

P-660HN-Tx

802.11n Wireless ADSL2+ 4-port Gateway

User's Guide

Default Login Details

IP Address	http://192.168.1.1
Password	1234

Firmware Version 1.02
Edition 1, 1/2011

www.zyxel.com

The logo for ZyXEL, featuring the brand name in a bold, blue, sans-serif font. The 'Z' and 'Y' are connected, and the 'X' is stylized with a diagonal slash.

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the ZyXEL Device using the web configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

- Quick Start Guide

The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.

- Support Disc

Refer to the included CD for support documents.

- ZyXEL Web Site

Please refer to www.zyxel.com for additional support documentation and product certifications.

Documentation Feedback

Send your comments, questions or suggestions to: techwriters@zyxel.com.tw

Thank you!

The Technical Writing Team, ZyXEL Communications Corp.,
6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 30099, Taiwan.

Need More Help?

More help is available at www.zyxel.com.



- Download Library

Search for the latest product updates and documentation from this link. Read the Tech Doc Overview to find out how to efficiently use the User Guide, Quick Start Guide and Command Line Interface Reference Guide in order to better understand how to use your product.

- Knowledge Base

If you have a specific question about your product, the answer may be here. This is a collection of answers to previously asked questions about ZyXEL products.

- Forum

This contains discussions on ZyXEL products. Learn from others who use ZyXEL products and share your experiences as well.

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. See http://www.zyxel.com/web/contact_us.php for contact information. Please have the following information ready when you contact an office.

- 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.

Disclaimer

Graphics in this book may differ slightly from the product due to differences in operating systems, operating system versions, or if you installed updated firmware/software for your device. Every effort has been made to ensure that the information in this manual is accurate.

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

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




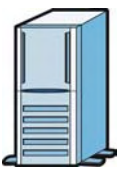




Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The P-660HN-Tx may be referred to as the "ZyXEL Device", the "device", the "system" or the "product" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The ZyXEL Device icon is not an exact representation of your device.

ZyXEL Device 	Computer 	Notebook computer 
Server 	Firewall 	Telephone 
Router 	Switch 	

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.



Contents Overview

User's Guide	19
Introduction	21
The Web Configurator	29
Status Screens	37
Tutorials	41
Technical Reference	55
Internet and Wireless Setup Wizard	57
WAN Setup	71
LAN Setup	89
Wireless LAN	103
Network Address Translation (NAT)	131
Firewall	143
Filters	147
Certificate	155
Static Route	159
Quality of Service (QoS)	165
Dynamic DNS Setup	175
Remote Management	177
Universal Plug-and-Play (UPnP)	185
CWMP	197
System Settings	201
Logs	205
Tools	209
Diagnostic	217
Troubleshooting	221
Product Specifications	227

Table of Contents

About This User's Guide	3
Document Conventions.....	5
Safety Warnings.....	7
Contents Overview	9
Table of Contents.....	11
Part I: User's Guide.....	19
Chapter 1	
Introduction.....	21
1.1 Overview	21
1.2 Ways to Manage the ZyXEL Device	21
1.3 Good Habits for Managing the ZyXEL Device	22
1.4 Applications for the ZyXEL Device	22
1.4.1 Internet Access	23
1.5 Wireless Access	23
1.5.1 Using the WPS/WLAN Button	24
1.6 LEDs (Lights)	26
1.7 The RESET Button	27
1.7.1 Using the Reset Button	28
Chapter 2	
The Web Configurator	29
2.1 Overview	29
2.1.1 Accessing the Web Configurator	29
2.2 The Main Screen	32
2.2.1 Title Bar	32
2.2.2 Navigation Panel	33
2.2.3 Main Window	34
2.2.4 Status Bar	35
Chapter 3	
Status Screens	37
3.1 Overview	37

3.2 The Status Screen	37
Chapter 4	
Tutorials	41
4.1 Overview	41
4.2 Setting Up a Secure Wireless Network	41
4.2.1 Configuring the Wireless Network Settings	42
4.2.2 Using WPS	43
4.2.3 Without WPS	48
4.3 Configuring the MAC Address Filter	48
4.4 Configuring Static Route for Routing to Another Network	50
4.5 Multiple WAN Connections Example	53
Part II: Technical Reference	55
Chapter 5	
Internet and Wireless Setup Wizard	57
5.1 Overview	57
5.2 Internet Access Wizard Setup	57
5.2.1 Manual Configuration	60
5.3 Wireless Connection Wizard Setup	66
5.3.1 Manually Assign a WPA-PSK key	68
5.3.2 Manually Assign a WEP Key	69
Chapter 6	
WAN Setup.....	71
6.1 Overview	71
6.1.1 What You Can Do in the WAN Screens	71
6.1.2 What You Need to Know About WAN	71
6.1.3 Before You Begin	72
6.2 The Internet Access Setup Screen	73
6.2.1 Advanced Internet Access Setup	76
6.3 The More Connections Screen	77
6.3.1 More Connections Edit	79
6.3.2 Configuring More Connections Advanced Setup	82
6.4 WAN Technical Reference	83
6.4.1 Encapsulation	83
6.4.2 Multiplexing	84
6.4.3 VPI and VCI	85
6.4.4 IP Address Assignment	85
6.4.5 Nailed-Up Connection (PPP)	86

6.4.6 NAT	86
6.5 Traffic Shaping	86
6.5.1 ATM Traffic Classes	87
Chapter 7	
LAN Setup.....	89
7.1 Overview	89
7.1.1 What You Can Do in the LAN Screens	89
7.1.2 What You Need To Know About LAN	90
7.1.3 Before You Begin	91
7.2 The LAN IP Screen	91
7.2.1 The Advanced LAN IP Setup Screen	92
7.3 The DHCP Setup Screen	93
7.4 The Client List Screen	94
7.5 The IP Alias Screen	96
7.5.1 Configuring the LAN IP Alias Screen	96
7.6 The IPv6 Screen	97
7.7 LAN Technical Reference	98
7.7.1 LANs, WANs and the ZyXEL Device	98
7.7.2 DHCP Setup	99
7.7.3 DNS Server Addresses	99
7.7.4 LAN TCP/IP	99
7.7.5 RIP Setup	101
7.7.6 Multicast	101
Chapter 8	
Wireless LAN.....	103
8.1 Overview	103
8.1.1 What You Can Do in the Wireless LAN Screens	103
8.1.2 What You Need to Know About Wireless	104
8.1.3 Before You Start	104
8.2 The AP Screen	105
8.2.1 No Security	106
8.2.2 WEP Encryption	107
8.2.3 WPA(2)-PSK	108
8.2.4 Wireless LAN Advanced Setup	109
8.2.5 MAC Filter	110
8.3 The More AP Screen	111
8.3.1 More AP Edit	112
8.4 The WPS Screen	113
8.5 The WPS Station Screen	114
8.6 Wireless LAN Technical Reference	115
8.6.1 Wireless Network Overview	115

8.6.2 Additional Wireless Terms	117
8.6.3 Wireless Security Overview	118
8.6.4 Signal Problems	121
8.6.5 BSS	121
8.6.6 MBSSID	122
8.6.7 WiFi Protected Setup (WPS)	123
Chapter 9	
Network Address Translation (NAT).....	131
9.1 Overview	131
9.1.1 What You Can Do in the NAT Screens	131
9.1.2 What You Need To Know About NAT	131
9.2 The NAT General Setup Screen	132
9.3 The Port Forwarding Screen	133
9.3.1 Configuring the Port Forwarding Screen	134
9.3.2 The Port Forwarding Rule Edit Screen	136
9.4 The ALG Screen	137
9.5 NAT Technical Reference	137
9.5.1 NAT Definitions	137
9.5.2 What NAT Does	138
9.5.3 How NAT Works	139
9.5.4 NAT Application	140
9.5.5 NAT Mapping Types	140
Chapter 10	
Firewall.....	143
10.1 Overview	143
10.1.1 What You Can Do in the Firewall Screens	143
10.1.2 What You Need to Know About Firewall	143
10.2 The Firewall Screen	145
Chapter 11	
Filters	147
11.1 Overview	147
11.1.1 What You Can Do in the Filter Screens	147
11.1.2 What You Need to Know About Filtering	147
11.2 The URL Filter Screen	148
11.3 The IP Filter Screen	149
11.4 IPv6 Filter	151
Chapter 12	
Certificate	155
12.1 Overview	155

12.1.1 What You Can Do in this Chapter	155
12.2 What You Need to Know	155
12.3 The Trusted CA Screen	156
12.3.1 View Trusted CA Certificate	157
12.3.2 Import Trusted CA Certificate	158
Chapter 13	
Static Route	159
13.1 Overview	159
13.1.1 What You Can Do in the Static Route Screens	160
13.2 The Static Route Screen	160
13.2.1 Static Route Edit	161
13.2.2 IPv6 Static Route	162
13.2.3 IPv6 Static Route Edit	163
Chapter 14	
Quality of Service (QoS).....	165
14.1 Overview	165
14.1.1 What You Can Do in the QoS Screens	166
14.1.2 What You Need to Know About QoS	166
14.2 The General Screen	167
14.2.1 The QoS Summary List Screen	168
14.3 The Queue Setup Screen	168
14.4 The Class Setup Screen	170
14.5 QoS Technical Reference	172
14.5.1 IEEE 802.1p	173
14.5.2 IP Precedence	173
14.5.3 Automatic Priority Queue Assignment	173
Chapter 15	
Dynamic DNS Setup	175
15.1 Overview	175
15.1.1 What You Can Do in the DDNS Screen	175
15.1.2 What You Need To Know About DDNS	175
15.2 The Dynamic DNS Screen	176
Chapter 16	
Remote Management.....	177
16.1 Overview	177
16.1.1 What You Can Do in the Remote Management Screens	178
16.1.2 What You Need to Know About Remote Management	178
16.2 The WWW Screen	179
16.2.1 Configuring the WWW Screen	179

16.3 The Telnet Screen	180
16.4 The FTP Screen	180
16.5 The SNMP Screen	181
16.5.1 Configuring SNMP	183
16.6 The ICMP Screen	184
Chapter 17	
Universal Plug-and-Play (UPnP).....	185
17.1 Overview	185
17.1.1 What You Can Do in the UPnP Screen	185
17.1.2 What You Need to Know About UPnP	185
17.2 The UPnP Screen	187
17.3 Installing UPnP in Windows Example	188
17.4 Using UPnP in Windows XP Example	191
Chapter 18	
CWMP.....	197
18.1 Overview	197
18.2 The CWMP Setup Screen	198
Chapter 19	
System Settings	201
19.1 Overview	201
19.1.1 What You Can Do in the System Settings Screens	201
19.2 The General Screen	201
19.3 The Time Setting Screen	202
Chapter 20	
Logs	205
20.1 Overview	205
20.1.1 What You Need To Know About Logs	205
20.2 The View Log Screen	205
20.3 The Log Settings Screen	206
Chapter 21	
Tools.....	209
21.1 Overview	209
21.1.1 What You Can Do in the Tool Screens	209
21.2 The Firmware Screen	209
21.3 The Configuration Screen	212
21.4 The Restart Screen	215
Chapter 22	
Diagnostic.....	217

22.1 Overview	217
22.1.1 What You Can Do in the Diagnostic Screens	217
22.2 The General Screen	217
22.3 The DSL Line Screen	218
Chapter 23	
Troubleshooting.....	221
23.1 Power, Hardware Connections, and LEDs	221
23.2 ZyXEL Device Access and Login	222
23.3 Internet Access	224
Chapter 24	
Product Specifications	227
24.1 Hardware Specifications	227
24.2 Firmware Specifications	227
24.3 Wireless Features	231
24.4 Power Adaptor Specifications	234
Appendix A Setting up Your Computer's IP Address.....	235
Appendix B IP Addresses and Subnetting	259
Appendix C Pop-up Windows, JavaScripts and Java Permissions.....	269
Appendix D Wireless LANs	279
Appendix E IPv6.....	295
Appendix F Services	305
Appendix G Legal Information.....	309
Index.....	313

PART I

User's Guide

Introduction

1.1 Overview

The P-660HN-Tx (x stands for 1 or 3) is an ADSL2+ router with 2x2 wireless. By integrating DSL and NAT, you are provided with ease of installation and high-speed, shared Internet access. With 802.11n 2x2, the P-660HN-Tx can transfer at data rates up to 300Mbps. The P-660HN-Tx is also a complete security solution with a robust firewall and content filtering.

Please refer to the following description of the product name format.

- "H" denotes an integrated 4-port hub (switch).
- "N" denotes 802.11n draft 2.0. The "N" models support 802.11n wireless connection mode.
- Models ending in "1", for example P-660HN-Tx, denote a device that works over the analog telephone system, POTS (Plain Old Telephone Service). Models ending in "3" denote a device that works over ISDN (Integrated Services Digital Network) or T-ISDN (UR-2).

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

Note: All screens displayed in this user's guide are from the **P-660HN-Tx** model.

See the product specifications for a full list of features.

1.2 Ways to Manage the ZyXEL Device

Use any of the following methods to manage the ZyXEL Device.

- Web Configurator. This is recommended for everyday management of the ZyXEL Device using a (supported) web browser.
- Command Line Interface. Line commands are mostly used for troubleshooting by service engineers.
- FTP for firmware upgrades and configuration backup/restore.
- TR-069. This is an auto-configuration server used to remotely configure your device.

1.3 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). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the ZyXEL Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the ZyXEL Device. You could simply restore your last configuration.

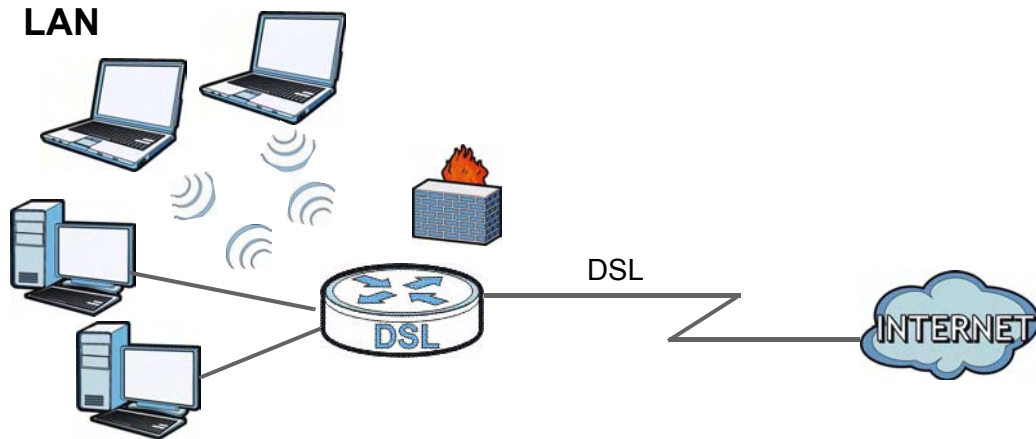
1.4 Applications for the ZyXEL Device

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

1.4.1 Internet Access

Your ZyXEL Device provides shared Internet access by connecting the DSL port to the **DSL** or **MODEM** jack on a splitter or your telephone jack. Computers can connect to the ZyXEL Device's LAN ports (or wirelessly).

