiFi security settings.

Click System Monitor > WLAN Station Status to open the following screen.

		WEAN Station Sta	los	
a da nasar san an				
a se se se se se se se	en .			
	See - See -	eas (asta)	and brand	 and the second sec
and the first sector				

Figure 172 System Monitor > WLAN Station Status

IABEL	DESC RIPTIO N
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.
Rate (Mbps)	This field displays the transmission rate of WiFi traffic between an associated wireless station and the Zyxel Device.
RSSI (dBm)	The RSSI (Received Signal Strength Indicator) field shows the WiFi signal strength of the station's wireless connection.
	The normal range is -30dBm to -79dBm. If the value drops below -80dBm, try moving the associated wireless station closer to the Zyxel Device to get better signal strength.

 Table 98
 System Monitor > WLAN Station Status

LABEL	DESC RIPIIO N
SNR	The Signal-to-Noise Ratio (SNR) is the ratio between the received signal power and the received noise power.
	The normal range is 15 to 40. If the value drops below 15, try moving the associated wireless station closer to the Zyxel Device to get better quality WiFi.
Level	This field displays a number which represents the strength of the WiFi signal between an associated wireless station and the Zyxel Device. The Zyxel Device uses the RSSI and SNR values to determine the strength of the WiFi signal.
	5 means the Zyxel Device is receiving an excellent WiFi signal.
	4 means the Zyxel Device is receiving a very good WiFi signal.
	3 means the Zyxel Device is receiving a weak WiFi signal.
	2 means the Zyxel Device is receiving a very weak WiFi signal.
	1 means the Zyxel Device is not receiving a WiFi signal.

C HAPTER 23 VoIP Status

23.1 Vo IP Status Screen

Click System Monitor > VoIP Status to open the following screen. You can view the VoIP registration, current call status and phone numbers in this screen.

Figure 173 System Monitor > VoIP Status

(100-sof	(E)			<u>.</u>		2	and and
ar slater	Paghtar 2.55	Fragestation	Reptionse	46	Vacaoga Andreg	Lost incoming Manager	cool Catpoin: Kenden
10	0		ŧ	Construction Construction	- 4.		
ini Webe General	e Hantor	Ballar S	an syn i Sada	e – 1990 Blanc Parch	10	nne Sallyso	Fris Nacion

The following table describes the labels in this screen.

Table 99	System	Monitor >	> VolP	Status
	59510111	101011101 -		510105

LABEL	DESC RIPTIO N
Poll Interval	Enter the number of seconds the Device needs to wait before updating this screen and then click Set Interval. Click Stop to have the Device stop updating this screen.
SIP Status	
Account	This column displays each SIP account in the Device.
Registration	This field displays the current registration status of the SIP account. You can change this in the Status screen. Registered - The SIP account is registered with a SIP server. Not Registered - The last time the Device tried to register the SIP account with the SIP server, the attempt failed. The Device automatically tries to register the SIP account when you turn on the Device or when you activate it. Inactive - The SIP account is not active. You can activate it in VoIP > SIP > SIP Account.

LTE Series User's Guide

LABEL	DESC RIPTIO N
Registration Time	This field displays the last time the Device successfully registered the SIP account. The field is blank if the Device has never successfully registered this account.
URI	This field displays the account number and service domain of the SIP account. You can change these in the VoIP > SIP screen.
Message Waiting	This field indicates whether or not there are any messages waiting for the SIP account.
Last Incoming Number	This field displays the last number that called the SIP account. The field is blank if no number has ever dialed the SIP account.
Last Outgoing Number	This field displays the last number the SIP account called. The field is blank if the SIP account has never dialed a number.
Call Status	
Account	This column displays each SIP account in the Device.
Duration	This field displays how long the current call has lasted.
Status	This field displays the current state of the phone call.
	Idle - There are no current VoIP calls, incoming calls or outgoing calls being made.
	Dial - The callee's phone is ringing.
	Ring - The phone is ringing for an incoming VoIP call.
	Process - There is a VoIP call in progress.
	DISC - The callee's line is busy, the callee hung up or your phone was left off the hook.
Call Type	This field displays the call direction type of the current VoIP call. Outgoing Call - It's a SIP VoIP call made by local phone ports, and this SIP account is able to issue a (SIP-based) call setup to the SIP account of remote peers for a VoIP call establishment. This (SIP-based) call setup signal is sent to the SIP server first, and then the SIP server would relay it to the target peer after correctly resolving and locating the target peer. During the call setup (signaling) phase, Calling state is displayed in the Status field, and it turns to InCall state once the call is successfully established.
	Incoming Call - It's a SIP VoIP call made or originated by remote SIP accounts to connect to this local SIP account. One or more local phone ports can be configured to receive this type of call, see the Incoming Number below, and all of them should begin to ring during the call setup (signaling phase), see the Status above. Once some remote SIP accounts start to ring one local phone, answer by off-hook to the call, and the call is successfully established. The other ringing local phone ports will stop ringing and turning to InCall state in the Status field.
	Internal Call - It's a local VoIP call between two different local phone ports. No SIP signaling is needed and thus no SIP server is involved to establish this type of call. This type of call is established via the Internal and Non-SIP local setup signaling procedure between the call-originating and call-terminating local phone ports. In general, one or more local phone ports can be designed to receive this type of call, and once any of the ringing phones answer the call, the other ringing ones will stop ringing. During the call setup phase (signaling phase), Calling state is displayed in Status field, and turns to InCall state once the call is successfully established.
Codec	This field displays what voice codec is being used for a current VoIP call through a phone port.
From Phone Port Type	This field displays the phone ports type used to originate, start, or create the current VoIP call. Type Two possible type values will be displayed here: SIP - For the current call which is categorized as Incoming Call in the Call Type filed, this field will show the type SIP. FXS - As for the other cases: Outgoing Call and Internal Call, this field will show the corresponding local phone port type: FXS, the legacy analog phone port on the device.

 Table 99
 System Monitor > VolP Status (continued)

LABEL	DESC RIPTIO N
To Phone Port Type	This field displays the phone ports type used to receive the current VoIP call. Three possible type Type values will be displayed here: SIP - For the current call which is categorized as Outgoing Call in the Call Type field, this field will show the type SIP. FXS and Unknown - As for the other cases: Incoming Call and Internal Call, this field will show the corresponding local phone port type: FXS, the legacy analog phone port on the device. While the call is established, this field shows Unknown during the call setup phase (signaling phase). This is because one or more local phone ports can be configured or designed to receive these two types of calls, see the Call Type above, and the local phone port will answer the call that hasn't been determined yet at that time.
Peer Number	This field displays the SIP number of the party that is currently engaged in a VoIP call through a phone port.
Phone Status	
Phone	This field displays the name of a phone port on the Device.
Outgoing Number	This field displays the SIP number that you use to make calls on this phone port.
Incoming Number	This field displays the SIP number that you use to receive calls on this phone port.
Hook Status	This field displays whether the phone is in the on or off hook status.

 Table 99
 System Monitor > VoIP Status (continued)

C HAPTER 24 Cellular WAN Status

24.1 Cellular WAN Status Overview

View the LTE connection details and LTE signal strength value that you can use as reference for positioning the Zyxel Device, as well as SIM card and module information.

24.2 Cellular WAN Status

To open this screen, click **System Monitor > Cellular WAN Status**. Cellular information is available on this screen only when you insert a valid SIM card in the Zyxel Device.

	Cellular WAN :	itatus
Vez te Researche Researche Statistics Laure montenes aus	ichte and development voor het voor development is Homoton Rationen tij konst angeween, bij waard	an una constructiva for positivita pina funda pina funda pina pina funda pina pina pina pina pina pina pina pin
terminate	Hora	2
Wodule Information		
International Advances		
SEW Status		
Ny Cold Pole	10me	
O Positinaugh Status		
Character de Conste	Lineary.	
Cellula: Status		
30000 (Co.		
Color Material Colored State	1254.0	
1.00		

239

- ,		•	
Service Intrimution			
Access Induidants			
Enc.	4.4		
120	DA .		
(H))	38		
Providen D	165		
$\{0,300,600,00\}, [0,70]$	-0.4		
U.S. Strand (White	405		
1808	6.6		
1.77	444		
8882	104		
ARCE	495		
1.50	19.95		
365	38		
001	495		
.1940.	-04		
αř.	- 16 M		
380	1075		
	-0.5		
14.S	- 10. m		
a)			
100	- 10 m		

Figure 175 System Monitor > Cellular WAN Status (Service Information)

Table 100	System	Monitor >	Cellular	WAN Status
	39310111		CCIIDIUI	

IABEL	DESC RIPIIO N
Refresh Interval	Select the time interval the Zyxel Device will check and refresh the fields shown on this screen. Select None to stop detection.
Module Information	on
IMEI	This shows the International Mobile Equipment Identity of the Zyxel Device.
Module SW Version	This shows the software version of the LTE module.
SIM Status	
SIM Card Status	This displays the SIM card status:
	None - the Zyxel Device does not detect that there is a SIM card inserted.
	$\mathbf{Available}$ - the SIM card could either have or doesn't have PIN code security.
	Locked - the SIM card has PIN code security, but you did not enter the PIN code yet.
	$\operatorname{Blocked}$ - 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.
	$\mathbf{Erro}\mathbf{r}$ - the Zyxel Device detected that the SIM card has errors.
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.