Figure 1 ZyXEL Device's Router Features



You can also configure firewall and filtering feature on the ZyXEL Device for secure Internet access. When the firewall is on, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files.

Use the filtering feature to block access to specific web sites or Internet applications such as MSN or Yahoo Messenger. You can also configure IP/MAC filtering rules for incoming or outgoing traffic.

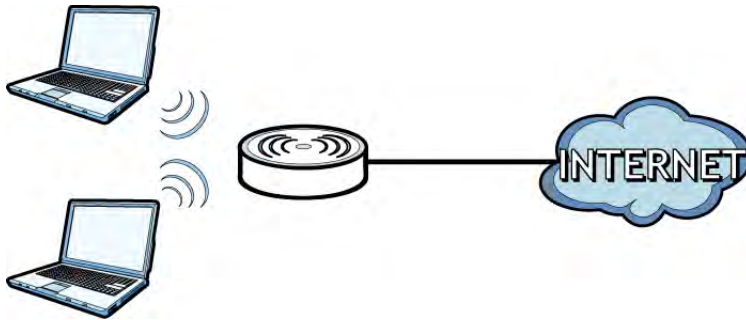
Use QoS to efficiently manage traffic on your network by giving priority to certain types of traffic and/or to particular computers. For example, you could make sure that the ZyXEL Device gives voice over Internet calls high priority, and/or limit bandwidth devoted to the boss's excessive file downloading.

1.5 Wireless Access

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

You can configure your wireless network in either the built-in Web Configurator, or using the WPS button.

Figure 2 Wireless Access Example



However, before you can use this ZyXEL Device to create a wireless network, you must set its country code first in the Web Configurator. This is very important.

To set the wireless country code:

- 1 Log into the ZyXEL Device's built-in Web Configurator. See [Chapter 8 on page 103](#).
- 2 Open the **Network > Wireless LAN > AP** screen.
- 3 Select your country from the **Channel Selection** list. See [Section 8.2 on page 105](#) for details.
- 4 Click **Apply** to save your changes.
- 5 Finally, open the Internet and Wireless Configuration wizards to set up your network. See [Chapter 5 on page 57](#).

1.5.1 Using the WPS/WLAN Button

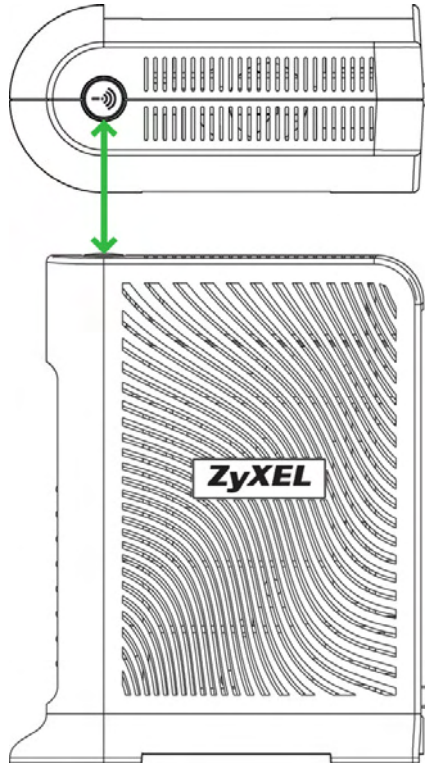
By default, the wireless network on the ZyXEL Device is turned on. To turn it off, simply press the **WPS/WLAN** button on top of the device for over 5 seconds. When the **WPS/WLAN** LED is green, the wireless network is active.

You can also use the **WPS/WLAN** button to quickly set up a secure wireless connection between the ZyXEL Device and a WPS-compatible client by adding one device at a time.

To activate WPS:

- 1 Make sure the **POWER** LED is on and not blinking.

- 2 Press the **WPS/WLAN** button for one to five seconds and release it.

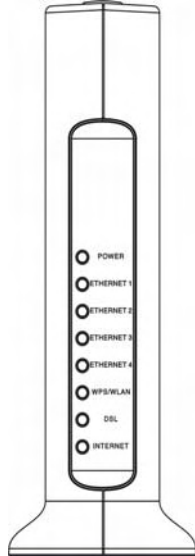


- 3 Press the WPS button on another WPS-enabled device within range of the ZyXEL Device. The **WPS/WLAN** LED should flash while the ZyXEL Device sets up a WPS connection with the other wireless device.
- 4 Once the connection is successfully made, the **WPS/WLAN** LED shines green.

1.6 LEDs (Lights)

The following graphic displays the labels of the LEDs.

Figure 3 LEDs



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

Table 1 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The ZyXEL Device is receiving power and ready for use.
		Blinking	The ZyXEL Device is self-testing.
	Red	On	The ZyXEL Device detected an error while self-testing, or there is a device malfunction.
		Off	The ZyXEL Device is power off.
LAN 1-4	Green	On	The ZyXEL Device has an Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The ZyXEL Device is transmitting data to or receiving data from the LAN.
		Off	The ZyXEL Device does not have an Ethernet connection with the LAN.
WPS/ WLAN	Green	On	The wireless network is activated.
		Blinking	The ZyXEL Device is communicating with other wireless clients.
	Orange	Blinking	The ZyXEL Device is setting up a WPS connection.
		Off	The wireless network is not activated.
DSL	Green	On	The DSL line is up.
		Blinking	The ZyXEL Device is initializing the DSL line.
		Off	The DSL line is down.

Table 1 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
INTERNET	Green	On	The ZyXEL Device has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a server), PPP negotiation was successfully completed (if used) and the DSL connection is up.
		Blinking	The ZyXEL Device is sending or receiving IP traffic.
	Red	On	The ZyXEL Device attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed, no IP address from IPCP.
		Off	The ZyXEL Device does not have an IP connection.

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

1.7 The RESET Button

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

1.7.1 Using the Reset Button

- 1 Make sure the **POWER** LED is on (not blinking).
- 2 To set the device back to the factory default settings, press the **RESET** button for ten seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the device restarts.

The Web Configurator

2.1 Overview

The web configurator is an HTML-based management interface that allows easy device setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

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

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

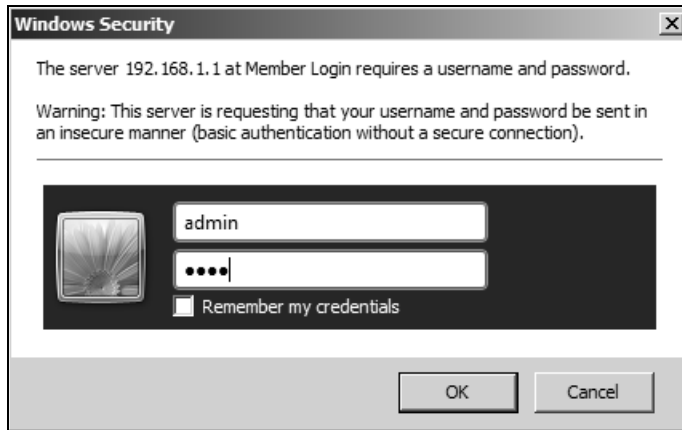
See [Appendix C on page 269](#) if you need to make sure these functions are allowed in Internet Explorer.

2.1.1 Accessing the Web Configurator

- 1 Make sure your ZyXEL Device hardware is properly connected (refer to the Quick Start Guide).
- 2 Launch your web browser.
- 3 Type "192.168.1.1" as the URL.

- 4 A password screen displays. To access the administrative web configurator and manage the ZyXEL Device, type the user name (admin by default) and admin password (1234 by default) in the password screen and click **Login**. Click **Cancel** to revert to the default user password in the password field. If you have changed the password, enter your password and click **Login**.

Figure 4 Password Screen



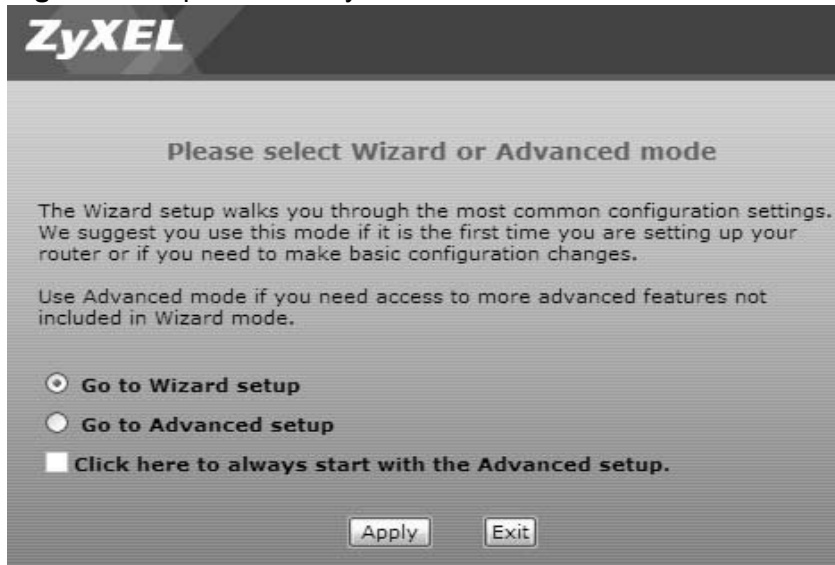
- 5 The following screen displays if you have not yet changed your password. It is strongly recommended you change the default password. Enter a new password, retype it to confirm and click **Apply**; alternatively click **Ignore** to proceed to the main menu if you do not want to change the password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

Figure 5 Change Password Screen



- 6 Select **Go to Wizard setup** and click **Apply** to display the wizard main screen. Otherwise, select **Go to Advanced setup** and click **Apply** to display the **Status** screen.

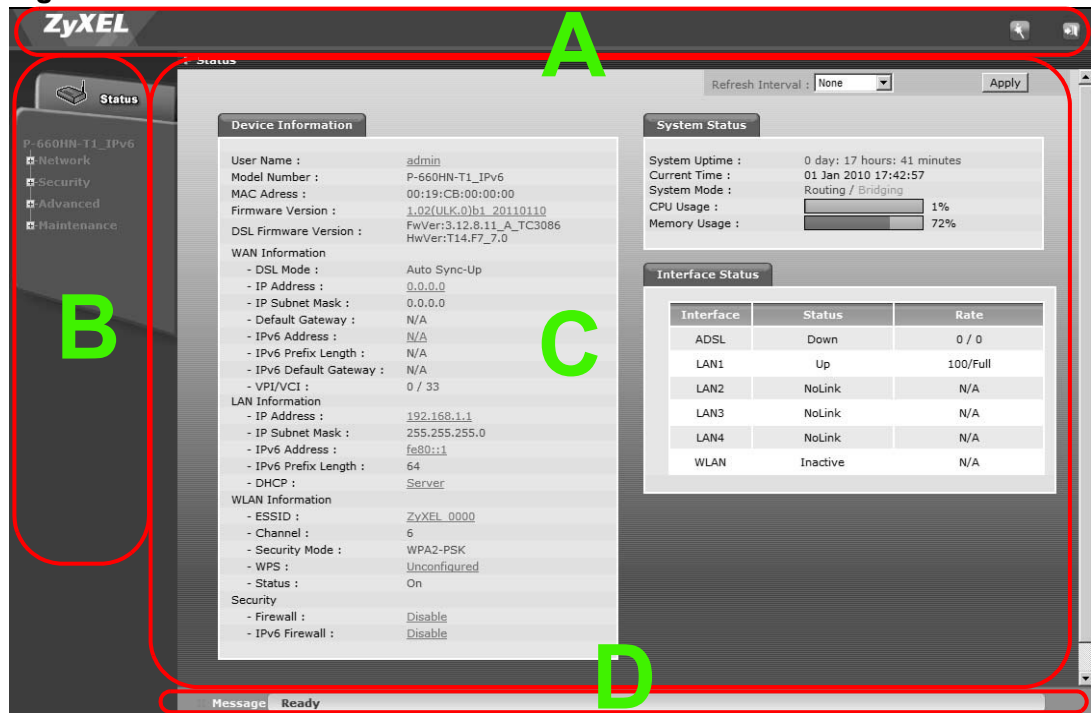
Figure 6 Replace Factory Default Certificate Screen



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

2.2 The Main Screen

Figure 7 Main Screen



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

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



2.2.1 Title Bar

The title bar provides some icons in the upper right corner.



The icons provide the following functions.

Table 2 Web Configurator Icons in the Title Bar

ICON	DESCRIPTION
	Wizards: Click this icon to go to the configuration wizards. See Chapter 5 on page 57 for more information.
	Logout: Click this icon to log out of the web configurator.

2.2.2 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 3 Navigation Panel Summary

LINK	TAB	FUNCTION
Status		This screen shows the ZyXEL Device's general device and network status information. Use this screen to access the statistics and client list.
Network		
WAN	Internet Connection	Use this screen to configure ISP parameters, WAN IP address assignment, and other advanced properties.
	More Connections	Use this screen to configure additional WAN connections.
LAN	IP	Use this screen to configure LAN TCP/IP settings, and other advanced properties.
	DHCP Server	Use this screen to configure LAN DHCP settings and DNS server.
	Client List	Use this screen to view current DHCP client information and to assign specific IP addresses to individual MAC addresses (and host names).
	IP Alias	Use this screen to partition your LAN interface into subnets.
	IPv6	Use this screen to configure the IPv6 settings on the ZyXEL device's LAN interface.
Wireless LAN	AP	Use this screen to configure the wireless LAN settings and WLAN authentication/security settings.
	More AP	Use this screen to configure multiple BSSs on the ZyXEL Device.
	WPS	Use this screen to configure and view your WPS (Wi-Fi Protected Setup) settings.
	WPS Station	Use this screen to set up a WPS wireless network.
NAT	General	Use this screen to enable NAT.
	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	ALG	Use this screen to enable or disable SIP ALG.
Security		
Firewall		Use this screen to activate/deactivate the firewall and SPI (Security Parameter Index).
Filter	URL Filter	Use this screen to block access to certain URL web sites.
	IP Filter	Use this screen to configure IPfiltering rules for incoming or outgoing traffic.
	IPv6 Filter	Use this screen to configure IPv6 filtering rules for incoming or outgoing traffic
Certificate		Use this screen to view and manage the list of trusted CAs.
Advanced		

Table 3 Navigation Panel Summary

LINK	TAB	FUNCTION
Static Route	Static Route	Use this screen to configure IP static routes to tell your device about networks beyond the directly connected remote nodes.
	IPv6 Static Route	Use this screen to configure IPv6 static routes.
QoS	General	Use this screen to enable QoS and traffic prioritizing.
	Class Setup	Use this screen to configure QoS rules and actions.
Dynamic DNS		This screen allows you to use a static hostname alias for a dynamic IP address.
Remote MGMT	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the ZyXEL Device.
	Telnet	Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the ZyXEL Device.
	FTP	Use this screen to configure through which interface(s) and from which IP address(es) users can use FTP to access the ZyXEL Device.
	SNMP	Use this screen to configure through which interface(s) and from which IP address(es) users can access the SNMP agent on the ZyXEL Device.
	ICMP	Use this screen to set whether or not your device will respond to pings and probes for services that you have not made available.
UPnP		Use this screen to turn UPnP on or off.
CWMP		Use this screen to have a management server manage the ZyXEL Device with TR-069.
Maintenance		
System	General	Use this screen to configure your device's password.
	Time and Date	Use this screen to change your ZyXEL Device's time and date.
Logs	View Log	Use this screen to view the logs for the level that you selected.
	Log Settings	Use this screen to change your ZyXEL Device's log settings.
Tools	Firmware	Use this screen to upload firmware to your device.
	Configuration	Use this screen to backup and restore your device's configuration (settings) or reset the factory default settings.
	Restart	This screen allows you to reboot the ZyXEL Device without turning the power off.
Diagnostic	General	Use this screen to test the connections to other devices.
	DSL Line	This screen displays information to help you identify problems with the DSL connection.

2.2.3 Main Window

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

Right after you log in, the **Status** screen is displayed. See [Chapter 3 on page 37](#) for more information about the **Status** screen.

2.2.4 Status Bar

Check the status bar when you click **Apply** or **OK** to verify that the configuration has been updated.

Status Screens

3.1 Overview

Use the **Status** screens to look at the current status of the device, system resources, and interfaces (LAN and WAN). The **Status** screen also provides detailed information from DHCP and statistics from bandwidth management, and traffic.

3.2 The Status Screen

Use this screen to view the status of the ZyXEL Device. Click **Status** to open this screen.

Figure 8 Status Screen

The screenshot displays the ZyXEL Status screen with the following sections:

- Device Information:**
 - User Name : admin
 - Model Number : P-660HN-T1_IPv6
 - MAC Address : 00:19:CB:00:00:00
 - Firmware Version : 1.02(U.L.K.0)b1_20110110
 - DSL Firmware Version : FwVer:3.12.8.11_A_TC3086 HwVer:T14.F7_7.0
- WAN Information:**
 - DSL Mode : Auto Sync-Up
 - IP Address : 0.0.0.0
 - IP Subnet Mask : 0.0.0.0
 - Default Gateway : N/A
 - IPv6 Address : N/A
 - IPv6 Prefix Length : N/A
 - IPv6 Default Gateway : N/A
 - VPI/VCI : 0 / 33
- LAN Information:**
 - IP Address : 192.168.1.1
 - IP Subnet Mask : 255.255.255.0
 - IPv6 Address : fe80::1
 - IPv6 Prefix Length : 64
 - DHCP : Server
- WLAN Information:**
 - ESSID : ZyXEL_0000
 - Channel : 6
 - Security Mode : WPA2-PSK
 - WPS : Unconfigured
 - Status : On
- Security:**
 - Firewall : Disable
 - IPv6 Firewall : Disable
- System Status:**
 - System Uptime : 0 day : 17 hours : 41 minutes
 - Current Time : 01 Jan 2010 17:44:42
 - System Mode : Routing / Bridging
 - CPU Usage : 1%
 - Memory Usage : 72%
- Interface Status:**

Interface	Status	Rate
ADSL	Down	0 / 0
LAN1	Up	100/Full
LAN2	NoLink	N/A
LAN3	NoLink	N/A
LAN4	NoLink	N/A
WLAN	Inactive	N/A

Each field is described in the following table.

Table 4 Status Screen

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the ZyXEL Device to update this screen.
Apply	Click this to update this screen immediately.
Device Information	
User Name	This field displays the ZyXEL Device system name. It is used for identification.
Model Number	This is the model name of your device.
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your ZyXEL Device.
Firmware Version	This is the current version of the firmware inside the device. Click this to go to the screen where you can change it.
DSL Firmware Version	This is the current version of the device's DSL modem code.
WAN Information	
DSL Mode	This is the DSL standard that your ZyXEL Device is using.
IP Address	This is the current IP address of the ZyXEL Device in the WAN. Click this to go to the screen where you can change it.
IP Subnet Mask	This is the current subnet mask in the WAN.
Default Gateway	This is the IP address of the default gateway, if applicable.
IPv6 Address	This is the current IPv6 address of the ZyXEL Device in the WAN. Click this to go to the screen where you can change it.
IPv6 Prefix Length	This is the current IPv6 prefix length in the WAN.
IPv6 Default Gateway	This is the IPv6 address of the default gateway, if applicable.
VPI/VCI	This is the Virtual Path Identifier and Virtual Channel Identifier that you entered in the wizard or WAN screen.
LAN Information	
IP Address	This is the current IP address of the ZyXEL Device in the LAN. Click this to go to the screen where you can change it.
IP Subnet Mask	This is the current subnet mask in the LAN.
IPv6 Address	This is the current IPv6 address of the ZyXEL Device in the LAN. Click this to go to the screen where you can change it.
IPv6 Prefix Length	This is the current IPv6 prefix length in the LAN.

Table 4 Status Screen

LABEL	DESCRIPTION
DHCP	<p>This field displays what DHCP services the ZyXEL Device is providing to the LAN. Choices are:</p> <p>Server - The ZyXEL Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN.</p> <p>Relay - The ZyXEL Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients.</p> <p>None - The ZyXEL Device is not providing any DHCP services to the LAN.</p> <p>Click this to go to the screen where you can change it.</p>
WLAN Information	
ESSID	This is the descriptive name used to identify the ZyXEL Device in a wireless LAN. Click this to go to the screen where you can change it.
Channel	This is the channel number used by the ZyXEL Device now.
Security Mode	This displays the type of security mode the ZyXEL Device is using in the wireless LAN.
WPS	This displays whether WPS is configured. Click this to go to the screen where you can configure the settings.
Status	This displays whether WLAN is activated.
Security	
Firewall	This displays whether or not the ZyXEL Device's firewall is activated. Click this to go to the screen where you can change it.
System Status	
System Uptime	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 > Tools > Restart), or when you reset it.
Current Time	This field displays the current date and time in the ZyXEL Device. You can change this in Maintenance > System > Time Setting .
System Mode	This displays whether the ZyXEL Device is functioning as a router or a bridge.
CPU Usage	This field displays what percentage of the ZyXEL Device's processing ability is currently used. When this percentage is close to 100%, the ZyXEL Device is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using QoS; see Chapter 14 on page 165).
Memory Usage	This field displays what percentage of the ZyXEL Device's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100%, the ZyXEL Device is probably becoming unstable, and you should restart the device. See Section 21.4 on page 215 , or turn off the device (unplug the power) for a few seconds.
Interface Status	
Interface	This column displays each interface the ZyXEL Device has.

Table 4 Status Screen

LABEL	DESCRIPTION
Status	<p>This field indicates whether or not the ZyXEL Device is using the interface.</p> <p>For the DSL interface, this field displays Down (line is down), Up (line is up or connected) and Drop (dropping a call) if you're using PPPoE encapsulation.</p> <p>For the LAN interface, this field displays Up when the ZyXEL Device is using the interface and NoLink when the ZyXEL Device is not using the interface.</p> <p>For the WLAN interface, it displays Active when WLAN is enabled or InActive when WLAN is disabled.</p>
Rate	<p>For the LAN interface, this displays the port speed and duplex setting.</p> <p>For the DSL interface, it displays the downstream and upstream transmission rate.</p> <p>For the WLAN interface, it displays the maximum transmission rate when WLAN is enabled or N/A when WLAN is disabled.</p>

Tutorials

4.1 Overview

This chapter shows you how to use the ZyXEL Device's various features.

- [Setting Up a Secure Wireless Network](#), see page 41
- [Configuring the MAC Address Filter](#), see page 48
- [Configuring Static Route for Routing to Another Network](#), see page 50
- [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.](#), see page 52
- [Multiple WAN Connections Example](#), see page 53

4.2 Setting Up a Secure Wireless Network

Thomas wants to set up a wireless network so that he can use his notebook to access the Internet. In this wireless network, the ZyXEL Device serves as an access point (AP), and the notebook is the wireless client. The wireless client can access the Internet through the AP.



Thomas has to configure the wireless network settings on the ZyXEL Device. Then he can set up a wireless network using WPS ([Section 4.2.2 on page 43](#)) or manual configuration ([Section 4.2.3 on page 48](#)).

4.2.1 Configuring the Wireless Network Settings

This example uses the following parameters to set up a wireless network.

SSID	Example
Security Mode	WPA2-PSK
Pre-Shared Key	DoNotStealMyWirelessNetwork
802.11 Mode	802.11b+g+n

- 1 Click **Network > Wireless LAN** to open the **AP** screen. Configure the screen using the provided parameters (see [page 42](#)). Click **Apply**.

The screenshot shows the 'Wireless Setup' configuration page. The 'Enable Wireless LAN' checkbox is checked. The 'Channel Selection' dropdown is set to '06' and the 'Current Channel' is '6'. In the 'Common Setup' section, the 'Name(SSID)' is 'ZyXEL_0000', 'Security Mode' is 'WPA2-PSK', and 'Pre-Shared Key' is 'DoNotStealMyWirelessNetwork'. The 'Apply' button is circled in red.

- 2 Click the **Advanced Setup** button and select **802.11b+g+n** in the **802.11 Mode** field. Click **Apply**.

The screenshot shows the 'Wireless Advanced Setup' configuration page. The '802.11 Mode' dropdown is set to '802.11b+g+n'. The 'Apply' button is circled in red.

Thomas can now use the WPS feature to establish a wireless connection between his notebook and the ZyXEL Device (see [Section 4.2.2 on page 43](#)). He can also use the notebook's wireless client to search for the ZyXEL Device (see [Section 4.2.3 on page 48](#)).

4.2.2 Using WPS

This section shows you how to set up a wireless network using WPS. It uses the ZyXEL Device as the AP and ZyXEL NWD210N as the wireless client which connects to the notebook.

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

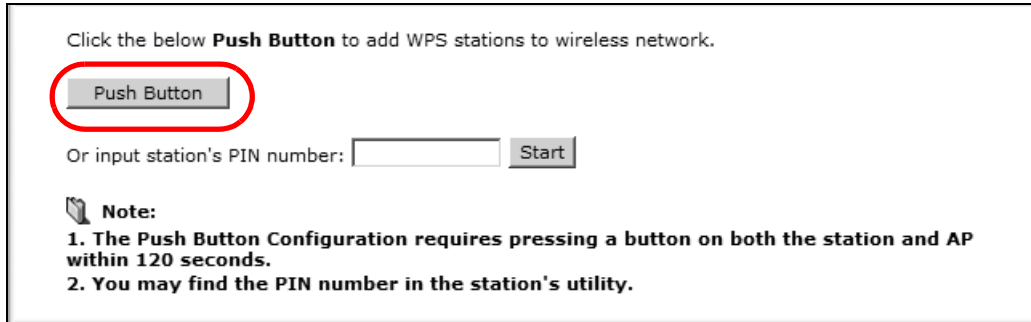
There are two WPS methods to set up the wireless client settings:

- **Push Button Configuration (PBC)** - simply press a button. This is the easier of the two methods.
- **PIN Configuration** - configure a Personal Identification Number (PIN) on the ZyXEL Device. A wireless client must also use the same PIN in order to download the wireless network settings from the ZyXEL Device.

Push Button Configuration (PBC)

- 1 Make sure that your ZyXEL Device is turned on and your notebook is within the cover range of the wireless signal.
- 2 Make sure that you have installed the wireless client driver and utility in your notebook.
- 3 In the wireless client utility, go to the WPS setting page. Enable WPS and press the WPS button (**Start** or **WPS** button).

- 4 Push and hold the **WPS** button located on the ZyXEL Device's rear panel for more than 1-5 seconds. Alternatively, you may log into ZyXEL Device's web configurator and click the **Push Button** in the **Network > Wireless LAN > WPS Station** screen.

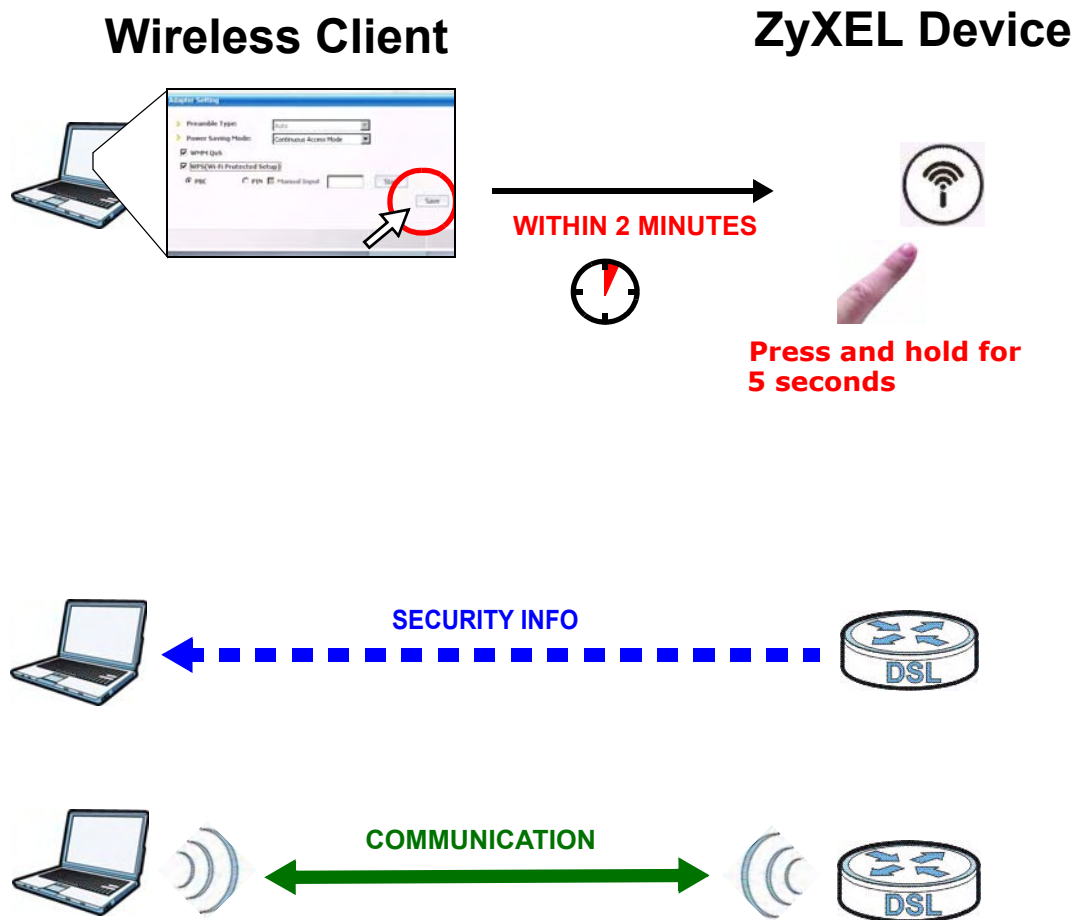


Note: Your ZyXEL Device has a WPS button located on its rear panel as well as a WPS button in its configuration utility. Both buttons have exactly the same function: you can use one or the other.