LTE Series User's Guide

LABEL	DESC RIPTIO N
PIN Protection	A PIN (Personal Identification Number) code is a key to a SIM card. Without the PIN code, you cannot use the SIM card.
	Shows \mathbf{Enable} if the service provider requires you to enter a PIN to use the SIM card.
	Shows Disa ble if the service provider lets you use the SIM without inputting a PIN.
PIN Remaining Attempts	This is how many more times you can try to enter the PIN code before the ISP blocks your SIM card.
IP Passthrough Sto	atus
IP Passthrough	This displays if IP Passthrough is enabled on the Zyxel Device.
Enable	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.
IP Passthrough	This displays the IP Passthrough mode.
Mode	This displays Dynamic and the Zyxel Device will allow traffic to be forwarded to the first LAN computer requesting an IP address from the Zyxel Device.
	This displays $Fixed$ and the Zyxel Device will allow traffic to be forwarded to a specific LAN computer on the local network of the Zyxel Device.
Cellular Status	This displays the status of the cellular Internet connection.
Data Roaming	This displays if data roaming is enabled on the Zyxel Device.
	4G roaming is to use your Zyxel 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.
Operator	This displays the name of the service provider.
PLMN	This displays the PLMN number.
Access Technology	This displays the type of the mobile network (such as LTE, UMTS, GSM) to which the Zyxel Device is connecting.
Band	This displays the current LTE band of your Zyxel Device (WCDMA2100).
RSSI	This displays the strength of the WiFi signal between an associated wireless station and an AP.
	The normal range is -30dBm to -79dBm. If the value drops below -80dBm, try moving the associated wireless station closer to the Zyxel Device to get better signal strength.
Cell ID	This shows the cell ID, which is a unique number used to identify the Base Transceiver Station to which the Zyxel Device is connecting.
	The value depends on the Current Access Technology:
	 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.
	The value is '0' (zero) or 'N/A' if there is no network connection.
Physical Cell ID	This shows the Physical Cell ID (PCI), which are queries and replies between the Zyxel Device and the mobile network it is connecting to. The normal range is 1 to 504.
UL Bandwidth (MHz)	This shows the LTE channel bandwidth from device to base station. According to 3GPP specifications, the bandwidths defined by the standard are 1.4, 3, 5, 10, 15, and 20 MHz. The wider the bandwidth the higher the throughput.
DL Bandwidth (MHz)	This shows the LTE channel bandwidth from base station to LTE device. According to 3GPP specifications, the bandwidths defined by the standard are 1.4, 3, 5, 10, 15, and 20 MHz. The wider the bandwidth the higher the throughput.

Table 100	System Manitors Collular MANI Status	(continued)
	System Monitor > Celiniar WAN Status ((commuea)

IABEL	DESC RIPTIO N
RFCN	This displays the Radio Frequency Channel Number of DL carrier frequency used by the mobile network to which the Zyxel Device is connecting.
	The value depends on the Current Access Technology:
	 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.
	The value is '0' (zero) or 'N/A' if there is no network connection.
RSRP	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.
	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.
	An undetectable signal is indicated by the lower limit, example -140 dBm.
	This parameter is for LTE only. The normal range is -30 to -140. The value is -140 if the Current Access Technology is not LTE. The value is 'N/A' if there is no network connection.
RSRQ	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.
	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.
	This parameter is for LTE only. The normal range is -30 to -240. The value is -240 if the Current Access Technology is not LTE. The value is 'N/A' if there is no network connection.
RSCP	This displays the Received Signal Code Power, which measures the power of channel used by the Zyxel Device.
	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.
	This parameter is for UMTS only. The normal range is -30 to -120. The value is -120 if the Current Access Technology is not UMTS. The value is 'N/A' if there is no network connection.
EcNo	This displays the ratio (in dB) of the received energy per chip and the interference level.
	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.
	This parameter is for UMTS only. The normal range is -30 to -240. The value is -240 if the Current Access Technology is not UMTS or there is no network connection.
TAC	This displays the Tracking Area Code (TAC), which is used to identify the country of a mobile subscriber.
	The physical cell ID of the connected E-UTRAN cell, is as specified in 3GPP-TS.36.101.
	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.
LAC	This displays the 2-octet Location Area Code (LAC), which is used to identify a location area within a PLMN.
	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].
	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

 Table 100
 System Monitor > Cellular WAN Status (continued)

IABEL	DESC RIPTIO N
RAC	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.
	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.
	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].
	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.
BSIC	The Base Station Identity Code (BSIC), which is a code used in GSM to uniquely identify a base station.
	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.
SINR	This displays the Signal to Interference plus Noise Ratio (SINR) in dB. This is also a measure of signal quality and used by the UE (User Equipment) to calculate the Channel Quality Indicator (CQI) that it reports to the network. A negative value means more noise than signal.
CQI	This displays the Channel Quality Indicator (CQI). It is an indicator carrying the information on how good/bad the communication channel quality is.
MCS	MCS stands for modulation coding scheme. The base station selects MCS based on current radio conditions. The higher the MCS the more bits can be transmitted per time unit.
RI	This displays the Rank Indication, one of the control information that a UE will report to eNodeB (Evolved Node-B) on either PUCCH (Physical Uplink Control Channel) or PUSCH (Physical Uplink Shared Channel) based on uplink scheduling.
PMI	This displays the Precoding Matrix Indicator (PMI).
	PMI is for transmission modes 4 (closed loop spatial multiplexing), 5 (multi-user MIMO), and 6 (closed loop spatial multiplexing using a single layer).
	PMI determines how cellular data are encoded for the antennas to improve downlink rate.

Table 100 System Monitor > Cellular WAN Status (continued)

C HAPTER 25 System

25.1 System Overview

Use this screen to name your Zyxel Device (Host) and give it an associated domain name for identification purposes.

25.2 System

Click **Maintenance > System** to open the following 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. **Figure 176** Maintenance > System

er o an associated daria in name forld renacijas on navinskima (155 age 1	der Mender dieneren 1991 in 1920 eterner	e.	
		na acelace	
methat biant	5,01,41,340110010.	2000230004	
egen)			
	mertak pani Kepis	menan basil Kepin	restan base Form

Table 101 Maintenance > System

LABEL	DESC RIPTIO N
Host Name	Type a host name for your Zyxel Device. Enter a descriptive name of up to 16 alphanumeric characters, not including spaces, underscores, and dashes.
Domain Name	Type a Domain name for your host Zyxel Device.
Cancel	Click Cancel to abandon this screen without saving.
Apply	Click Apply to save your changes.

C HAPTER 26 UserAccount

26.1 UserAccountOverview

In the UserAccount screen, you can view the settings of the "admin" and other user accounts that you use to log into the Zyxel Device to manage it.

26.2 UserAccount

Click **Maintenance** > UserAccount to open the following screen. Use this screen to create or manage user accounts and their privileges on the Zyxel Device.

Figure 177	Maintenance > User A	ccount
------------	----------------------	--------

			į.	User Account			
VEW	Point and the	ve "todrok" and orner	interstation, Par Parl Vol.	Gene as Monto Soci	te/m.		
<u> 995</u>	1210012004	tio popolititi englitisi	Supported Strengther Social	19-93 1			
						- /	a transformer
	723ee	the table	i sets tittet	ste Lovest	too: recad	urces = 1	attere State Notifi
•	N2344 El	the same	NOT STOLEN	KIN LIVESST	tato herod	seas ann Ann	all rectan Vocies Ma

Tuble Tuz Maimenance > User Accourt	Table 102	Maintenance >	User Account
-------------------------------------	-----------	---------------	--------------

IABEL	DESC RIPIIO N
Add New Account	Click this button to add a new user account (up to 4 Administrator accounts and 4 User accounts).
#	This is the index number.
Active	This indicates whether the user account is active or not.
	The check box is selected when the user account is enabled. It is cleared when it is disabled.
User Name	This displays the name of the account used to log into the Zyxel Device Web Configurator.
Retry Times	This displays the number of times consecutive wrong passwords can be entered for this account. O means there is no limit.

IABEL	DESC RIPIIO N
Idle Timeout	This 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 a user must wait before attempting to log in again after a number of consecutive wrong passwords have been entered as defined in Re try Tim e s .
Group	This field displays whether this user has Administra tor or User privileges.
Modify	Click the Edit icon to configure the entry. Click the Delete icon to remove the entry.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

Table 102 Maintenance > User Account (continued)

26.2.1 UserAccountAdd/Edit

Add or change the name of the user account, set the security password and the retry times, and whether this user will have Administrator or User privileges. Click Add New Account or the Edit icon of an existing account in the Maintenance > UserAccount to open the following screen.

Addressed angest erstan Neric Azer/Addresse of D	en di ber are can con Cord di seria gran os s sendell'eleca	ille - Remércien le colette la arrect
ke ni		
dim Harris		
000100		60
New Press 1		(0
Reary Televisi	<i>y</i>	(Statistic first
secondos.	4	- 10 a. (17 × 16
para man	4	$(B_{1})_{1} = g(B, X)$
and the second	Annatow.	135-200

Figure 178 Maintenance > User Account > Add/Edit

LABEL	DESC RIPTIO N			
Active	Click to enable (switch turns blue) or disable (switch turns gray) to activate or deactivate the user account.			
User Name	Enter a new name for the account (up to 15 characters). Special characters are allowed except the following: double quote (") back quote (`) apostrophe or single quote (') less than (<) greater than (>) caret or circumflex accent (^) dollar sign (\$) vertical bar () ampersand (&) semicolon (;)			
Password	Type your new system password (up to 256 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the Zyxel Device.			

Table 103 Maintenance > User Account > Add/Edit

IABEL	DESC RIPTIO N
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. 0 means there is 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 Re try Times .
Group	 Specify whether this user will have Administrator or User privileges. The Administrator privileges are the following: Quick Start setup. The following screens are visible for setup: Broadband, Wireless, Home Networking, Routing, NAT, DNS, Fire wall, MAC Filter, Certificates, Voice, Log, Traffic Status, ARP Table, Routing Table, Cellular WAN Status, System, User Account, Remote Management, TR-069 Client, Time, Email Notification, Log Setting, Firm ware Upgrade, Backup/Restore, Reboot, Diagnostic. The User privileges are the following: The following screens are visible for setup: Log, Traffic Status, ARP Table, Routing Table, Cellular WAN Status, User Account, Remote Management, The Offication, Log Setting, Firmware Upgrade, Backup/Restore, Reboot, Diagnostic.
Cancel	Click Cancel to restore your previously saved settings.
ОК	Click OK to save your changes.

 Table 103
 Maintenance > User Account > Add/Edit (continued)

CHAPTER 27 Remote Management

27.1 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.

27.2 MGMTServices

Note: The MGMTServices screen will be hidden if you enable the IP Passthrough function in Network Setting > Broadband > Cellular IP Passthrough screen.