Note: It doesn't matter which button is pressed first. You must press the second button within two minutes of pressing the first one.

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

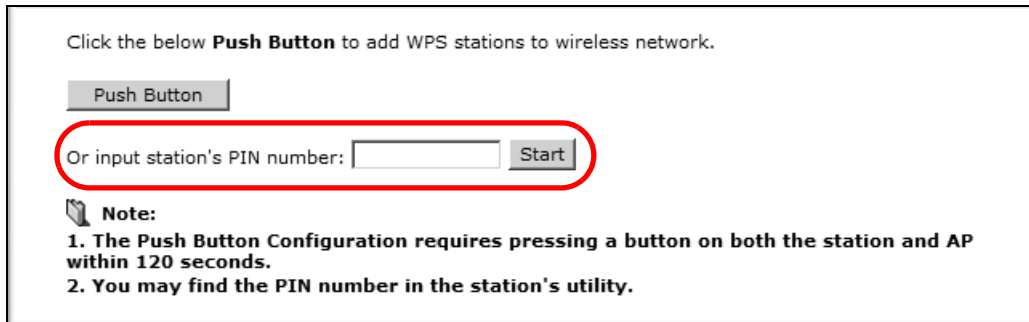
The following figure shows you an example of how to set up a wireless network and its security by pressing a button on both ZyXEL Device and wireless client.



PIN Configuration

When you use the PIN configuration method, you need to use both the ZyXEL Device's web configurator and the wireless client's utility.

- 1 Launch your wireless client's configuration utility. Go to the WPS settings and select the PIN method to get a PIN number.
- 2 Enter the PIN number in the **PIN** field in the **Network > Wireless LAN > WPS Station** screen on the ZyXEL Device.



Click the below **Push Button** to add WPS stations to wireless network.

Or input station's PIN number:

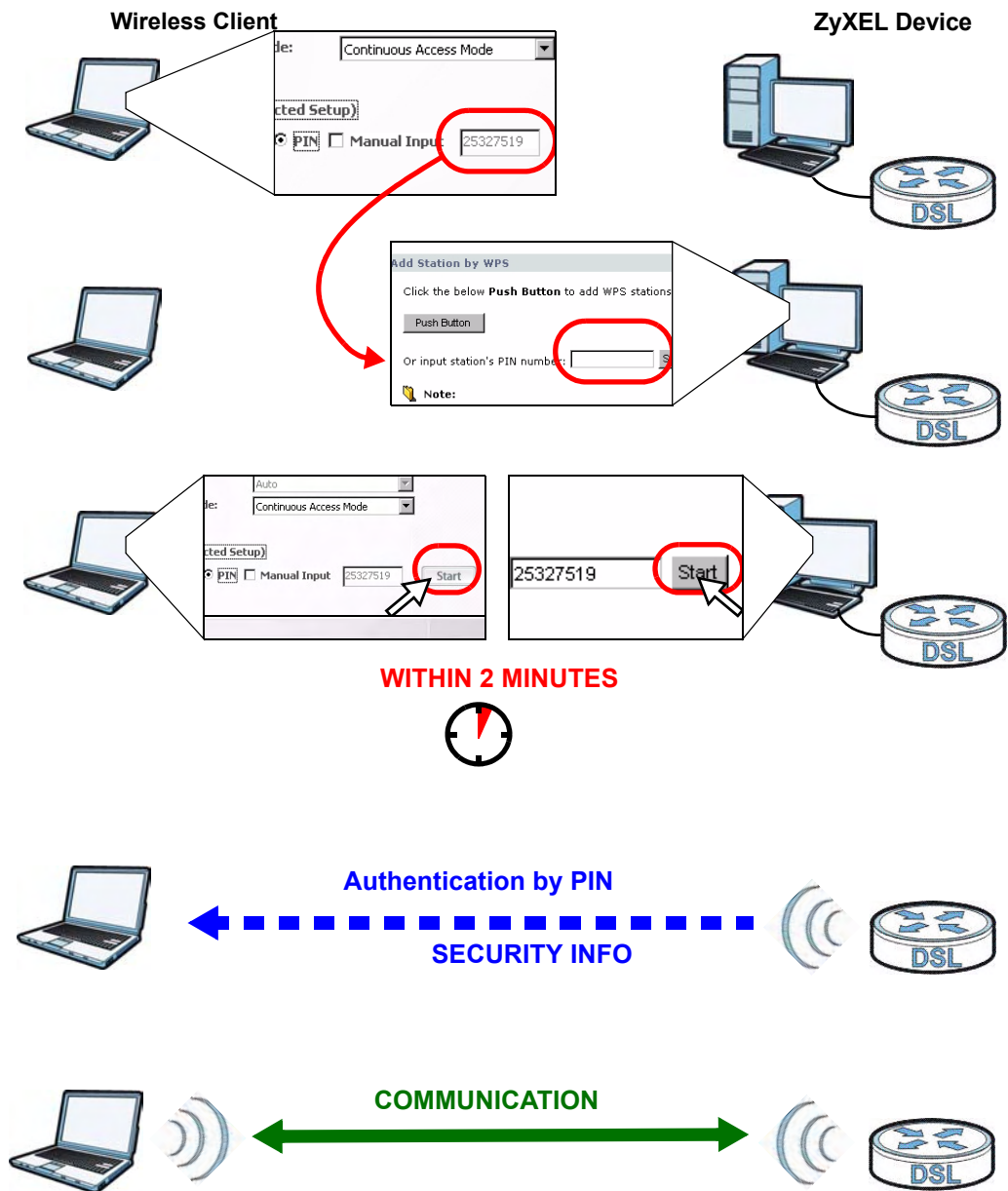
Note:

1. The **Push Button Configuration** requires pressing a button on both the station and AP within 120 seconds.
2. You may find the **PIN** number in the station's utility.

- 3 Click the **Start** buttons (or the button next to the PIN field) on both the wireless client utility screen and the ZyXEL Device's **WPS Station** 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. The wireless client is then able to communicate with the ZyXEL Device securely.

The following figure shows you how to set up a wireless network and its security on a ZyXEL Device and a wireless client by using PIN method.



4.2.3 Without WPS

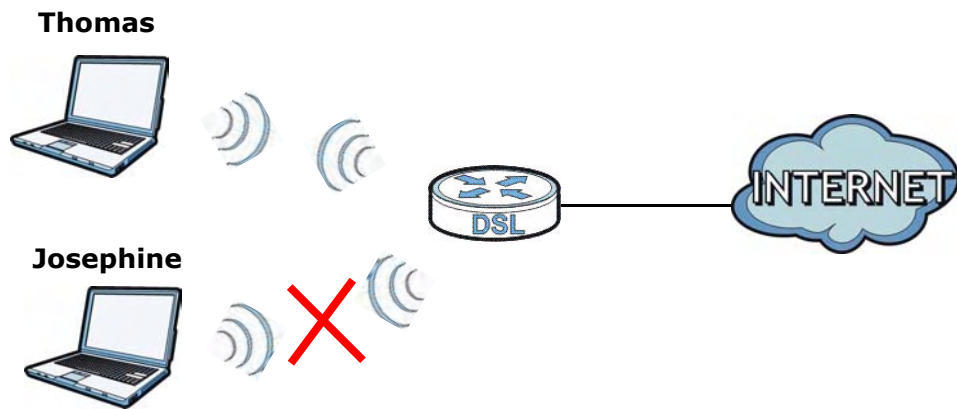
Use the wireless adapter's utility installed on the notebook to search for the "Example" SSID. Then enter the "DoNotStealMyWirelessNetwork" pre-shared key to establish an wireless Internet connection.

Note: The ZyXEL Device supports IEEE 802.11b and IEEE 802.11g wireless clients. Make sure that your notebook or computer's wireless adapter supports one of these standards.

4.3 Configuring the MAC Address Filter

Thomas noticed that his daughter Josephine spends too much time surfing the web and downloading media files. He decided to prevent Josephine from accessing the Internet so that she can concentrate on preparing for her final exams.

Josephine's computer connects wirelessly to the Internet through the ZyXEL Device. Thomas can deny access to the wireless network using the MAC address of Josephine's computer.



- 1 Click **Network > LAN > Client List** to open the following screen. Look for the MAC address of Josephine's computer.

DHCP Client Table

IP Address: MAC Address:

#	Status	HostName	IPAddress	MacAddress	Remove	Modify
1		twpc13477	192.168.1.33	00:0F:FE:32:B4:12	<input type="checkbox"/>	
2		Josephine-PC	192.168.1.34	00:1E:52:C3:5C:1B	<input type="checkbox"/>	

- 2 Click **Network > Wireless LAN** to open the **AP** screen. Click the **Edit** button in the **MAC Filter** field.

AP More AP WPS WPS Station

Wireless Setup

Enable Wireless LAN
 Channel Selection: Current Channel:

Common Setup

Name(SSID):
 Hide SSID
 Security Mode:
 WPA Compatible
 Pre-Shared Key:
 WPA Group Key Update Timer: (seconds)
 MAC Filter: Deny Association
 Enable QoS

- 3 Select **Enable MAC Filter** and **Deny Association**. Enter the MAC address you found in the **Client List** screen. Click **Apply**.

Mac Filter

Enable MAC Filter

Association Allow Deny

Set	Mac Address	Set	MAC Address
1	00:1E:52:C3:5C:1B	2	
3		4	
5		6	
7		8	
9		10	
11		12	
13		14	
15		16	

Back Apply Reset

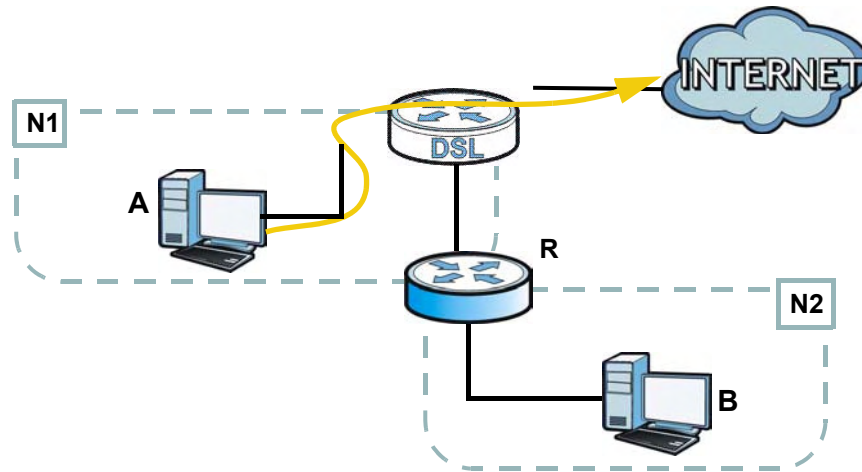
Josephine will no longer be able to access the Internet through the ZyXEL Device.

4.4 Configuring Static Route for Routing to Another Network

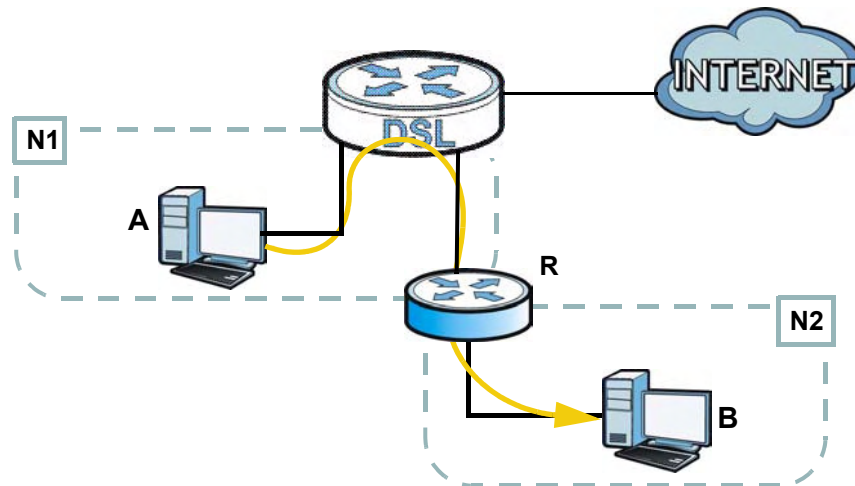
In order to extend your Intranet and control traffic flowing directions, you may connect a router to the ZyXEL Device's LAN. The router may be used to separate two department networks. This tutorial shows how to configure a static routing rule for two network routings.

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:

Table 5 IP Settings in this Tutorial

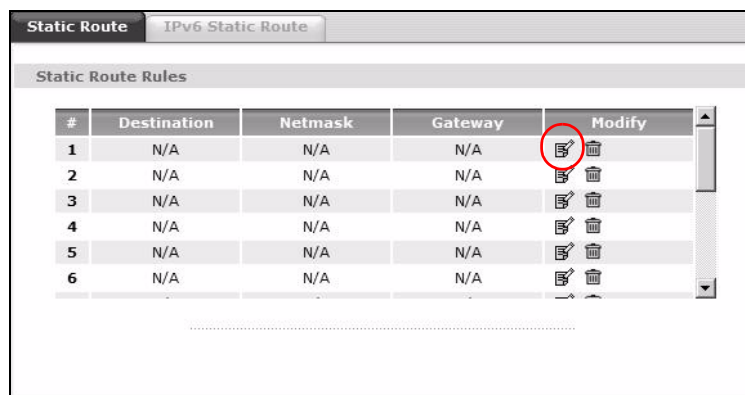
DEVICE / COMPUTER	IP ADDRESS
The ZyXEL Device's WAN	172.16.1.1
The ZyXEL Device's LAN	192.168.1.1
A	192.168.1.34
R's N1	192.168.1.253

Table 5 IP Settings in this Tutorial

DEVICE / COMPUTER	IP ADDRESS
R's N2	192.168.10.2
B	192.168.10.33

To configure a static route to route traffic from **N1** to **N2**:

- 1 Log into the ZyXEL Device's Web Configurator in advanced mode.
- 2 Click **Advanced** > **Static Route**.
- 3 Click **Edit** on a new rule in the **Static Route** screen.



- 4 Configure the **Static Route Setup** screen using the following settings:
 - 4a Type **192.168.10.0** 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.