Use this screen to configure the interfaces through which services can access the Zyxel Device. Click **Maintenance > Remote Management** to open the following screen.

te Contol				
	terrer and	🔄 e al avel 👩 te al avel		
		Canad MA		
Rectories	128,99128	- WAR	and Dama	1.00
+114	and the second	E Paramet	10.5	87
rinki	C	(T-7=+	To enter the	194
171	Distanti	() (Drate=	L. Posti	10 C
etter	🖪 red are	(1) hard dates	11 marine	14
120	E Trate	(1) Drame	(C. Irus)	40
No.		Devision	1. Contraction	

Figure 179 Maintenance > Remote Management

Table 104	Maintenance > Remote Management
-----------	---------------------------------

IABEL	DESC RIPTIO N	
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 Ne twork Setting > Broadband > Cellular WAN to access the service on the Zyxel Device.	
ETHWAN	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.	

27.3 MGMTServices for IP Passthrough

Configure which interfaces you can use to access the Zyxel Device in **IP Pa ssthrough** mode (bridge mode) for a given service. You can also specify the service port numbers computers must use to connect to the Zyxel Device. IP Passthrough allows Internet traffic to go to a LAN computer behind the Zyxel Device without going through NAT. Make sure to enable IP Passthrough in **Ne twork Setting** > **Bro a db a nd** > **Ce Ilula r IP Pa ssthrough**. See Section 6.9 on page 97 for details.

Click Maintenance > Remote Management > MGMTServices for IP Passthrough to open the following screen.

The figure satisfies the class (a) years and satisfies the state of the satisfies of the satisfies t	n ann an An Cynel Cewin de P. Presile en glane rann a chladar Cynel Cewin a P. Presile en glan	n in Bailge ment (Theory) version from the second plant. The second from the Baile product 120 menus of the first first part
Device without poing through NAT. Holes	ura to enclose IP Accelhrough in Network Setting	g - Seeaddand - Ceilaiar if foarthrough.
Service Control		
Service	WAR	Part
eru ne	🔤 Produkt	20080
AT HITES	🛃 LAGON	25.42
6.0 P	Endble	20031
PT TELSET	in state	20022
M_/00H	Endels	25 (7)
	Concel Ap	apiy.

Figure 180 Maintenance > Remote Management > MGMT Services for IP Passthrough

Table 10	5 Maintenance >	Remote Management	> MGMT Services for IP Passthroug	h
		Remore management.		

LABEL	DESC RIPIIO N	
Service	This is the service you may use to access the Zyxel Device.	
WAN	Select the Enable check box for the corresponding services that you want to allow access to the Zyxel Device from all WAN connections.	
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.	

27.4 Trust Domain

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 > MGMTServices screen. Click Maintenance > Remote Management > Thust Domain to open the following screen.

Note: Enter the IP address of the management station permitted to access the local management services. If specific services from the trusted hosts are allowed access but the trust domain list is empty, all public IP addresses can access the Zyxel Device from the WAN using the specified services.

Figure 181 Maintenance > Remote Management > Trust Domain

where the state state is a second or indicate the state of the state o	
${\bf r}$ are started with order to constrain the rest of the rest rest of the rest started with the rest for the rest ${\bf r}$	
	📥 Analysis (States)
an a state of the	Linex.

Table 106	Maintenance > Remote	Management >	Trust Domain
		managomoni	nosi Domani

IABEL	DESC RIPTIO N
Add Trust Domain	Click this to add a trusted host IP address.
IP Address	This field shows a trusted host IP address.
Delete	Click the Delete icon to remove the trusted host IP address.

27.5 Add Trust Domain

Use this screen to add a public IP addresses or a complete domain name of a device 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 182 Maintenance > Remote Management > Trust Domain > Add Trust Domain

	Add Trust Domain	
отну, е орало è разнич в Аллек	артусь напто скок собесто те усе сеное.	Jacobing C
		1.6.1.1

The following table describes the fields in this screen.

IABEL	DESC RIPTIO N
IP Address	Enter a public IPv4/IPv6 IP address which is allowed to access the service on the Zyxel Device from the WAN.
ОК	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to restore your previously saved settings.

Table 107 Maintenance > Remote Management > Trust Domain > Add Trust Domain

27.6 Trust Domain for IP Passthrough

Use this screen to view a list of public IP addresses/complete domain names which are allowed to access the Zyxel Device in **IP Passthrough** mode (bridge mode). IP Passthrough allows Internet traffic to go to a LAN computer behind the Zyxel Device without going through NAT. Make sure to enable IP Passthrough in **Network Setting** > **Broadband** > **Cellular IP Passthrough**. See Section 6.9 on page 97 for details.

Click Maintenance > Remote Management > Thust Domain for IP Passthrough to open the following screen.



Remote Manag	jemenl
an an in the local of the second of the second s	ed Borna to P. Prestanioli
When only of provide Γ order wave while Γ one want is please crosses to surger τ	ter Spei Deckse Hassigh trie services carefly reache ins
1 , the π^{+} , wrights all pole is 1^{4} used assession access the dynal best π^{-}	eren ha Wab menginin apad ise arwera.
	🔫 Auki Turi Dire ak
	Delete

Table 108 Maintenance > Remote Management > Trust Domain for IP Passthrough

LABEL	DESC RIPIIO N
Add Trust Domain	Click this to add a trusted host IP address.
IP Address	This field shows a trusted host IP address.
Delete	Click the Delete icon to remove the trusted host IP address.

27.7 Add Trust Domain

Use this screen to add a public IP address or a complete domain name of a device which is allowed to access the Zyxel Device. Click the Add Thust Domain button in the Maintenance > Remote Management > Thust Domain for IP Passthrough screen to open the following screen.

κ.	Add Trust Domain	
Contopore a Coble. Prise	describes a construct the online and second solution of the Zeonfederman.	Lines and a second
	Cancel OK	

Figure 184 Maintenance > Remote Management > Trust Domain for IP Passthrough > Add Trust Domain

The following table describes the fields in this screen.

Table 109	Maintenance	> Remote M	anaaement >	> Trust Domair	n for IP Pas	ssthrouah >	Add Trust	Domain
	internetion of the		anagomon	noor Donnan		John Cogni	7 (0 0 11 0 0 1	Donnan

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

LTE Series User's Guide
CHAPTER 28 TR-069 Client

28.1 Overview

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

28.2 TR-069 Client

TR-069 is a protocol that defines how your Zyxel Device can be managed via a management server. You can use a management server to remotely set up the Zyxel Device, modify settings, perform firmware upgrades as well as monitor and diagnose the Zyxel Device.

Click Maintenance > TR-069 Client to open the following screen.

Figure 185	Maintenance >	TR-069 Client
------------	---------------	---------------

	TR-069 Client	
A device Not Device to more	an na mana a baran waka Contra nation Sanan (#210 julia 19 68).	
CAVP.Action	1 10	
Kipro-	1.0	
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0	w(z	
R Second Second	E INNERSESSEE E ISSUE FOR THE REPAIRS	e a travelation
an ann an Naise AG 27 a Shuara		
vale interface corples Table Clean	🔆 bey Mar 🌰 Ne (Kar	
Carlos e Artes		
und symbol Versperantieran Labore		
unrecenterent des des des secondes de la constante		
upprecipite and an approximately apprecipite of the second s		
Lovector requel (policio Lovector requertors		
Weiter APP and the state	37 0	
$\begin{array}{c} (1+1) = (1+1) +$		•
	Cuncel Apply	

The following table describes the fields in this screen.

Table 110	Maintenance >	TR-069	Client
	11101101100	110 007	0.011

IABEL	DESC RIPTIO N
CWMP Active	CPE WAN Management Protocol (CWMP) enables the Zyxel Device to be remotely configured via a WAN link. Communication between the Zyxel Device and the management server is conducted via SOAP/HTTP(S) in the form of remote procedure calls (RPC).
	Click to enable (switch turns blue) to allow the Zyxel Device to be managed by a management server. Otherwise, click to disable (switch turns gray) to disallow the Zyxel Device to be managed by a management server.
Inform	Click to enable (switch turns blue) the Zyxel Device to send periodic inform via TR-069 on the WAN. Otherwise, click to disable (switch turns gray).
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	Select a WAN interface through which the TR-069 traffic passes.
used by IR-069 client	If you select $\mathbf{Any}_W \mathbf{AN}$, the Zyxel Device automatically passes the TR-069 traffic when any WAN connection is up.
	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.
Cellular WAN	The Zyxel Device automatically passes the TR-069 traffic when cellular WAN connection is up.
Display SOAP messages on serial console	Click to enable (switch turns blue) the dumping of 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	Enter the connection request user name.
Request User Name	When the ACS makes a connection request to the Zyxel Device, this user name is used to authenticate the ACS.
Connection	Enter the connection request password.
Request Password	When the ACS makes a connection request to the Zyxel Device, this password is used to authenticate the ACS.
Connection	This shows the connection request URL.
Request URL	The ACS can use this URL to make a connection request to the Zyxel Device.
Validate ACS Certificate	Click to enable (switch turns blue) the validation of a local certificate used by TR-069 client.
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.

C HAPTER 29 Time Settings

29.1 Time Settings Overview

This chapter shows you how to configure system related settings, such as system time, password, name, the domain name and the inactivity timeout interval.

29.2 Time

Use this screen to configure the Zyxel Device's time based on your local time zone. You can enter a time server address, select the time zone where the Zyxel Device is physically located, and configure Daylight Savings settings if needed.

To change your Zyxel Device's time and date, click Maintenance > Time. The screen appears as shown.



Figure 186 Maintenance > Tim

tument carto/data				
(Viert Tre	(42)20			
(2)-wei (1)-a e	Here was			
too and ttale setup				
Brow Trailorca	2010/02-0381			
I as an investor in a second	instala esp		1	
Topone Time Tower Address	descertand.		<u>а</u>	
Peter Term School Account	Secole relation		2 7	
Let she be a score	NO14			
Other Street Contract	(Desc)			
iene Zonic				
Internet.	juelet, 108003 Täipeer		54 - C	
avlight Lavings				
Activ	100			
ker bote	12			
320		1.000	21	
	10			
(coner)	WORD?		<u></u>	
24	30	1.		
ad lose.				
56	1 (m. 1)		24 CO	
	2	in the second		
0549	Celebia		84 -	
- 311	4	4	-	

The following table describes the fields in this screen.

Table 111 Maintenance > Tir

LABEL	DESC RIPTIO N	
Current Date/Time		
Current Time	This displays the time of your Zyxel Device.	
	Each time you reload this screen, the Zyxel Device synchronizes the time with the time server.	
Current Date	This displays the date of your Zyxel Device.	
	Each time you reload this screen, the Zyxel Device synchronizes the date with the time server.	
Time and Date Setup		
Time Protocol	This displays the time protocol used by your Zyxel Device.	

IABEL	DESC RIPTIO N
First ~ Fifth Time	Select an NTP time server from the drop-down list box.
Server Address	Otherwise, select Other and enter the IP address or URL (up to 29 extended ASCII characters in length) of your time server.
	Select $None$ if you don't want to configure the time server.
	Check with your ISP/network administrator if you are unsure of this information.
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 Saving Time 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.
Active	Click this switch to enable or disable Daylight Saving Time. When the switch turns blue 📬 , the function is enabled. Otherwise, it's not.
Start Rule	Configure the day and time when Daylight Saving Time starts if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The $Time$ field uses the 24 hour format. Here are a couple of examples:
	Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States, set the day to Second , Sunday , the month to March and the time to 2 in the Hour field.
	Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would set the day to Last , Sunday and the month to March . The time you select in the o'clock field depends on your time zone. In Germany for instance, you would select 2 in the Hour field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Rule	Configure the day and time when Daylight Saving Time ends if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The Time field uses the 24 hour format. Here are a couple of examples:
	Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would set the day to First , Sunday , the month to November and the time to 2 in the Hour field.
	Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would set the day to Last , Sunday , and the month to October . The time you select in the o'clock field depends on your time zone. In Germany for instance, you would select 2 in the Hour field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Cancel	Click Cancel to exit this screen without saving.
Apply	Click Apply to save your changes.

Table 111 Maintenance > Time (continued)

C HA PTER 30 E-mail No tific a tion

30.1 E-mail Notification Overview

A mail server is an application or a computer that can 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.

30.2 E-mail Notification

Use this screen to view, remove and add e-mail account information on the Zyxel Device. This account can be set to send e-mail notifications for logs.

Click Maintenance > E mail Notification to open the E mail Notification screen.

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

n moli ververi y an assorbar en ora dor	ngu teh half e en roceixe. R	head and do-	erenst research		
o have the Quel Davies cardinates.	aar or to Machine (Veren	el oto state	activity of the set that set is	ni hu anal castana di ka	stication brackets
lew, temple and bod priod decision	References the Svec C	er to The sec	n e contrative rore	entral no Realism for box.	
					🛨 Alaities va
	In the local	tor	Sector 10	L MOL KADING	bergone .

Figure 187 Maintenance > E-mail Notification

The following table describes the labels in this screen.

LABEL	DESC RIPIIO N
Add New e-mail	Click this button to create a new entry (up to 32 can be created).
Mail Server Address	This displays the server name or the IP address of the mail server.
User name	This displays the user name of the sender's mail account.
Port	This field displays the port number of the mail server.
Security	This field displays the protocol used for encryption.

Table 112 Maintenance > E-mail Notification

LTE Series User's Guide

Table 112 Maintenance > E-mail Notification (continued)

IABEL	DESC RIPIIO N
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).

30.2.1 E-mail Notification Edit

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



E mail Nottication Conf	guration	
NW Server Andrew		- 2000-12 - 19 a 19 20-14 - 14 - 14
For -	35	Ealth 4.55
Authority view Bechange		
Automatication (movered)		•
Second Constant		
Contraction Reports	🗇 XV 🕷 STARTES	

The following table describes the labels in this screen.

Table 1	13	E-mail Notification > Add	d
			~

LABEL	DESC RIPTIO N
Mail Server Address	Enter the server name or the IP address of the mail server for the e-mail address specified in the Accounte-mail Address field.
	If this field is left blank, reports, logs or notifications will not be sent via e-mail.
Port	Enter the same port number here as is on the mail server for mail traffic.
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 email 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/TLS authentication, the e-mail address must be able to be authenticated by the mail server as well.

LABEL	DESC RIPIIO N
Connection Security	Select SSL to use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) if you want encrypted communications between the mail server and the Zyxel Device.
	Select STARTILS to upgrade a plain text connection to a secure connection using SSL/TLS.
Cancel	Click this button to begin configuring this screen afresh.
OK	Click this button to save your changes and return to the previous screen.

 Table 113
 E-mail Notification > Add (continued)

C HAPTER 31 Log Setting

31.1 Log Setting Overview

Use this screen to configure where the Zyxel Device sends logs, and which type of logs the Zyxel Device records.

31.2 Log Setting

You can configure where the Zyxel Device sends logs and which type of logs the Zyxel Device records in the Logs Setting screen.

If you have a server that is running a syslog service, you can also save log files to it by enabling Syslog Logging, and then entering the IP address of the server in the Syslog Server field. Select Remote to store logs on the syslog server, or select Local File to store logs on the Zyxel Device. Select Local File and Remote to store logs on both the Zyxel Device and the syslog server. To change your Zyxel Device's log settings, click Maintenance > Log Setting. The screen appears as shown.

Figure 189	Maintenance >	Log Setting
------------	---------------	-------------

		Log Set	ting		
You can configure onere the 2	sel É evice server ognario	onien logt endlichter	паран раткор	vel Cence record	
nthan 30 was Carl to store System and states Apple days works that she we then been with the Docker	andre provenste server h de la face deleta a l'Analan orto evito i premetto las vice de colo encontrato conce	nationaring a Maley Line Weath and Line Sal Ric Blown Source	nitter vol controle den en " die Pour Katolikon antikolo	ning Repfron Last Design of Rep (chap and Coving: Joseph School Soviet: Joseph	computer to Bio year opling remote a Care Bio any Sector (1991) Recard Romatic record at a social
System Selling					
-14 00-000mg					
1970 av	1				
	4	¥.			Deriver - Auff of Brit, Pail
21251	194				Der ver Prett
e-mail tog anting:					
C-institute Settings	- CO				
Mathematics	Second streption of			1	
optimizing the line part of					
and the second second second					
(endbopre					with Assess
Carlo Agent Io					WWW Assessed
ADT RMAD	- 64 				
Actor top					
Sectors and	Scoully Los				
2 Wellington	1 - Series (1997)				
Contraction and the second	CT nessour				
📴 39459	E Revell				
1977	UNK				
Tan					
There					
100					
and the second					
🚮 Charles (MAR),					
	3	Sance	Abel 1		

The following table describes the fields in this screen.

LA BEL	DESCRIPTION
Syslog Settings	
Syslog Logging	Click the switch (it will turn blue) to enable syslog logging.
Mode	Select Remote to have the Zyxel Device send it to an external syslog server.
	Select Local File to have the Zyxel Device save the log file on the Zyxel Device itself.
	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.
	Note: A warning appears upon selecting Remote or Local File and Remote . Just click OK to continue.

IABEL	DESC RIPIIO N
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 Setting	S
E-mail Log Setting	Click the switch (it will turn blue) to allow the sending via e-mail the system and security logs to the e-mail address specified in Send Log to.
	Note: Make sure that the Mail Server Address field is not left blank in the Maintenance > Email Notifications screen.
Mail Account	Select a server specified in Maintenance $> E mail Notifications$ to send the logs to.
System Log Mail Subject	This field allows you to enter a descriptive name for the system log e-mail (for example Zyxel System Log). Up to 127 characters are allowed for the System Log Mail Subject including special characters inside the square brackets $[!\#\%(]^{*+},/:=?@[] \$.
Security Log Mail Subject	This field allows you to enter a descriptive name for the security log e-mail (for example Zyxel Security Log). Up to 127 characters are allowed for the Security Log Mail Subject including special characters inside the square brackets $[!#\%()^{*+},/:=?@[] \$
Send Log to	This field allows you to enter the log's designated e-mail recipient. The log's format is plain text file sent as an e-mail attachment.
Send Alarm to	This field allows you to enter the alarm's designated e-mail recipient. The alarm's format is plain text file sent as an e-mail attachment.
Alarm Interval	Select the frequency of showing of the alarm.
Active Log	
System Log	Select the categories of System Logs that you want to record.
Security Log	Select the categories of \mathbf{Sec} unity \mathbf{Log} s that you want to record.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

Table 114 Maintenance > Log Setting (continued)

CHAPTER 32 Firm ware Upgrade

32.1 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 Zyxel Device's performance.

Only use firm ware for your Zyxel Device's specific model. Refer to the label on the bottom of your Zyxel Device.

32.2 Firmware Upgrade

This screen lets you upload new firmware to your Zyxel Device. 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.

Click Maintenance > Firm ware Upgrade to open the following screen.

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



	Firmware Upgrade	
Autors and Remove to your loss Device or sover care Device The actives process and PTM in eacher Remote Remote	ha, fra later filmwer, fildfram fra Tarch Met scotl and mee tale up for here min	ndele. V un vol 4 verser in veleze 4 in eeu 2001 An elektrik waard 4 veleze 41 Eeu 2005 ele
Degrade Fornware		
Robert Cold - July Cold State (Special	3	
Current Immodel - and on 2004-0645-2 CO		
Tia Spin	disayada vi milara	(Indiana)
Online Firmware Upgrade		
Creative and Previous New		

The following table describes the labels in this screen.

IABEL	DESC RIPTIO N
Upgrade Firmware	Use these fields to upload firmware to the Zyxel Device.
Restore Default Settings After Firmware	Click to enable this option that restores the factory-default to the Zyxel Device after upgrading the firmware.
Upgrade	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 33.2 on page 266.
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.