Static Route Setup

Destination IP Address: 192.168.10.0

IP Subnet Mask: 255.255.255.0

Gateway IP Address: 192.168.1.253

Note :
The Destination IP Address and IP Subnet Mask fields must be matched; e.g. host/255.255.255.255 or subnet/255.255.255.0.

Back Apply Cancel

- 4a Click **Apply**.

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.

4.5 Multiple WAN Connections Example

This example shows an application for multiple WAN connections.

Your ISP may configure more than one WAN connection on the ZyXEL Device to record traffic statistics or calculate service charges.

In [Figure 9](#), three WAN connections are configured over the ADSL line:

- The connection with VPI/VCI, **0/33**, is dedicated for Media-On-Demand (MOD) service.
- The connection with VPI/VCI, **0/34**, is dedicated for VoIP service.
- The connection with VPI/VCI, **0/35**, is dedicated for general data transmission.

Figure 9 Example for Multiple WAN Connections

#	Active	Name:	VPI/VCI	Encapsulation	Modify
1		Internet Connection	0/33	ENET ENCAP	
2	<input checked="" type="checkbox"/>	VoIP	0/34	ENET ENCAP	
3	<input checked="" type="checkbox"/>	Data	0/35	ENET ENCAP	
4	-	--	--	--	
5	-	--	--	--	
6	-	--	--	--	
7	-	--	--	--	
8	-	--	--	--	

PART II

Technical Reference

Internet and Wireless Setup Wizard

5.1 Overview

Use the wizard setup screens to configure your system for Internet access with the information given to you by your ISP.

Note: See the advanced menu chapters for background information on these fields.

5.2 Internet Access Wizard Setup


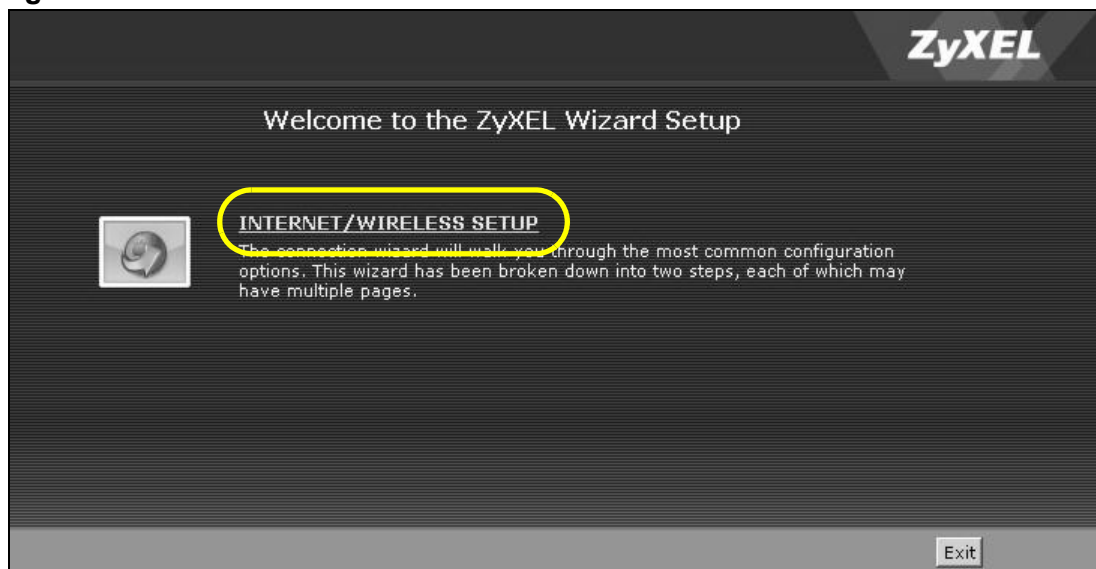
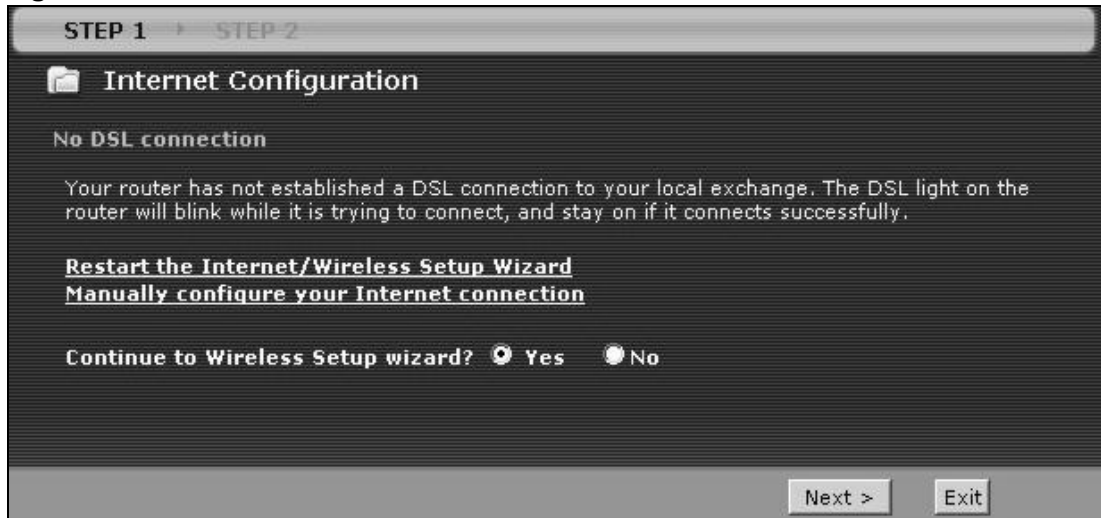
- 1 After you enter the password to access the web configurator, click the wizard icon () in the top right corner of the web configurator to go to the wizards.
- 2 Click **INTERNET/WIRELESS SETUP** to configure the system for Internet access and wireless connection.

Figure 10 Wizard Welcome



- 3 Your ZyXEL device attempts to detect your DSL connection and your connection type.
 - 3a The following screen appears if a connection is not detected. Check your hardware connections and click **Restart the INTERNET/WIRELESS SETUP Wizard** to return to the wizard welcome screen. If you still cannot connect, click **Manually configure your Internet connection**. Follow the directions in the wizard and enter your Internet setup information as provided to you by your ISP. See [Section 5.2.1 on page 60](#) for more details. If you would like to skip your Internet setup and configure the wireless LAN settings, leave **Yes** selected and click **Next**.

Figure 11 Auto Detection: No DSL Connection



- 3b** The following screen displays if a PPPoE or PPPoA connection is detected. Enter your Internet account information (username, password and/or service name) exactly as provided by your ISP. Then click **Next** and see [Section 5.3 on page 66](#) for wireless connection wizard setup.

Figure 12 Auto-Detection: PPPoE

The screenshot shows a wizard window titled "Internet Configuration" with a progress bar at the top indicating "STEP 1" and "STEP 2". Below the title is a folder icon and the text "Internet Configuration". Underneath, it says "Auto-Detected ISP". The "Connection Type" is listed as "PPP over Ethernet (PPPoE)". A section titled "ISP Parameters for Internet Access" contains the instruction: "Please enter the User Name and Password given to you by your Internet Service Provider here. If your ISP gave you a Service Name, enter it in the third field". There are three input fields: "User Name", "Password", and "Service Name" (with "(optional)" to its right). At the bottom right, there are three buttons: "< Back", "Next >", and "Exit".

- 3c** The following screen appears if the ZyXEL device detects a connection but not the connection type. Click **Next** and refer to [Section 5.2.1 on page 60](#) on how to manually configure the ZyXEL Device for Internet access.

Figure 13 Auto Detection: Failed

The screenshot shows a wizard window titled "Internet Configuration" with a progress bar at the top indicating "STEP 1" and "STEP 2". Below the title is a folder icon and the text "Internet Configuration". Underneath, it says "Auto-Detected ISP". The "Connection Type" field contains the message: "Detection Failed. Please make sure the DSL cable is connected. Click the 'Next' button below to manually configure your Internet connection". Below this is a "Note:" section with a hand icon, stating: "This wizard can only automatically detect PPP over Ethernet (PPPoE), PPP over ATM (PPPoA), or dynamically assigned Ethernet Internet connections. Your Internet connection may use a Static IP address which cannot be detected automatically." At the bottom right, there are three buttons: "<Back", "Next >", and "Exit".

5.2.1 Manual Configuration

- 1 If the ZyXEL Device fails to detect your DSL connection type but the physical line is connected, enter your Internet access information in the wizard screen exactly as your service provider gave it to you. Leave the defaults in any fields for which you were not given information.

Figure 14 Internet Access Wizard Setup: ISP Parameters

The screenshot shows a wizard window titled "Internet Configuration" with a progress bar at the top indicating "STEP 1" is active. Below the title is the section "ISP Parameters for Internet Access". A paragraph of text asks the user to verify settings with their ISP. The configuration fields are:

- Mode:** A dropdown menu set to "Routing". Below it, text explains that "Routing" is the default for multiple computers sharing an account, while "Bridge" is for individual IP addresses.
- Encapsulation:** A dropdown menu set to "ENET ENCAP". Below it, text explains that the user should select the method used by their ISP, with "ENET ENCAP" being equivalent to "Static IP" or "Dynamic IP".
- Multiplexing:** A dropdown menu set to "LLC". Below it, text explains that the user should select the multiplexing type used by their ISP.
- Virtual Circuit ID:** Two input fields: "VPI" with the value "8" and "VCI" with the value "35". Below these fields, text explains that VPI is the Virtual Path Identifier and VCI is the Virtual Channel Identifier, with valid ranges of 0-255 for VPI and 32-65535 for VCI.

At the bottom of the window are three buttons: "< Back", "Next >", and "Exit".

The following table describes the fields in this screen.

Table 6 Internet Access Wizard Setup: ISP Parameters

LABEL	DESCRIPTION
Mode	Select Routing (default) from the drop-down list box if your ISP give you one IP address only and you want multiple computers to share an Internet account. Select Bridge when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. If you select Bridge , you cannot use Firewall, DHCP server and NAT on the ZyXEL Device.
Encapsulation	Select the encapsulation type your ISP uses from the Encapsulation drop-down list box. Choices vary depending on what you select in the Mode field. If you select Routing in the Mode field, select PPPoA , RFC 1483 , ENET ENCAP or PPPoE . If you select Bridge in the Mode field, only RFC 1483 method of encapsulation is available.

Table 6 Internet Access Wizard Setup: ISP Parameters

LABEL	DESCRIPTION
Multiplexing	Select the multiplexing method used by your ISP from the Multiplex drop-down list box either VC-based or LLC-based.
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.
VPI	Enter the VPI assigned to you. This field may already be configured.
VCI	Enter the VCI assigned to you. This field may already be configured.
Back	Click this to return to the previous screen without saving.
Next	Click this to continue to the next wizard screen. The next wizard screen you see depends on what protocol you chose above.
Exit	Click this to close the wizard screen without saving.

- 2 The next wizard screen varies depending on what mode and encapsulation type you use. All screens shown are with routing mode. Configure the fields and click **Next** to continue. See [Section 5.3 on page 66](#) for wireless connection wizard setup

Figure 15 Internet Connection with PPPoE

STEP 1 → STEP 2

Internet Configuration

ISP Parameters for Internet Access
Please enter the User Name and Password given to you by your Internet Service Provider here. If your ISP gave you a Service Name, enter it in the third field

User Name

Password

Service Name (optional)

Note:
Device is automatically configured to obtain an IP address automatically. The ISP will assign you a different one each time you connect to the Internet.

< Back Apply Exit

The following table describes the fields in this screen.

Table 7 Internet Connection with PPPoE

LABEL	DESCRIPTION
User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
Service Name	Type the name of your PPPoE service here.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Exit	Click this to close the wizard screen without saving.

Figure 16 Internet Connection with RFC 1483

STEP 1 → STEP 2

Internet Configuration

ISP Parameters for Internet Access

IP Address

< Back Next > Exit

The following table describes the fields in this screen.

Table 8 Internet Connection with RFC 1483

LABEL	DESCRIPTION
IP Address	This field is available if you select Routing in the Mode field. Type your ISP assigned IP address in this field.
Back	Click this to return to the previous screen without saving.
Next	Click this to continue to the next wizard screen.
Exit	Click this to close the wizard screen without saving.

Figure 17 Internet Connection with ENET ENCAP

STEP 1 STEP 2

Internet Configuration

ISP Parameters for Internet Access

Select 'Obtain an IP Address Automatically' if your ISP assigns you a dynamic IP address (DHCP); otherwise select 'Static IP Address' and type the static IP information your ISP gave you.

Obtain an IP Address Automatically
 Static IP Address

IP Address 0.0.0.0
 Subnet Mask 0.0.0.0
 Gateway IP address 0.0.0.0
 First DNS Server 0.0.0.0
 Second DNS Server 0.0.0.0

<Back Apply Exit

The following table describes the fields in this screen.

Table 9 Internet Connection with ENET ENCAP

LABEL	DESCRIPTION
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 Obtain an IP Address Automatically if you have a dynamic IP address.
Static IP Address	Select Static IP Address if your ISP gave you an IP address to use.
IP Address	Enter your ISP assigned IP address.
Subnet Mask	Enter a subnet mask in dotted decimal notation. Refer to the appendix to calculate a subnet mask if you are implementing subnetting.
Gateway IP address	You must specify a gateway IP address (supplied by your ISP) when you use ENET ENCAP in the Encapsulation field in the previous screen.
First DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Second DNS Server	As above.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Exit	Click this to close the wizard screen without saving.

Figure 18 Internet Connection with PPPoA

STEP 1 STEP 2

Internet Configuration

ISP Parameters for Internet Access
Please enter the User Name and Password given to you by your Internet Service Provider here

User Name

Password

Note:
Device is automatically configured to obtain an IP address automatically. The ISP will assign you a different one each time you connect to the Internet.

< Back Apply Exit

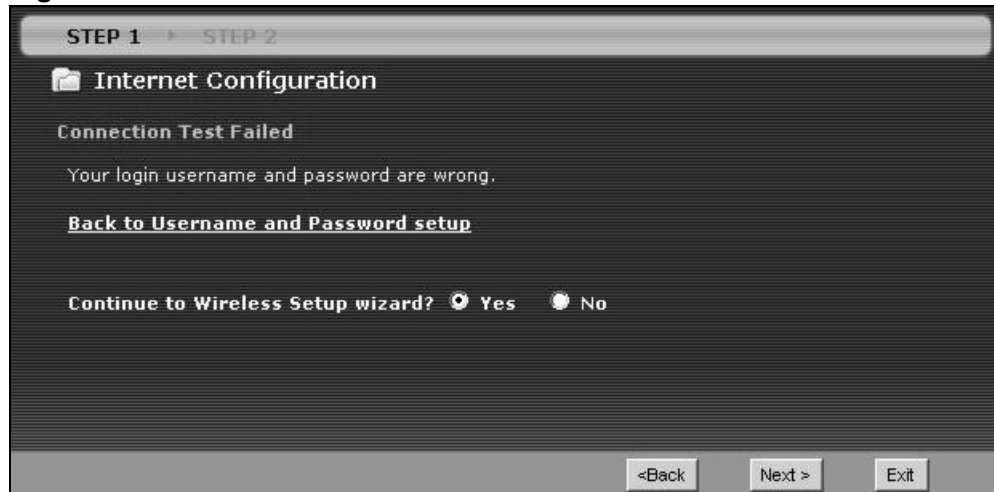
The following table describes the fields in this screen.