Table 115 Maintenance > Firmware Upgrade

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 191 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 **Firm ware Upgrade** screen.

C HA PTER 33 Backup/Restore

33.1 Backup/Restore Overview

Information related to factory default settings and backup configuration are shown in this screen. You can also use this to restore previous device configurations.

33.2 Backup/Restore

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

Figure 192 Maintenance > Backup/Restore

	Backup/Restore	
Cork up and roater	e vour Zwo. Der de benlig werken. Het dan skonteket wate Breil Gerkes och nin back kurte k	actory at land.
Nan bege Califique de Syber Devide la porte recesarja e construite de la	ne nill en yn a trefne en a strawej Tar Anel Henner Anseren I an pry a dae da a Henner an a gwed ar t fwraffar ny property i'r 1 ngreg reformer nan fwr golarada y gwed ar tyfwr yn yw a straffar yn yw a s a wlene yn Part a refne a refne a fwr di refin aethr a da fernau yw a treffar far berne ar ar ar	gale Dirolle of Beberge Manadian
sectore compared	an allow types to up to be a native of previously to read that high lands the Born your optimation to s	or don rende
Backup Configura	liza	
Cilles Cockup to so-ent	he surrent configuration of your ordern. Is your computery	
malage		
Realore Configural	Nan	
To heritare o previously	coversion of figuration file to your system. Betwee to the location of the configuration file and si	ick Vipiopa
114 serie	(using 1) to the new res	
linck is Factory D	afort Settings	
State Street is a low-	are we have been to be by particle to the mark to be a first on the back may be back to be bright. All we need to get	
Press - Field In 17	24	
LAN & COOKER WITH	ac 192,166.(*	
- DIST will canvent	s para a crimp	
THE R. L.		
and the second se		

Backup Configuration

Backup Configuration allows you to back up (save) the Zyxel Device's current configuration to a file on your computer. Once your Zyxel Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes.

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.

IABEL	DESC RIPIIO N
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 Zyxel Device settings back to the factory default.

Table 116 Restore Configuration

Do not tum 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 193 Network Temporarily Disconnected

```
No comence - No comence of a second la 

A 🔮 🌠 dat entre 200004 💭
```

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.

33.3 Reboot

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 194 Maintenance > Reboot

Keboot			
Advalued we become which a real parts the coveral sites remerched. The time by e become a callo real profile description if e is a beyond a state of a sta			
dan a mana			

C HAPTER 34 Diagnostic

34.1 Diagnostic Overview

The Diagnostic screens display information to help you identify problems with the Zyxel Device.

34.2 Ping/TraceRoute/NslookupTest

Use this screen to 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/Trace Route/Nslookup** screen shown next.

Disgnostic							
 Sector such Sector Sector sector sector sector sector sector in the default for weather Sector problem was a dealy block the biology year that the experimental sector sect							
Plag (inter de	with Territ						
NMP .							
er hin o				100	na ang	terre internet	en e seren p

Figure 195 Maintenance > Diagnostic > Ping/Trace Route/Nslookup

The following table describes the fields in this screen.

Table 117 Maintenance > Diagnostic

IABEL	DESC RIPTIO N
Ping/ TraceRoute Test	The result of tests is shown here in the info area.
TCP/IP	

LABEL	DESC RIPTIO N
Address	Enter either an IP address or a host name to start a test.
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.

 Table 117
 Maintenance > Diagnostic (continued)

C HAPTER 35 Trouble shooting

35.1 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
- USB Device Connection
- UPnP
- SIM Card
- Cellular Signal

35.2 Power and Hardware Connections

The Zyxel Device does not turn on.

For LIE3301-PLUS / LIE5388-M804 / LIE5398-M904 / LIE3316-M604

- 1 Make sure you are using the power adapter included with the Zyxel Device.
- 2 Make sure the power adapter is connected to the Zyxel Device and plugged in to an appropriate power source. Make sure the power source is turned on.
- 3 Disconnect and re-connect the power adapter to the Zyxel Device.
- 4 Make sure you've pressed the **POWER** button to turn on the Zyxel Device.
- 5 If the problem continues, contact the vendor.

For LIE7240-M403/LIE7461-M602/LIE7480-S905

1 Make sure you are using the PoE injector and cable (Power over Ethernet, PoE) included with the Zyxel Device.

- 2 Make sure the PoE is connected to the Zyxel Device and plugged in to an appropriate power source. Make sure the power source is turned on.
- **3** Turn the Zyxel Device off and on.
- 4 If the problem continues, contact the vendor.

35.3 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 Zyxel Device to its factory defaults. Refer to Section 33.2 on page 266.

I forgot the password.

- 1 See the Zyxel Device label for the default admin password.
- 2 If you changed the password, and can't remember the password, you have to reset the Zyxel Device to its factory defaults. Refer to Section 33.2 on page 266.

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 8.2 on page 132), 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 Zyxel Device to its factory default, and try to access the Zyxel Device with the default IP address. Refer to Section 33.2 on page 266.
- 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 Zyxel Device to its factory default. See Section 33.2 on page 266.

I cannot use FTP, Telnet, SSH or Ping to access the Zyxel Device.

See the Remote Management Chapter 27 on page 248 for details on allowing web services (such as HTTP, HTTPS, FTP, Telnet, SSH and Ping) to access the Zyxel Device.

Check the server **Port** number field for the web service in the **Maintenance > Remote Management** screen. You must use the same port number in order to use that web service for remote management.

35.4 Internet Access

I cannot access the Internet.

- 1 Check the hardware connections and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.5.1 on page 24.
- 2 Check the SIM card. Maybe it has wrong settings (refer to Section 6.6 on page 92), the account has expired, it became loose (remove and reinsert it refer to the Quick Start Guide) or it's missing (stolen). See Section 35.7 on page 276 for possible SIM card problems.

- 3 Make sure you entered your ISP account information correctly. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 4 For LTE3301-PLUS / LTE5388-M804 / LTE5398-M904 / LTE3316-M604 make sure you converted the first or fourth LAN port to a WAN port. Click Enable in Network Setting > Broadband > Ethernet WAN screen. Make sure you have the Ethernet WAN port connected to a modem or router.
- 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 Check the signal strength. Look at the LEDs, and check the LED section for more information. If the signal strength is low, try moving the Zyxel Device closer to the ISP's base station if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).
- 3 For the LTE3301-PLUS / LTE5388-M804 / LTE5398-M904 / LTE3316-M604, connect two external antennas to improve the wireless WAN signal strength. Point the antennas to the base stations directions if you know where they are, or try pointing the antennas in different directions and check which provides the strongest signal to the Zyxel Device. See the Introduction chapter for more information.
- **4** Turn the Zyxel Device off and on.
- 5 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).
 - Note: Since your Zyxel Device is an outdoor-type, inclement weather like rain and hot weather may affect LTE signals.

35.5 USB Device Connection

The Zyxel Device fails to detect my USB device.

- 1 Disconnect the USB device.
- 2 Reboot the Zyxel Device.
- 3 If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.
- 4 Re-connect your USB device to the Zyxel Device.

35.6 UPnP

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

- 1 Make sure that UPnP is enabled in your computer. For Windows 7, see Section 8.6 on page 140. For Windows 10, see Section 8.7 on page 144.
- 2 Make sure that UPnP is enabled in the **Network Settings** > **Home Networking** > **UPnP** screen. See Section 8.4 on page 138 for details.
- 3 Disconnect the Ethernet cable from the Zyxel Device's Ethernet port or from your computer.
- 4 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.

35.7 SIM Card

The SIM card cannot be detected.

- 1 Disconnect the Zyxel Device from the power supply.
- 2 Remove the SIM card from its slot.
- 3 Clean the SIM card slot of any loose debris using compressed air.
- 4 Clean the gold connectors on the SIM card with a clean lint-free cloth.
- 5 Insert the SIM card into its slot and connect the Zyxel Device to the power supply to restart it.

I get an **Invalid** SIM card alert.

- 1 Make sure you have an active plan with your ISP.
- 2 Make sure that the Zyxel Device is in the coverage area of a cellular network.

35.8 CellularSignal

How should I position the Zyxel Device to get a strong cellular signal?

1 Find the location of your nearest cellular base station(s), then install the Zyxel Device towards the direction of those sites. The nearest site or site with a direct line-of-sight is usually preferred.

Note: It is best to test towards more than one cellular site, as the nearest site / line-of-sight is not always the best due to the terrain, interference, density of usage, etc. All of these factors influence the stability, availability and throughput of the link to the Zyxel Device.

- 2 Position the Zyxel Device towards a direction where coverage is expected (example the nearest town).
- 3 Conduct test measurements using the Web Configurator's System Monitor > Cellular WAN Status screen to obtain a report of the cellular network signal strength and quality at various test positions.

Note: It is best to reboot the Zyxel Device before each test measurement is taken to ensure that it is not camping on the previous cellular site. This is because the Zyxel Device can 'lock' onto the previous cellular site even when the new cellular site is at a much better signal level and quality. Although installing the Zyxel Device as high as possible is the usual rule of thumb, it is sometimes possible that the Zyxel Device is in a weak coverage spot at that specific height. Adjust the height to achieve the best service possible.

Note: Cellular network signals and quality can fluctuate. A measurement taken now and a few moments later can differ substantially even if nothing apparent has changed – this can be due to many aspects, such as fading, reflections, interference, capacity due to high network traffic, etc.

It is possible that the network topology and usage changes over time, even from one minute to the next as network utilization increases. If poor performance is experienced at a later stage, re-test different installation locations again. It is possible that the current serving cellular site has become over utilized or is out-of-service. As the network design and topology changes, so will the experience change, either for the better or for the worse.

PART III Appendices

Appendices contain general information. Some information may not apply to your Zyxel Device.

A PPENDIX 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 *https://www.zyxelcom/homepage.shtml* and also *https://www.zyxelcom/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)

Ta iwa n

- Zyxel Communications Corporation
- https://www.zyxel.com

Asia

China

- Zyxel Communications (Shanghai) Corp. Zyxel Communications (Beijing) Corp.
 - Zyxel Communications (Tianjin) Corp.
- https://www.zyxel.com/cn/zh/

India

- Zyxel Technology India Pvt Ltd
- https://www.zyxel.com/in/en/

Ka za khsta n

- Zyxel Kazakhstan
- https://www.zyxel.kz

Ko re a

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

Ma la ysia

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

Pa kista n

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

Philip pine s

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

Singapore

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

Ta iwa n

- Zyxel Communications Corporation
- https://www.zyxel.com/tw/zh/

Tha ila nd

- Zyxel Thailand Co., Ltd
- https://www.zyxel.com/th/th/

Vie tna m

- Zyxel Communications Corporation-Vietnam Office
- https://www.zyxel.com/vn/vi

Europe

Be la rus

- Zyxel BY
- https://www.zyxel.by

Be lg ium

- Zyxel Communications B.V.
- https://www.zyxel.com/be/nl/

https://www.zyxel.com/be/fr/

Bulg a ria

- Zyxel България
- https://www.zyxel.com/bg/bg/

Czech Republic

- Zyxel Communications Czech s.r.o
- https://www.zyxel.com/cz/cs/

Denmark

- Zyxel Communications A/S
- https://www.zyxel.com/dk/da/

Esto nia

- Zyxel Estonia
- https://www.zyxel.com/ee/et/

Finla nd

- Zyxel Communications
- https://www.zyxel.com/fi/fi/

Fra nc e

- Zyxel France
- https://www.zyxel.fr

Gemany

- Zyxel Deutschland GmbH
- https://www.zyxel.com/de/de/

Hung a ry

- Zyxel Hungary & SEE
- https://www.zyxel.com/hu/hu/

Ita ly

- Zyxel Communications Italy
- https://www.zyxel.com/it/it/

La tvia

- Zyxel Latvia
- https://www.zyxel.com/lv/lv/

Lithua nia

- Zyxel Lithuania
- https://www.zyxel.com/lt/lt/

Ne the rlands

- Zyxel Benelux
- https://www.zyxel.com/nl/nl/

Norway

- Zyxel Communications
- https://www.zyxel.com/no/no/

Poland

- Zyxel Communications Poland
- https://www.zyxel.com/pl/pl/

Rom a nia

- Zyxel Romania
- https://www.zyxel.com/ro/ro

Russia

- Zyxel Russia
- https://www.zyxel.com/ru/ru/

Slo va kia

- Zyxel Communications Czech s.r.o. organizacna zlozka
- https://www.zyxel.com/sk/sk/

Spain

- Zyxel Communications ES Ltd
- https://www.zyxel.com/es/es/

Sweden

- Zyxel Communications
- https://www.zyxel.com/se/sv/

Switze rla nd

- Studerus AG
- https://www.zyxel.ch/de
- https://www.zyxel.ch/fr

Turke y

- Zyxel Turkey A.S.
- https://www.zyxel.com/tr/tr/

UK

- Zyxel Communications UK Ltd.
- https://www.zyxel.com/uk/en/

Ukra ine

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

South America

Argentina

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

Bra zil

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

Colombia

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

Ecuador

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

South America

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

Middle East

Isra e l

- Zyxel Communications Corporation
- http://il.zyxel.com/

Middle East

- Zyxel Communications Corporation
- https://www.zyxel.com/me/en/

North America

USA

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

O c e a nia

Austra lia

- Zyxel Communications Corporation
- https://www.zyxel.com/au/en/

A fric a

So uth Afric a

- Nology (Pty) Ltd.
- https://www.zyxel.com/za/en/

A PPENDIX B IPv6

Ove rvie w

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 3.4×10^{38} IP addresses.

IPv6 Addressing

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

IPv6 addresses can be abbreviated in two ways:

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

Prefix and Prefix Length

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

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

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

Link-local Address

A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a "private IP address" in IPv4. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of fe80::/10. The link-local unicast address format is as follows.

Table 118 Link-local Unicast Address Format

1111 1110 10	0	Interface ID
10 bits	54 bits	64 bits

GlobalAddress

A global address uniquely identifies a device on the Internet. It is similar to a "public IP address" in IPv4. A global unicast address starts with a 2 or 3.

Unspecified Address

An unspecified address (0:0:0:0:0:0:0:0:0 or ::) is used as the source address when a device does not have its own address. It is similar to "0.0.0.0" in IPv4.

Loopback Address

A loopback address (0:0:0:0:0:0:0:0:1 or ::1) allows a host to send packets to itself. It is similar to "127.0.0.1" in IPv4.

Multic a st Addre ss

In IPv6, multicast addresses provide the same functionality as IPv4 broadcast addresses. Broadcasting is not supported in IPv6. A multicast address allows a host to send packets to all hosts in a multicast group.

Multicast scope allows you to determine the size of the multicast group. A multicast address has a predefined prefix of ff00::/8. The following table describes some of the predefined multicast addresses.

Table 119 Predefined Multicast Address

MULTICASTADDRESS	DESC RIPIIO N
FF01:0:0:0:0:0:1	All hosts on a local node.
FF01:0:0:0:0:0:2	All routers on a local node.
FF02:0:0:0:0:0:1	All hosts on a local connected link.
FF02:0:0:0:0:0:2	All routers on a local connected link.
FF05:0:0:0:0:0:2	All routers on a local site.
FF05:0:0:0:0:1:3	All DHCP severs on a local site.

The following table describes the multicast addresses which are reserved and cannot be assigned to a multicast group.

Table 120	Reserved	Multicast	Address

MULTIC AST ADDRESS
FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0

Table 120 Reserved Multicast Address (continued)

MULIIC	ASTADDRESS
FF0E:0:	0:0:0:0:0:0
FFOF:0:	0:0:0:0:0:0

Subnet Masking

Interface ID

In IPv6, an interface ID is a 64-bit identifier. It identifies a physical interface (for example, an Ethernet port) or a virtual interface (for example, the management IP address for a VLAN). One interface should have a unique interface ID.

EUI-64

The EUI-64 (Extended Unique Identifier) defined by the IEEE (Institute of Electrical and Electronics Engineers) is an interface ID format designed to adapt with IPv6. It is derived from the 48-bit (6-byte) Ethernet MAC address as shown next. EUI-64 inserts the hex digits fffe between the third and fourth bytes of the MAC address and complements the seventh bit of the first byte of the MAC address. See the following example.



Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface. The DHCP client uses the IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information. The IA type is the type of address in the IA. Each IA holds one type of address. IA_NA means an identity association for non-temporary addresses and IA_TA is an identity association for temporary addresses. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA were obtained) a Renew message. If the time T2 is reached and the server

does not respond, the client sends a Rebind message to any available server (**S2**). For an IA_TA, the client may send a Renew or Rebind message at the client's discretion.



DHCP Re la y Agent

A DHCP relay agent is on the same network as the DHCP clients and helps forward messages between the DHCP server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCP server on its network, it then needs a DHCP relay agent to send a message to a DHCP server that is not attached to the same network.

The DHCP relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string, such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCP server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

Pre fix De le g a tio n

Prefix delegation enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The Zyxel Device uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by multicast, the Zyxel Device passes the IPv6 prefix information to its LAN hosts. The hosts then can use the prefix to generate their IPv6 addresses.

IC MPv6

Internet Control Message Protocol for IPv6 (ICMPv6 or ICMP for IPv6) is defined in RFC 4443. ICMPv6 has a preceding Next Header value of 58, which is different from the value used to identify ICMP for IPv4. ICMPv6 is an integral part of IPv6. IPv6 nodes use ICMPv6 to report errors encountered in packet processing and perform other diagnostic functions, such as "ping".

Neighbor Discovery Protocol (NDP)

The Neighbor Discovery Protocol (NDP) is a protocol used to discover other IPv6 devices and track neighbor's reachability in a network. An IPv6 device uses the following ICMPv6 messages types:

- Neighbor solicitation: A request from a host to determine a neighbor's link-layer address (MAC address) and detect if the neighbor is still reachable. A neighbor being "reachable" means it responds to a neighbor solicitation message (from the host) with a neighbor advertisement message.
- Neighbor advertisement: A response from a node to announce its link-layer address.
- Router solicitation: A request from a host to locate a router that can act as the default router and forward packets.
- Router advertisement: A response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters.

IPv6 Cache

An IPv6 host is required to have a neighbor cache, destination cache, prefix list and default router list. The Zyxel Device maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the Zyxel Device configures a link-local address automatically, and then sends a neighbor solicitation message to check if the address is unique. If there is an address to be resolved or verified, the Zyxel Device also sends out a neighbor solicitation message. When the Zyxel Device receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor cache. When the Zyxel Device uses a router solicitation message to query for a router and receives a router advertisement message, it adds the router's information to the neighbor cache, prefix list and destination cache. The Zyxel Device creates an entry in the default router list cache if the router can be used as a default router.

When the Zyxel Device needs to send a packet, it first consults the destination cache to determine the next hop. If there is no matching entry in the destination cache, the Zyxel Device uses the prefix list to determine whether the destination address is on-link and can be reached directly without passing through a router. If the address is unlink, the address is considered as the next hop. Otherwise, the Zyxel Device determines the next-hop from the default router list or routing table. Once the next hop IP address is known, the Zyxel Device looks into the neighbor cache to get the link-layer address and sends the packet when the neighbor is reachable. If the Zyxel Device cannot find an entry in the neighbor cache or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

Multic a st Liste ner Disc overy

The Multicast Listener Discovery (MLD) protocol (defined in RFC 2710) is derived from IPv4's Internet Group Management Protocol version 2 (IGMPv2). MLD uses ICMPv6 message types, rather than IGMP message types. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3.

MLD allows an IPv6 switch or router to discover the presence of MLD listeners who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.

MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.

MLD filtering controls which multicast groups a port can join.

MID Messages

A multicast router or switch periodically sends general queries to MLD hosts to update the multicast forwarding table. When an MLD host wants to join a multicast group, it sends an MLD Report message for that address.