Table 10 Internet Connection with PPPoA

LABEL	DESCRIPTION
User Name	Enter the login name that your ISP gives you.
Password	Enter the password associated with the user name above.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Exit	Click this to close the wizard screen without saving.

- If the user name and/or password you entered for PPPoE or PPPoA connection are not correct, the screen displays as shown next. Click **Back to Username and Password setup** to go back to the screen where you can modify them.

Figure 19 Connection Test Failed-1



- If the following screen displays, check if your account is activated or click **Restart the Internet/Wireless Setup Wizard** to verify your Internet access settings.

Figure 20 Connection Test Failed-2.

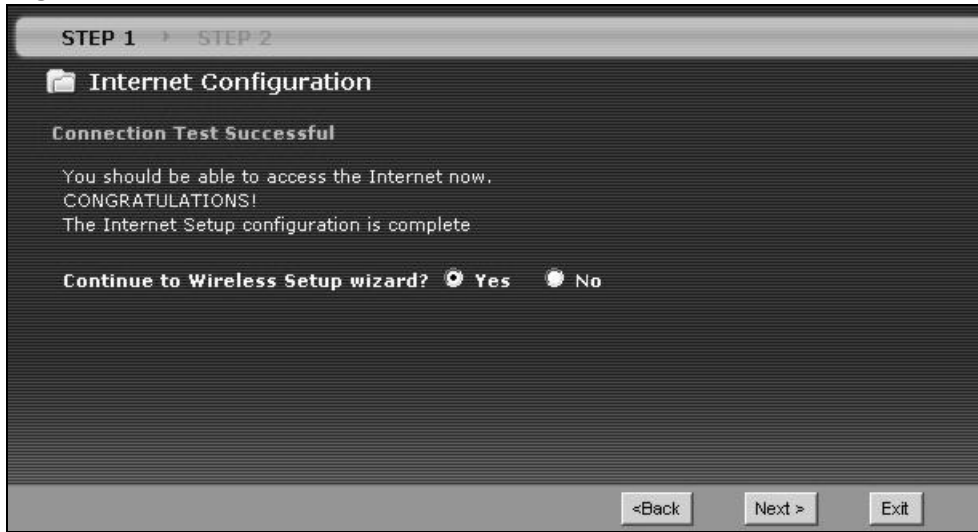


5.3 Wireless Connection Wizard Setup

After you configure the Internet access information, use the following screens to set up your wireless LAN.

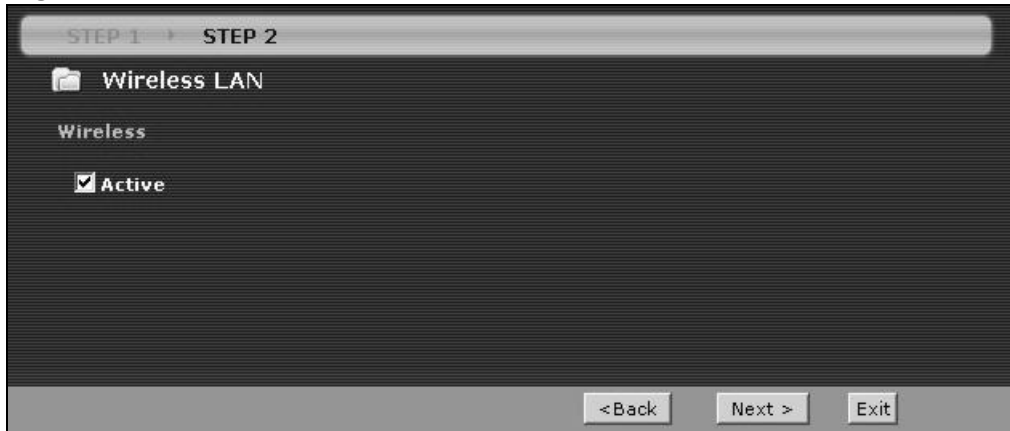
- 1 Select **Yes** and click **Next** to configure wireless settings. Otherwise, select **No** and skip to Step 6.

Figure 21 Connection Test Successful



- 2 Use this screen to activate the wireless LAN. Click **Next** to continue.

Figure 22 Wireless LAN Setup Wizard 1



The following table describes the labels in this screen.

Table 11 Wireless LAN Setup Wizard 1

LABEL	DESCRIPTION
Active	Select the check box to turn on the wireless LAN.
Back	Click this to return to the previous screen without saving.

Table 11 Wireless LAN Setup Wizard 1

LABEL	DESCRIPTION
Next	Click this to continue to the next wizard screen.
Exit	Click this to close the wizard screen without saving.

- 3 Configure your wireless settings in this screen. Click **Next**.

Figure 23 Wireless LAN

The following table describes the labels in this screen.

Table 12 Wireless LAN Setup Wizard 2

LABEL	DESCRIPTION
Network Name(SSID)	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you change this field on the ZyXEL Device, make sure all wireless stations use the same SSID in order to access the network.
Channel Selection	The range of radio frequencies used by IEEE 802.11b/g wireless devices is called a channel. Select a channel ID that is not already in use by a neighboring device.
Security	Select Manually assign a WPA-PSK key to configure a Pre-Shared Key (WPA-PSK). Choose this option only if your wireless clients support WPA. See Section 5.3.1 on page 68 for more information. Select Manually assign a WEP key to configure a WEP Key. See Section 5.3.2 on page 69 for more information. Select Disable wireless security to have no wireless LAN security configured and your network is accessible to any wireless networking device that is within range.
Back	Click this to return to the previous screen without saving.

Table 12 Wireless LAN Setup Wizard 2

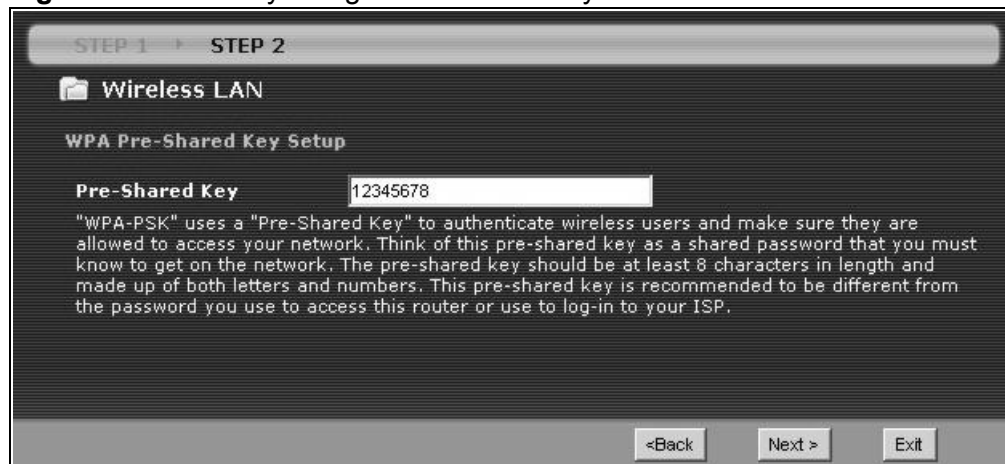
LABEL	DESCRIPTION
Next	Click this to continue to the next wizard screen.
Exit	Click this to close the wizard screen without saving.

Note: The wireless stations and ZyXEL Device must use the same SSID, channel ID and WEP encryption key (if WEP is enabled), WPA-PSK (if WPA-PSK is enabled) for wireless communication.

- This screen varies depending on the security mode you selected in the previous screen. Fill in the field (if available) and click **Next**.

5.3.1 Manually Assign a WPA-PSK key

Choose **Manually assign a WPA-PSK key** in the Wireless LAN setup screen to set up a **Pre-Shared Key**.

Figure 24 Manually Assign a WPA-PSK key

The following table describes the labels in this screen.

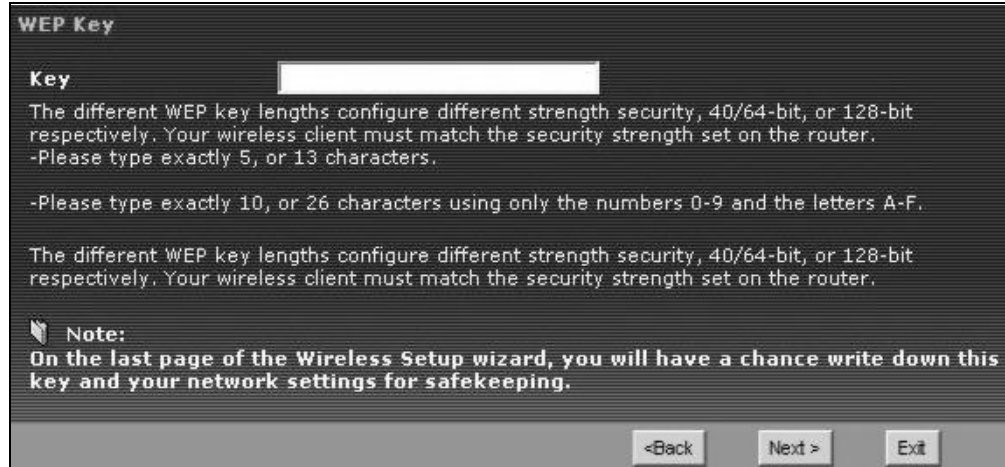
Table 13 Manually Assign a WPA-PSK key

LABEL	DESCRIPTION
Pre-Shared Key	Type from 8 to 63 case-sensitive ASCII characters. You can set up the most secure wireless connection by configuring WPA in the wireless LAN screens. You need to configure an authentication server to do this.
Back	Click this to return to the previous screen without saving.
Next	Click this to continue to the next wizard screen.
Exit	Click this to close the wizard screen without saving.

5.3.2 Manually Assign a WEP Key

Choose **Manually assign a WEP key** to setup WEP Encryption parameters.

Figure 25 Manually Assign a WEP key



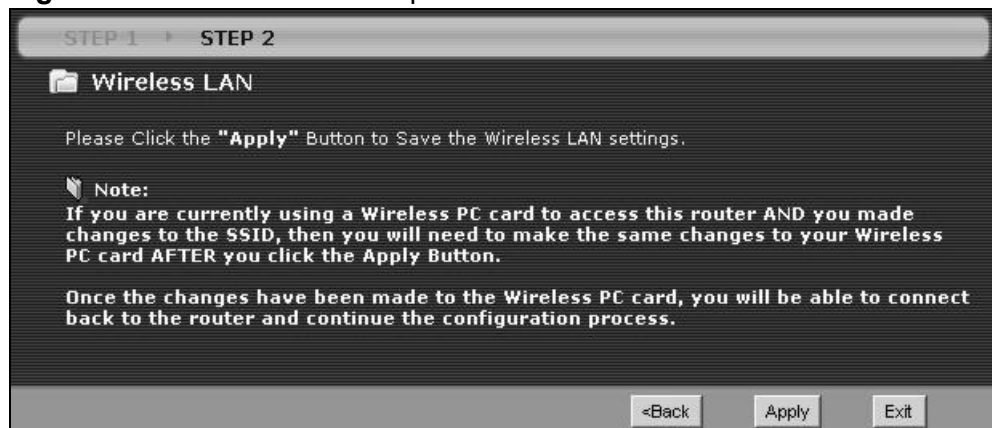
The following table describes the labels in this screen.

Table 14 Manually Assign a WEP key

LABEL	DESCRIPTION
Key	The WEP keys are used to encrypt data. Both the ZyXEL Device and the wireless stations must use the same WEP key for data transmission. Enter any 5 or 13 ASCII characters, or 10 or 26 hexadecimal characters ("0-9", "A-F") for a 64-bit or 128-bit WEP key respectively.
Back	Click this to return to the previous screen without saving.
Next	Click this to continue to the next wizard screen.
Exit	Click this to close the wizard screen without saving.

- 5 Click **Apply** to save your wireless LAN settings.

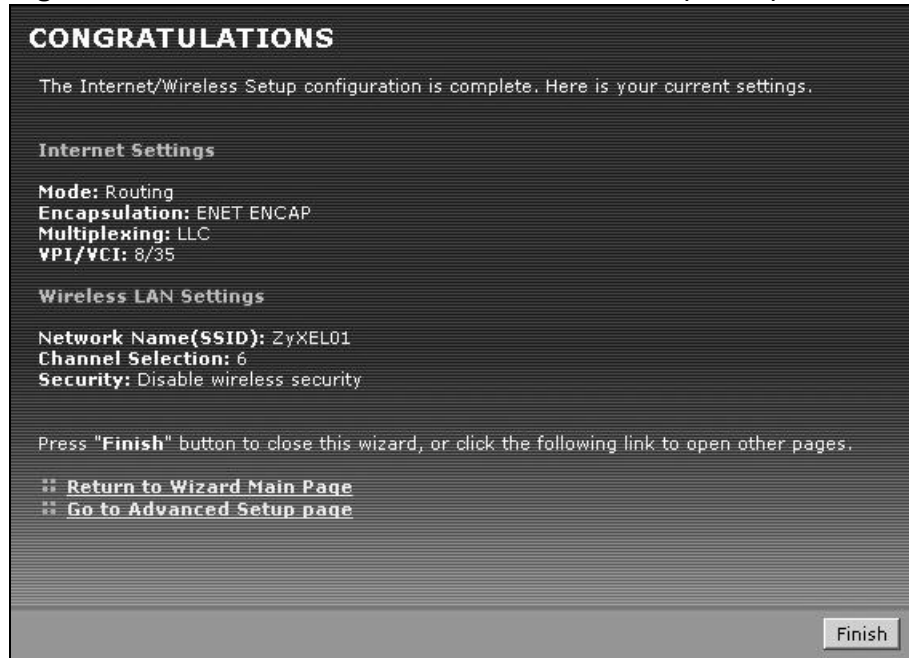
Figure 26 Wireless LAN Setup 3



- 6 Use the read-only summary table to check whether what you have configured is correct. Click **Finish** to complete and save the wizard setup.

Note: No wireless LAN settings display if you chose not to configure wireless LAN settings.

Figure 27 Internet Access and WLAN Wizard Setup Complete



- 7 Launch your web browser and navigate to www.zyxel.com. Internet access is just the beginning. Refer to the rest of this guide for more detailed information on the complete range of ZyXEL Device features. If you cannot access the Internet, open the web configurator again to confirm that the Internet settings you configured in the wizard setup are correct.