An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

Example - Enabling IPv6 on Windows 7

Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

To enable IPv6 in Windows 7:

- 1 Select Control Panel > Network and Sharing Center > Local Area Connection.
- 2 Select the Internet Protocol Version 6 (TCP/IPv6) checkbox to enable it.
- 3 Click **OK** to save the change.

Connect using	
🔮 Broadco	n NetXterne Gigebit Ethernet
This concertor	Configure
B Paer	for Morpsoft Networks
Coll File at	lacket Scheduler Id Rinder Sheeing for Microsoft Networks
Call - Canada	
a liter	Pertonel Version 4 (TCP) Evel
E + Intern	et Pistocol Version 4 (TCP//Pv4)
	et Postocol Version 4 (TCP//Pv4)
Intel.	t Potocol Verson 4 (TCP/IPv4)

- 4 Click Close to exit the Local Area Connection Status screen.
- 5 Select Start > All Programs > Accessories > Command Prompt.
- 6 Use the ipconfig command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.



A PPENDIX C Legal Information

Copyright

Copyright © 2020 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.

Disc la im e r

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

EURO PEAN UNIO N



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:

(LIE7240-M403)

- WiFi
 - The band 2,400 to 2,483.5 MHz is 88.51 mW
- GSM
 - The GSM 900 is 1967.89 mW
 - The DCS 1800 is 968.28 mW
- WCDMA
 - The WCDMA Band I is 213.8 mW
 - The WCDMA Band VIII is 208.93 mW
- LTE
 - The LTE Band 1 is 204.17 mW
 - The LTE Band 3 is 199.53 mW
 - The LTE Band 7 is 190.55 mW
 - The LTE Band 8 is 208.93 mW
 - The LTE Band 20 is 223.87 mW
 - The LTE Band 38 is 147.91 mW
 - The LTE Band 40 is 141.25 mW

(LIE3301-PLUS)

- WiFi
 - The band 2,400 to 2,483.5 MHz is 81.28 mW
 - The band 5,150 to 5,350 MHz is 180.3 mW
 - The band 5,470 to 5,725 MHz is 612.35 mW
- WCDMA
 - The WCDMA Band I is 193.64 mW

- The WCDMA Band III is 228.56 mW
- The WCDMA Band VIII is 198.15 mW
- LTE
 - The LTE Band 1 is 223.87 mW
 - The LTE Band 3 is 239.88 mW
 - The LTE Band 7 is 218.78 mW
 - The LTE Band 8 is 186.21 mW
 - The LTE Band 20 is 186.21 mW
 - The LTE Band 28 is 206.06 mW
 - The LTE Band 38 is 247.17 mW
 - The LTE Band 40 is 231.21 mW

(LIE7480-M804 & LIE7490-M904)

- The band 2,400 to 2,483.5 MHz is 87.1 mW (LTE7480-M804)
- The band 2,400 to 2,483.5 MHz is 87.1 mW (LTE7490-M904)
- WCDMA
 - The WCDMA Band I is 316.23 mW
 - The WCDMA Band III is 316.23 mW
 - The WCDMA Band VIII is 281.84 mW
- LTE

• The LTE Band 1/3/7/8/20/28/38/40 is 281.84 mW

- (LTE3316-M604)
- WCDMA
 - The WCDMA Band I is 193.64 mW
 - The WCDMA Band III is 228.56 mW
 - The WCDMA Band VIII is 198.15 mW
- LTE
 - The LTE Band 1 is 223.87 mW
 - The LTE Band 3 is 251.19 mW
 - The LTE Band 7 is 218.78 mW
 - The LTE Band 8 is 186.21 mW
 - The LTE Band 20 is 186.21 mW
 - The LTE Band 28 is 206.06 mW
 - The LTE Band 38 is 247.17 mW
 - The LTE Band 40 is 231.21 mW
- 802.11 Mode
 - 802.11b Band is 84.3 mW
 - 802.11g Band is 95.72 mW
 - 802.11n Band is 96.83 mW
 - 802.11ac Band is 195.88 mW
 - 802.11ac Band is 392.64 mW

Български (Bulgarian)	С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/ЕС.
	Na tional Restric tions
	 The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details. Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens. Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails.
Español (Spanish)	Por medio de la presente Zyxel declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/UE
Čeština (Czech)	Zyxel tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU.
Dansk (Danish)	Undertegnede Zyxel erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU.
	Na tional Restrictions
	 In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage. I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.
Deutsch (German)	Hiermit erklärt Zyxel, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU befindet.
Eesti keel (Estonian)	Käesolevaga kinnitab Zyxel seadme seadmed vastavust direktiivi 2014/53/EL põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ ΖΥΧΕΙ ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/ΕΕ.

LTE Series User's Guide

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.
	Na tional Restrictions
	 This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check http://www.sviluppoeconomico.gov.it/ for more details. Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare http://www.sviluppoeconomico.gov.it/ per maggiori dettagli.
Latviešu valoda	Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 2014/53/ES būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
(Latvian)	Na tional Restrictions
	 The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details. 2.4 GHz frekvenèu joslas izmantoðanai ârpus telpâm nepiecieðama afïauja no Elektronisko sakaru direkcijas. Vairâk informâcijas: http://www.esd.lv.
Lietuvių kalba (Lithuanian)	Šiuo Zyxel deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/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-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 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). .

•

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	СҮ	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	СН
Ireland	IE	Sweden	SE
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

List of national codes

United States of America (LIE7461-M602 and LIE7480-S905)



The following information applies if you use the product within USA area.

FCC EMC Statement

- This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
- (1) This device may not cause harmful interference, and
- (2) This device must accept any interference received, including interference that may cause undesired operation.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
- This product has been tested and complies with the specifications for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
- If this device does cause harmful interference to radio or television reception, which is found by turning the equipment off and on, the user is
 encouraged to try to correct the interference by one or more of the following measures:
 - Reorient or relocate the receiving antenna.
 - Increase the separation between the equipment or devices
 - Connect the equipment to an outlet other than the receiver's
 - Consult a dealer or an experienced radio/TV technician for assistance

The following information applies if you use the product with RF function within USA area.

FCC Radiation exposure statement

• This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.

(12127461-M602) This transmitter must be at least 30 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.

(LTE7480-S905) This transmitter must be at least 20 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.

CANADA (LIE7461-M602)

The following information applies if you use the product within Canada area.

Innovation, Science and Economic Development Canada ICES Statement

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

Innovation, Science and Economic Development Canada RSS-GEN & RSS-247 Statement

- This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's
 licence-exempt RSS(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device
 must accept any interference, including interference that may cause undesired operation of the device.
- This radio transmitter (2468C-LTE7461M602)) has been approved by Innovation, Science and Economic Development Canada to operate
 with the antenna types listed below with the maximum permissible gain indicated. Antenna types not included in this list that have, a gain
 greater than the maximum gain indicated for any type listed, are strictly prohibited for use with this device.

Antenna Information

Chain No.	Antenna Type	Frequency Range	WiFiGain (dBi)	LIE Gain (dBi)	Connector
WLAN-ANTO	PIFA	2.4 ~ 2.4835 GHz	6	N.A.	iPEX
WLAN-ANT1	PIFA	2.4 ~ 2.4835 GHz	5	N.A.	iPEX
WWAN	Dipole	2500 ~ 2570 MHz	N.A.	9	iPEX
		698 ~ 716 MHz	N.A.	3.5	iPEX
		777 ~ 787 MHz	N.A.	3	iPEX
		1850 ~ 1915 MHz	N.A.	8	iPEX
		814 ~ 849 MHz	N.A.	3.6	iPEX
		2305 ~ 2315 MHz	N.A.	9	iPEX
		1710 ~ 1780 MHz	N.A.	6	iPEX

If the product with 5G wireless function operating in 5150-5250 MHz and 5725-5850 MHz, the following attention must be paid,

- The device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.
- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits as appropriate; and
- Where applicable, antenna type(s), antenna models(s), and the worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in Section 6.2.2.3 of RSS 247 shall be clearly indicated.
- If the product with 5G wireless function operating in 5250-5350 MHz and 5470-5725 MHz, the following attention must be paid.
- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit.
- L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage; (2) L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.
- Le présent émetteur radio (2468C-LTE7461M602) a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenne énumérés ci dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué pour tout type figurant sur la liste, sont strictement interdits pour l'exploitation de l'émetteur.

Chaîne NB.	Antenne Type	Gamme de fréquences	WiFi Gain (dBi)	LIE Gain (dBi)	Connecteur
WLAN-ANTO	PIFA	2.4 ~ 2.4835 GHz	6	N.A.	iPEX
WLAN-ANT1	PIFA	2.4 ~ 2.4835 GHz	5	N.A.	iPEX
WWAN	Dipole	2500 ~ 2570 MHz	N.A.	9	iPEX
		698 ~ 716 MHz	N.A.	3.5	iPEX
		777 ~ 787 MHz	N.A.	3	iPEX
		1850 ~ 1915 MHz	N.A.	8	iPEX
		814 ~ 849 MHz	N.A.	3.6	iPEX
		2305 ~ 2315 MHz	N.A.	9	iPEX
		1710 ~ 1780 MHz	N.A.	6	iPEX

inform a tions antenne

Lorsque la fonction sans fil 5G fonctionnant en 5150-5250 MHz and 5725-5850 MHz est activée pour ce produit , il est nécessaire de porter une attention particulière aux choses suivantes

• Les dispositifs fonctionnant dans la bande de 5 150 à 5 250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

 Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5 725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée, selon le cas;

 Lorsqu'il y a lieu, les types d'antennes (s'il y en a plusieurs), les numéros de modèle de l'antenne et les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élévation, énoncée à la section 6.2.2.3 du CNR-247, doivent être clairement indiqués. Lorsque la fonction sans fil 5G fonctionnant en 5250-5350 MHz et 5470-5725 MHz est activée pour ce produit , il est nécessaire de porter une attention particulière aux choses suivantes.

 Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis pour les dispositifs utilisant les bandes de 5 250 à 5 350 MHz et de 5 470 à 5 725 MHz doit être conforme à la limite de la p.i.r.e.

Industry Canada radiation exposure statement

This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 30 cm between the radiator and your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 30 cm de distance entre la source de rayonnement et votre corps.

Safety Warnings (All LIE Models)

- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Do not expose your Zyxel Device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not obstruct the Zyxel Device ventilation slots as insufficient airflow may harm your Zyxel Device. For example, do not place the Zyxel 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 Zyxel Device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the Zyxel Device.
- Do not open the Zyxel 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 Zyxel 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 Zyxel 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 Zyxel 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 Zyxel Device or where the plug on the power supply cord is intended to serve as the disconnect device,
 - For permanently connected Zyxel Device, a readily accessible disconnect device shall be incorporated external to the Zyxel Device;
 - For pluggable devices, the socket-outlet shall be installed near the Zyxel Device and shall be easily accessible.

Environment Statement

ErP (LTE3301-PLUS / LTE5388-M804 / LTE5398-M904 / LTE3316-M604)

Zyxel products put on the EU market in compliance with the requirement of the European Parliament and the Council published Directive 2009/ 125/EC establishing a framework for the setting of ecodesign requirements for energy-related products (recast), so called as "ErP Directive (Energy-related Products directive) as well as ecodesign requirement laid down in applicable implementing measures, power consumption has satisfied regulation requirements which are:

- Network standby power consumption < 8W, and/or
- Off mode power consumption < 0.5W, and/or
- Standby mode power consumption < 0.5W.

(Wireless settings, please refer to the chapter about wireless settings for more detail.)

European Union - Disposal and Recycling Information

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

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

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la domástica. 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.









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110VAC,歐洲是230VAC)。
- 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.

SYMBOL	EXPLANATION
	Alternating current (AC):
\sim	AC is an electric current in which the flow of electric charge periodically reverses direction.
	Direct current (DC):
	DC if the unidirectional flow or movement of electric charge carriers.
	Earth; ground:
A	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.

Explanation of the Symbols

Viewing Certifications

Go to <u>http://www.zyxel.com</u> 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 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 Zyxel Device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online at <u>www.zyxel.com</u> to receive e-mail notices of firmware upgrades and related information.

Open Source Licenses

This product may contain 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 <u>www.zyxel.com</u>. If you cannot find it there, contact your vendor or Zyxel Technical Support at <u>support@zyxel.com.tw</u>.

To obtain the source code covered under those Licenses, please contact your vendor or Zyxel Technical Support at support@zyxel.com.



Index

Α

access troubleshooting 272 Access Control (Rules) screen 188 ACS 253 activation firewalls 185 Add New ACL Rule screen 189 Address Resolution Protocol 229 Any_WAN Remote Management 249 TR-069 traffic 254 **APN** information obtain 91 APN Settings 92 Application Layer Gateway (ALG) 170 applications Internet access 18 wireless WAN 18 ARP Table 229, 231, 234 ARP Table screen 230 authentication 120, 121 RADIUS server 121 Authentication Type APN 92 Auto Configuration Server, see ACS 253

В

backup configuration 267 backup configuration 267 Backup/Restore screen 266 Band Configuration Screen 93 Basic Service Set, see BSS blinking LEDs 24 Broadband 83 BSS 122 example 123

С

CA 207 Cellular Band screen 93 Cellular SIM screen 92 Cellular WAN 249 TR-069 traffic 254 Cellular WAN Screen 91 Cellular WAN screen 89, 91 certificate details 209 factory default 202 file format 208 file path 206 import 202, 205 public and private keys 208 verification 208 certificate request create 202 view 203 certificates 201 advantages 208 authentication 201 CA 207 creating 202 public key 201 replacing 202 storage space 202 thumbprint algorithms 209 thumbprints 209 trusted CAs 206 verifying fingerprints 208 Certification Authority, see CA certifications 295 viewing 299 channel, wireless LAN 119 client list 136 configuration

backup 267 firewalls 185 restoring 267 static route 176 contact information 279 copyright 292 Create Certificate Request screen 202 creating certificates 202 CTS threshold 114, 120 customer support 279 customized service add 187 customized services 187, 188

D

data fragment threshold 114, 120 Data Roaming enable 91 Denials of Service, see DoS DHCP 132 DHCP Server Lease Time 134 DHCP Server State 134 diagnostic 269 diagnostic screens 269 digital IDs 201 disclaimer 292 DMZ screen 170 DNS 132 DNS Values 134 domain name system, see DNS DoS 184 thresholds 185 DoS protection blocking enable 192 dynamic DNS 175 wildcard 175 Dynamic Host Configuration Protocol, see DHCP DYNDNS wildcard 175

Ε

e-mail log setting 263 Extended Service Set IDentification 102, 107

F

factory-default RESET button 31 filters MAC address 108, 121 firewall enhancing security 193 security considerations 193 traffic rule direction 191 Firewall DoS screen 191 Firewall General screen 186 firewall rules direction of travel 192 firewalls 184, 185 actions 191 configuration 185 customized services 187, 188 DoS 184 thresholds 185 ICMP 184 rules 192 security 193 firmware 264 version 73 Firmware Upgrade screen 264 firmware upload 264 firmware version check 265 fragmentation threshold 114, 120 FTP 163 unusable 273

G

General wireless LAN screen 100

Η

hardware connections troubleshooting 271

I

IANA 140 ICMP 184 Import Certificate screen 206 importing trusted CAs 206 Internet no access 273 wizard setup 44 Internet access 18 wizard setup 44 Internet Assigned Numbers Authority See IANA Internet Blocking 71 Internet connection slow or erratic 274 Internet Control Message Protocol, see ICMP Internet Protocol version 6, see IPv6 **IP** address WAN 84 IP address access control 251 IP Passthrough mode 98 IP Passthrough screen 39, 97 IPv4 firewall 186 IPv6 285 addressing 285 EUI-64 287 global address 285 interface ID 287 link-local address 285 Neighbor Discovery Protocol 285 ping 285 prefix 285 prefix length 285 unspecified address 286 IPv6 firewall 186

L

LAN 131 client list 136 MAC address 116, 137 status 74, 81 LAN IP address 134 LAN IPv6 Mode Setup 134 LAN Setup screen 132 LAN subnet mask 134 limitations wireless LAN 122 WPS 129 listening port 217 Local Area Network, see LAN local certificate TR-069 client 254 Local Certificates screen 201 Log Setting screen 261 login 35 passwords 35 troubleshooting 272 Login screen no access 272 logs 223, 226, 239, 261

Μ

MAC Address LAN 137 MAC address 110, 116, 137 filter 108, 121 MAC authentication 108 MAC Authentication screen 104, 109 Mac filter 195 managing the device good habits 20 using FTP. See FTP. MGMT Services screen 248, 249 **MSN** Messenger problem 275 Multi WAN Remote Management 249 TR-069 traffic 254

Ν

NAT default server 170 DMZ host 170 multiple server example 163 NAT ALG screen 170, 171, 173 Network Address Translation, see NAT network disconnect temporary 265 Network Map 71 network map 39 network type select 94 Nslookup test 270

0

Others screen 113

Ρ

password admin 272 good habit 20 lost 272 user 272 passwords 35 PBC 124 PIN Protection 93 PIN, WPS 124 example 126 Ping unusable 273 Ping test 270 Ping/TraceRoute/Nslookup screen 269 PLMN Configuration Screen 94 PoE injector 18, 271 port forwarding rule add/edit 164 Port Forwarding screen 164 Port Triggering add new rule 168

Port Triggering screen 166 ports 24 power troubleshooting 271 preamble 115, 120 preamble mode 123 problem troubleshooting 271 Protocol (Customized Services) screen 187 Protocol Entry add 187 Push Button Configuration, see PBC push button, WPS 124

R

RADIUS server 121 Reboot screen 267 remote management TR-069 253 Remote Procedure Calls, see RPCs 253 RESET Button 31 restart system 267 restore default settings after firmware upgrade 265 restoring configuration 267 RFC 1058. See RIP. RFC 1389. See RIP. RFC 1631 162 RFC 3164 223 RIP 161 router features 18 Routing Information Protocol. See RIP Routing Table screen 232, 234 RPPCs 253 RTS threshold 114, 120

S

security network **193** wireless LAN **120** Security Log 224 service access control 249, 251 Service Set 102, 107 setup firewalls 185 static route 176 SIM card status 75, 240 SIM configuration 92 SSH unusable 273 SSID 121 Static DHCP 136 Configuration 137 Static DHCP screen 136 static route 154, 161 configuration 176 status 71 firmware version 73 LAN 74, 81 WAN 73 wireless LAN 74 status indicators 24 syslog protocol 223 severity levels 223 syslog logging enable 262 syslog server name or IP address 263 system firmware 264 version 73 passwords 35 status 71 LAN 74, 81 WAN 73 wireless LAN 74 time 255

Т

Telnet unusable 273 The 84

thresholds data fragment 114, 120 DoS 185 RTS/CTS 114, 120 time 255 TR-069 253 authentication 254 TR-069 Client screen 253 Trace Route test 270 troubleshooting 271 Trust Domain add 251 Trust Domain screen 250 Trusted CA certificate view 206 Trusted CA screen 205 Turning on UPnP Windows 7 example 140

U

Universal Plug and Play, see UPnP upgrading firmware 264 UPnP 138 forum 132 security issues 132 State 138 undetectable 275 usage confirmation 132 UPnP screen 138 UPnP-enabled Network Device auto-discover 141, 146

W

WAN status 73 Wide Area Network, see WAN 83 warranty 299 note 299 Web Configurator easy access 149 web configurator

login 35 passwords 35 WEP Encryption 103 Wireless General screen 100 wireless LAN 99 authentication 120, 121 BSS 122 example 123 channel 119 example 119 fragmentation threshold 114, 120 limitations 122 MAC address filter 108, 121 preamble 115, 120 RADIUS server 121 RTS/CTS threshold 114, 120 security 120 SSID 121 status 74 WPS 123, 126 example 127 limitations 129 PIN 124 push button 124 Wireless tutorial 48 wizard setup Internet 44 WMM screen 112 WPS 123, 126 example 127 limitations 129 PIN 124 example 126 push button 124 WPS screen 110