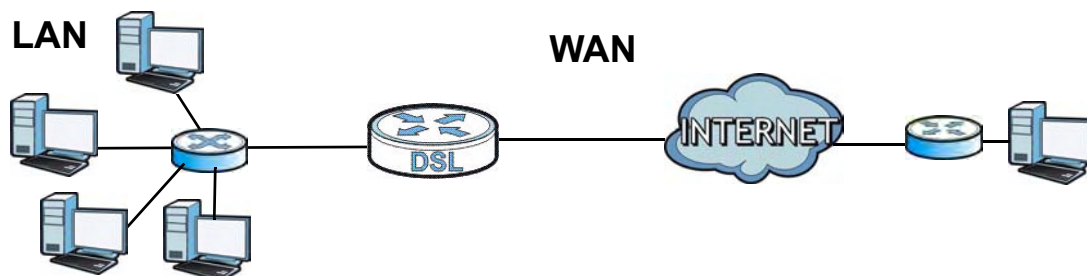
WAN Setup

6.1 Overview

This chapter describes how to configure WAN settings from the **WAN** screens. Use these screens to configure your ZyXEL Device for Internet access.

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

Figure 28 LAN and WAN



6.1.1 What You Can Do in the WAN Screens

- Use the **Internet Access Setup** screen ([Section 6.2 on page 73](#)) to configure the WAN settings on the ZyXEL Device for Internet access.
- Use the **More Connections** screen ([Section 6.3 on page 77](#)) to set up additional Internet access connections.

6.1.2 What You Need to Know About WAN

Encapsulation Method

Encapsulation is used to include data from an upper layer protocol into a lower layer protocol. To set up a WAN connection to the Internet, you need to use the same encapsulation method used by your ISP (Internet Service Provider). If your ISP offers a dial-up Internet connection using PPPoE (PPP over Ethernet) or PPPoA,

they should also provide a username and password (and service name) for user authentication.

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. It can be static (fixed) or dynamically assigned by the ISP each time the ZyXEL Device tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es) (and a gateway IP address if you use the Ethernet or ENET ENCAP encapsulation method).

Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just one.

IGMP

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. There are three versions of IGMP. IGMP version 2 and 3 are improvements over version 1, but IGMP version 1 is still in wide use.

IPv6

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The ZyXEL Device supports IPv4/IPv6 dual stack and can connect to IPv4 and IPv6 networks. See ([Appendix E on page 295](#)) for more information about IPv6.

Finding Out More

See [Section 6.4 on page 83](#) for technical background information on WAN.

6.1.3 Before You Begin

You need to know your Internet access settings such as encapsulation and WAN IP address. Get this information from your ISP.

6.2 The Internet Access Setup Screen

Use this screen to change your ZyXEL Device's WAN settings. Click **Network > WAN > Internet Access Setup**. The screen differs by the WAN type and encapsulation you select.

Figure 29 Network > WAN > Internet Access Setup (PPPoE)

The following table describes the labels in this screen.

Table 15 Network > WAN > Internet Access Setup

LABEL	DESCRIPTION
General	
Mode	Select Routing (default) from the drop-down list box if your ISP gives you one IP address only and you want multiple computers to share an Internet account. Select Bridge when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. If you select Bridge , you cannot use Firewall, DHCP server and NAT on the ZyXEL Device.

Table 15 Network > WAN > Internet Access Setup (continued)

LABEL	DESCRIPTION
Encapsulation	<p>Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the Mode field.</p> <p>If you select Routing in the Mode field, select PPPoA, RFC 1483, ENET ENCAP or PPPoE.</p> <p>If you select Bridge in the Mode field, method of encapsulation is not available.</p>
User Name	(PPPoA and PPPoE encapsulation only) Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	(PPPoA and PPPoE encapsulation only) Enter the password associated with the user name above.
Service Name	(PPPoE only) Type the name of your PPPoE service here.
Multiplexing	Select the method of multiplexing used by your ISP from the drop-down list. Choices are VC or LLC .
IPv6/IPv4 Dual Stack	If you select Enable , the ZyXEL Device can connect to IPv4 and IPv6 networks and choose the protocol for applications according to the address type. If you select Disable , the ZyXEL Device will operate in IPv4 mode.
PPP Authentication	<p>The ZyXEL Device supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms.</p> <p>Use the drop-down list box to select an authentication protocol for outgoing calls. Options are:</p> <p>AUTO - Your ZyXEL Device accepts either CHAP or PAP when requested by this remote node.</p> <p>CHAP - Your ZyXEL Device accepts CHAP only.</p> <p>PAP - Your ZyXEL Device accepts PAP only.</p>
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
IP Address	<p>This option is available if you select Routing in the Mode field.</p> <p>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.</p> <p>Select Obtain an IP Address Automatically if you have a dynamic IP address; otherwise select Static IP Address and type your ISP assigned IP address in the IP Address field below.</p>
Subnet Mask	Enter a subnet mask in dotted decimal notation.
Gateway	Specify a gateway IP address (supplied by your ISP).

Table 15 Network > WAN > Internet Access Setup (continued)

LABEL	DESCRIPTION
IPv6 Address	
Obtain an IP Address Automatically	Select this option 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 IP Address	Select this option if you have a fixed IPv6 address assigned by your ISP.
DHCP IPv6	<p>Select DHCP if you want to obtain an IPv6 address from a DHCPv6 server.</p> <p>The IP address assigned by a DHCPv6 server has priority over the IP address automatically generated by the ZyXEL Device using the IPv6 prefix from an RA.</p> <p>Select SLAAC (Stateless address autoconfiguration) to have the ZyXEL Device use the prefix to automatically generate a unique IP address that does not need to be maintained by a DHCP server.</p>
DHCP PD	Select Enable to use DHCP PD (Prefix Delegation) to allow the Zyxel Device to pass the IPv6 prefix information to its LAN hosts. The hosts can then use the prefix to generate their IPv6 addresses.
Connection (PPPoA and PPPoE encapsulation only)	
Keep Alive	Select Keep Alive when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select Connect on Demand when you don't want the connection up all the time and specify an idle time-out in the Max Idle Timeout field.
Max Idle Timeout	Specify an idle time-out in the Max Idle Timeout field when you select Connect on Demand . The default setting is 0, which means the Internet session will not timeout.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.
Advanced Setup	Click this to display the Advanced WAN Setup screen and edit more details of your WAN setup.

6.2.1 Advanced Internet Access Setup

Use this screen to edit your ZyXEL Device's advanced WAN settings. Click the **Advanced Setup** button in the **Internet Access Setup** screen. The screen appears as shown.

Figure 30 Network > WAN > Internet Access Setup: Advanced Setup

The following table describes the labels in this screen.

Table 16 Network > WAN > Internet Access Setup: Advanced Setup

LABEL	DESCRIPTION
RIP & Multicast Setup	This section is not available when you configure the ZyXEL Device to be in bridge mode.
RIP Direction	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. Use this field to control how much routing information the ZyXEL Device sends and receives on the subnet. Select the RIP direction from None , Both , In Only and Out Only .
RIP Version	This field is not configurable if you select None in the RIP Direction field. Select the RIP version from RIP-1 , RIP-2B and RIP-2M .
Multicast	Multicast packets are sent to a group of computers on the LAN and are an alternative to unicast packets (packets sent to one computer) and broadcast packets (packets sent to every computer). Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports IGMP-v1 and IGMP-v2 . Select None to disable it.
ATM QoS	

Table 16 Network > WAN > Internet Access Setup: Advanced Setup (continued)

LABEL	DESCRIPTION
ATM QoS Type	Select CBR (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select UBR (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select rtVBR (real-time Variable Bit Rate) type for applications with bursty connections that require closely controlled delay and delay variation. Select nrtVBR (non real-time Variable Bit Rate) type for connections that do not require closely controlled delay and delay variation.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustain Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

6.3 The More Connections Screen

The ZyXEL Device allows you to configure more than one Internet access connection. To configure additional Internet access connections click **Network > WAN > More Connections**. The screen differs by the encapsulation you select. When you use the **WAN > Internet Access Setup** screen to set up Internet access, you are configuring the first WAN connection.

Figure 31 Network > WAN > More Connections

Internet Connection		More Connections			
#	Active	Node Name	VPI/VCI	Encapsulation	Modify
1	<input checked="" type="checkbox"/>	Wan_PVC0	0/33	PPPoA LLC	
2	<input type="checkbox"/>	N/A	0/34	1483 Bridged Only LLC	
3	<input type="checkbox"/>	N/A	0/35	1483 Bridged Only LLC	
4	<input type="checkbox"/>	N/A	0/36	1483 Bridged Only LLC	
5	<input type="checkbox"/>	N/A	0/37	1483 Bridged Only LLC	

The following table describes the labels in this screen.

Table 17 Network > WAN > More Connections

LABEL	DESCRIPTION
#	This is an index number indicating the number of the corresponding connection.
Active	This field indicates whether the connection is active or not. Clear the check box to disable the connection. Select the check box to enable it.
Name	This is the name you gave to the Internet connection.
VPI/VCI	This field displays the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers configured for this WAN connection.
Encapsulation	This field indicates the encapsulation method of the Internet connection.
Modify	The first (ISP) connection is read-only in this screen. Use the WAN > Internet Access Setup screen to edit it. Click the Edit icon to edit the Internet connection settings. Click this icon on an empty configuration to add a new Internet access setup. Click the Remove icon to delete the Internet access setup from your connection list.

6.3.1 More Connections Edit

Use this screen to configure a connection. Click the edit icon in the **More Connections** screen to display the following screen.

Figure 32 Network > WAN > More Connections: Edit

The following table describes the labels in this screen.

Table 18 Network > WAN > More Connections: Edit

LABEL	DESCRIPTION
General	
Active	Select the check box to activate or clear the check box to deactivate this connection.
Name	Enter a unique, descriptive name of up to 13 ASCII characters for this connection.
Mode	Select Routing from the drop-down list box if your ISP allows multiple computers to share an Internet account. If you select Bridge , the ZyXEL Device will forward any packet that it does not route to this remote node; otherwise, the packets are discarded.

Table 18 Network > WAN > More Connections: Edit (continued)

LABEL	DESCRIPTION
Encapsulation	<p>Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the Mode field.</p> <p>If you select Routing in the Mode field, select PPPoA, RFC 1483, ENET ENCAP or PPPoE.</p> <p>If you select Bridge in the Mode field, method of encapsulation is not available.</p>
Multiplexing	<p>Select the method of multiplexing used by your ISP from the drop-down list. Choices are VC or LLC.</p> <p>By prior agreement, a protocol is assigned a specific virtual circuit, for example, VC1 will carry IP. If you select VC, specify separate VPI and VCI numbers for each protocol.</p> <p>For LLC-based multiplexing or PPP encapsulation, one VC carries multiple protocols with protocol identifying information being contained in each packet header. In this case, only one set of VPI and VCI numbers need be specified for all protocols.</p>
IPv6/IPv4 Dual Stack	<p>If you select Enable, the ZyXEL Device can connect to IPv4 and IPv6 networks and choose the protocol for applications according to the address type. If you select Disable, the ZyXEL Device will operate in IPv4 mode.</p>
VPI	<p>The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.</p>
VCI	<p>The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.</p>
IP Address	<p>This option is available if you select Routing in the Mode field.</p> <p>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.</p> <p>If you use the encapsulation type except RFC 1483, select Obtain an IP Address Automatically when you have a dynamic IP address; otherwise select Static IP Address and type your ISP assigned IP address in the IP Address field below.</p> <p>If you use RFC 1483, enter the IP address given by your ISP in the IP Address field.</p>
Subnet Mask	<p>Enter a subnet mask in dotted decimal notation.</p>
Default Gateway	<p>Specify a gateway IP address (supplied by your ISP).</p>
IPv6 Address	
Obtain an IP Address Automatically	<p>Select this option 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.</p>
Static IP Address	<p>Select this option if you have a fixed IPv6 address assigned by your ISP.</p>

Table 18 Network > WAN > More Connections: Edit (continued)

LABEL	DESCRIPTION
DHCP IPv6	<p>Select DHCP if you want to obtain an IPv6 address from a DHCPv6 server.</p> <p>The IP address assigned by a DHCPv6 server has priority over the IP address automatically generated by the ZyXEL Device using the IPv6 prefix from an RA.</p> <p>Select SLAAC (Stateless address autoconfiguration) to have the ZyXEL Device use the prefix to automatically generate a unique IP address that does not need to be maintained by a DHCP server.</p>
DHCP PD	<p>Select Enable to use DHCP PD (Prefix Delegation) to allow the ZyXEL Device to pass the IPv6 prefix information to its LAN hosts. The hosts can then use the prefix to generate their IPv6 addresses.</p>
Connection	
Nailed-Up Connection	<p>Select Nailed-Up Connection when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.</p>
Connect on Demand	<p>Select Connect on Demand when you don't want the connection up all the time and specify an idle time-out in the Max Idle Timeout field.</p>
Max Idle Timeout	<p>Specify an idle time-out in the Max Idle Timeout field when you select Connect on Demand. The default setting is 0, which means the Internet session will not timeout.</p>
NAT	<p>SUA only is available only when you select Routing in the Mode field.</p> <p>Select SUA Only if you have one public IP address and want to use NAT. Click Edit Detail to go to the Port Forwarding screen to edit a server mapping set.</p> <p>Otherwise, select None to disable NAT.</p>
Back	<p>Click this to return to the previous screen without saving.</p>
Apply	<p>Click this to save your changes.</p>
Advanced Setup	<p>Click this to display the More Connections Advanced Setup screen and edit more details of your WAN setup.</p>

6.3.2 Configuring More Connections Advanced Setup

Use this screen to edit your ZyXEL Device's advanced WAN settings. Click the **Advanced Setup** button in the **More Connections Edit** screen. The screen appears as shown.

Figure 33 Network > WAN > More Connections: Edit: Advanced Setup

The screenshot shows the 'Advanced Setup' configuration page. It has a title bar 'RIP & Multicast Setup' and three main sections. The first section, 'RIP & Multicast Setup', contains three dropdown menus: 'RIP Direction' set to 'Both', 'Version' set to 'RIP1', and 'Multicast' set to 'None'. The second section, 'ATM QoS', contains four input fields: 'ATM QoS Type' is a dropdown set to 'UBR With PCR'; 'Peak Cell Rate' is a text box with '0' and 'cell/sec' label; 'Sustain Cell Rate' is a text box with '0' and 'cell/sec' label; 'Maximum Burst Size' is a text box with '0' and 'cell' label. The third section, 'MTU', contains one text box for 'MTU' with the value '1500'. At the bottom, there are three buttons: 'Back', 'Apply', and 'Cancel'.

The following table describes the labels in this screen.

Table 19 Network > WAN > More Connections: Edit: Advanced Setup

LABEL	DESCRIPTION
RIP & Multicast Setup	
RIP Direction	Select the RIP Direction from None, Both, In Only and Out Only .
Version	This field is not configurable if you select None in the RIP Direction field. Select the RIP Version from RIP-1, RIP-2B and RIP-2M .
Multicast	Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports IGMP-v1 and IGMP-v2 . Select None to disable it.
ATM QoS	
ATM QoS Type	Select CBR (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select UBR (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select nrtVBR (Variable Bit Rate-non Real Time) or rtVBR (Variable Bit Rate-Real Time) for bursty traffic and bandwidth sharing with other applications.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.

Table 19 Network > WAN > More Connections: Edit: Advanced Setup (continued)

LABEL	DESCRIPTION
Sustain Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
MTU	
MTU	The Maximum Transmission Unit (MTU) defines the size of the largest packet allowed on an interface or connection. Enter the MTU in this field. For ENET ENCAP, the MTU value is 1500. For PPPoE, the MTU value is 1492. For PPPoA and RFC, the MTU is 100-1500.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

6.4 WAN Technical Reference

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

6.4.1 Encapsulation

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

6.4.1.1 ENET ENCAP

The MAC Encapsulated Routing Link Protocol (ENET ENCAP) is only implemented with the IP network protocol. IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. For instance, it encapsulates routed Ethernet frames into bridged ATM cells. ENET ENCAP requires that you specify a gateway IP address in the **Gateway IP Address** field in the wizard or WAN screen. You can get this information from your ISP.

6.4.1.2 PPP over Ethernet

The ZyXEL Device supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The PPPoE option is for a dial-up connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example RADIUS).

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the ZyXEL Device (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the ZyXEL Device does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

6.4.1.3 PPPoA

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). A PPPoA connection functions like a dial-up Internet connection. The ZyXEL Device encapsulates the PPP session based on RFC1483 and sends it through an ATM PVC (Permanent Virtual Circuit) to the Internet Service Provider's (ISP) DSLAM (Digital Subscriber Line (DSL) Access Multiplexer). Please refer to RFC 2364 for more information on PPPoA. Refer to RFC 1661 for more information on PPP.

6.4.1.4 RFC 1483

RFC 1483 describes two methods for Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5). The first method allows multiplexing of multiple protocols over a single ATM virtual circuit (LLC-based multiplexing) and the second method assumes that each protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). Please refer to RFC 1483 for more detailed information.

6.4.2 Multiplexing

There are two conventions to identify what protocols the virtual circuit (VC) is carrying. Be sure to use the multiplexing method required by your ISP.

VC-based Multiplexing

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit; for example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

LLC-based Multiplexing

In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

6.4.3 VPI and VCI

Be sure to use the correct Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers assigned to you. The valid range for the VPI is 0 to 255 and for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Please see the appendix for more information.

6.4.4 IP Address Assignment

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

IP Assignment with PPPoA or PPPoE Encapsulation

If you have a dynamic IP, then the **IP Address** and **Gateway IP Address** fields are not applicable (N/A). If you have a **Static IP Address** assigned by your ISP, then they should also assign you a **Subnet Mask** and a **Gateway IP Address**.

IP Assignment with RFC 1483 Encapsulation

In this case the IP address assignment must be static.

IP Assignment with ENET ENCAP Encapsulation

In this case you can have either a static or dynamic IP. For a static IP you must fill in all the **IP Address** and **Gateway IP Address** fields as supplied by your ISP. However for a dynamic IP, the ZyXEL Device acts as a DHCP client on the WAN

port and so the **IP Address** and **Gateway IP Address** fields are not applicable (N/A) as the DHCP server assigns them to the ZyXEL Device.

6.4.5 Nailed-Up Connection (PPP)

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The ZyXEL Device does two things when you specify a nailed-up connection. The first is that idle timeout is disabled. The second is that the ZyXEL Device will try to bring up the connection when turned on and whenever the connection is down. A nailed-up connection can be very expensive for obvious reasons.

Do not specify a nailed-up connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern.

6.4.6 NAT

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.

6.5 Traffic Shaping

Traffic Shaping is an agreement between the carrier and the subscriber to regulate the average rate and fluctuations of data transmission over an ATM network. This agreement helps eliminate congestion, which is important for transmission of real time data such as audio and video connections.

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

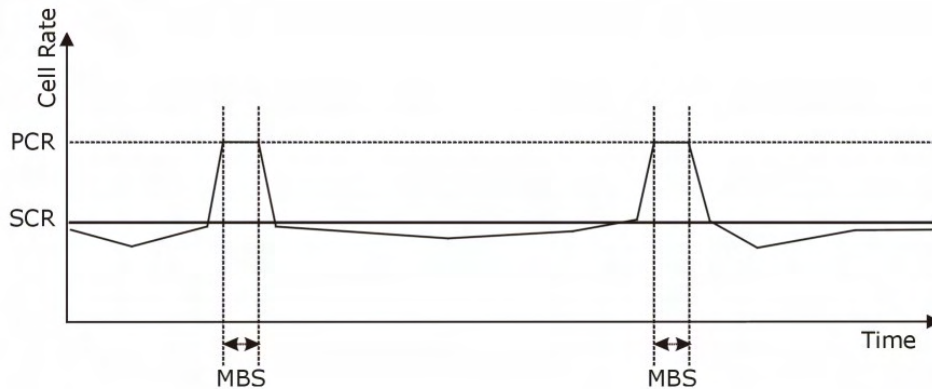
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

If the PCR, SCR or MBS is set to the default of "0", the system will assign a maximum value that correlates to your upstream line rate.

The following figure illustrates the relationship between PCR, SCR and MBS.

Figure 34 Example of Traffic Shaping



6.5.1 ATM Traffic Classes

These are the basic ATM traffic classes defined by the ATM Forum Traffic Management 4.0 Specification.

Constant Bit Rate (CBR)

Constant Bit Rate (CBR) provides fixed bandwidth that is always available even if no data is being sent. CBR traffic is generally time-sensitive (doesn't tolerate delay). CBR is used for connections that continuously require a specific amount of bandwidth. A PCR is specified and if traffic exceeds this rate, cells may be dropped. Examples of connections that need CBR would be high-resolution video and voice.

Variable Bit Rate (VBR)

The Variable Bit Rate (VBR) ATM traffic class is used with bursty connections. Connections that use the Variable Bit Rate (VBR) traffic class can be grouped into real time (VBR-RT) or non-real time (VBR-nRT) connections.

The VBR-RT (real-time Variable Bit Rate) type is used with bursty connections that require closely controlled delay and delay variation. It also provides a fixed amount of bandwidth (a PCR is specified) but is only available when data is being sent. An example of an VBR-RT connection would be video conferencing. Video conferencing requires real-time data transfers and the bandwidth requirement varies in proportion to the video image's changing dynamics.

The VBR-nRT (non real-time Variable Bit Rate) type is used with bursty connections that do not require closely controlled delay and delay variation. It is commonly used for "bursty" traffic typical on LANs. PCR and MBS define the burst levels, SCR defines the minimum level. An example of an VBR-nRT connection would be non-time sensitive data file transfers.

Unspecified Bit Rate (UBR)

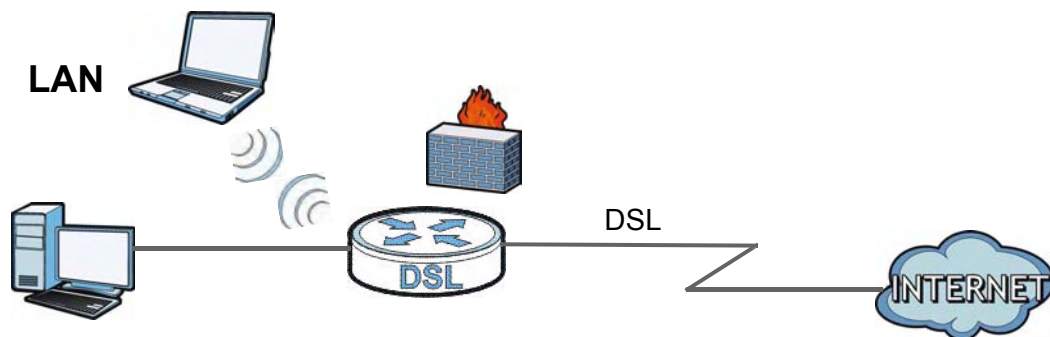
The Unspecified Bit Rate (UBR) ATM traffic class is for bursty data transfers. However, UBR doesn't guarantee any bandwidth and only delivers traffic when the network has spare bandwidth. An example application is background file transfer.

LAN Setup

7.1 Overview

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

Use the LAN screens to help you configure a LAN DHCP server and manage IP addresses.



7.1.1 What You Can Do in the LAN Screens

- Use the **LAN IP** screen ([Section 7.2 on page 91](#)) to set the LAN IP address and subnet mask of your ZyXEL device. You can also edit your ZyXEL Device's RIP, multicast and Windows Networking settings from this screen.
- Use the **DHCP Setup** screen ([Section 7.3 on page 93](#)) to configure the ZyXEL Device's DHCP settings.
- Use the **Client List** screen ([Section 7.4 on page 94](#)) to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.
- Use the **IP Alias** screen ([Section 7.5 on page 96](#)) to change your ZyXEL Device's IP alias settings.

- Use the **IPv6** screen ([Section 7.6 on page 97](#)) to configure the IPv6 settings on your ZyXEL device's LAN interface.

7.1.2 What You Need To Know About LAN

IP Address

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

Subnet Mask

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

DHCP

A DHCP (Dynamic Host Configuration Protocol) server can assign your ZyXEL Device an IP address, subnet mask, DNS and other routing information when it's turned on.

RIP

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers.

Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. There are three versions of IGMP. IGMP version 2 and 3 are improvements over version 1, but IGMP version 1 is still in wide use.

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 networking device before you can access it.

Finding Out More

See [Section 7.7 on page 98](#) for technical background information on LANs.

7.1.3 Before You Begin

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

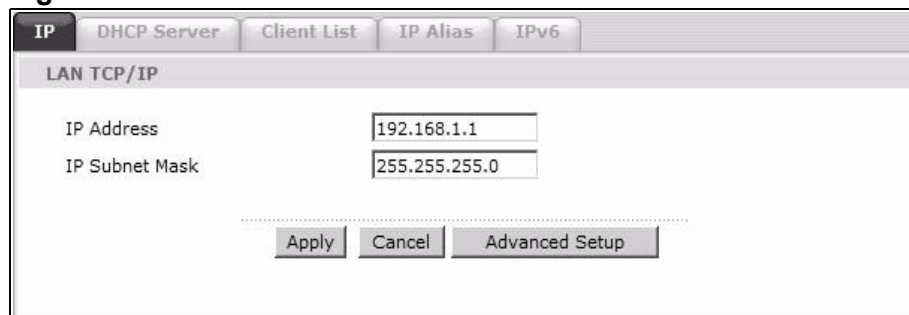
7.2 The LAN IP Screen

Use this screen to set the Local Area Network IP address and subnet mask of your ZyXEL Device. Click **Network > LAN** to open the **IP** screen.

Follow these steps to configure your LAN settings.

- 1 Enter an IP address into the **IP Address** field. The IP address must be in dotted decimal notation. This will become the IP address of your ZyXEL Device.
- 2 Enter the IP subnet mask into the **IP Subnet Mask** field. Unless instructed otherwise it is best to leave this alone, the configurator will automatically compute a subnet mask based upon the IP address you entered.
- 3 Click **Apply** to save your settings.

Figure 35 Network > LAN > IP



The screenshot shows a web-based configuration interface for LAN TCP/IP settings. At the top, there are five tabs: IP (selected), DHCP Server, Client List, IP Alias, and IPv6. Below the tabs, the title is "LAN TCP/IP". There are two input fields: "IP Address" with the value "192.168.1.1" and "IP Subnet Mask" with the value "255.255.255.0". At the bottom, there are three buttons: "Apply", "Cancel", and "Advanced Setup".

The following table describes the fields in this screen.

Table 20 Network > LAN > IP

LABEL	DESCRIPTION
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).
IP 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.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.
Advanced Setup	Click this to display the Advanced LAN Setup screen and edit more details of your LAN setup.

7.2.1 The Advanced LAN IP Setup Screen

Use this screen to edit your ZyXEL Device's RIP, multicast and Windows Networking settings. Click the **Advanced Setup** button in the **LAN IP** screen. The screen appears as shown.

Figure 36 Network > LAN > IP: Advanced Setup

The following table describes the labels in this screen.

Table 21 Network > LAN > IP: Advanced Setup

LABEL	DESCRIPTION
RIP & Multicast Setup	
RIP Direction	Select the RIP Direction from None , Both , In Only and Out Only .
RIP Version	This field is not configurable if you select None in the RIP Direction field. Select the RIP Version from RIP-1 , RIP-2B and RIP-2M .
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports IGMP-v1 and IGMP-v2 . Select None to disable it.
IGMP Snooping	Select Enabled to activate IGMP Snooping. This allows the ZyXEL Device to passively learn memberships in multicast groups.

Table 21 Network > LAN > IP: Advanced Setup

LABEL	DESCRIPTION
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

7.3 The DHCP Setup Screen

Use this screen to configure the DNS server information that the ZyXEL Device sends to the DHCP client devices on the LAN. Click **Network > DHCP Setup** to open this screen.

Figure 37 Network > LAN > DHCP Setup

The screenshot shows the DHCP Setup configuration page. It features a navigation bar with tabs: IP, DHCP Server (active), Client List, IP Alias, and IPv6. The main content area is divided into two sections: DHCP Setup and DNS Server. In the DHCP Setup section, there is a dropdown menu for 'DHCP' set to 'Server', an 'IP Pool Starting Address' field containing '192.168.1.33', a 'Pool Size' field with '32', and an empty 'Remote DHCP Server' field. The DNS Server section is titled 'DNS Servers Assigned by DHCP Server' and contains two fields: 'Primary DNS Server' and 'Secondary DNS Server', both containing '0.0.0.0'. At the bottom of the page, there are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 22 Network > LAN > DHCP Setup

LABEL	DESCRIPTION
DHCP Setup	
DHCP	<p>If set to Server, your ZyXEL Device can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client.</p> <p>If set to None, the DHCP server will be disabled.</p> <p>If set to Relay, the ZyXEL Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the Remote DHCP Server field in this case.</p> <p>When DHCP is used, the following items need to be set:</p>
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
Remote DHCP Server	If Relay is selected in the DHCP field above then enter the IP address of the actual remote DHCP server here.
DNS Server	
DNS Servers Assigned by DHCP Server	The ZyXEL Device passes a DNS (Domain Name System) server IP address to the DHCP clients.
Primary / Secondary DNS Server	Enter the IP address of your primary/secondary DNS server.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

7.4 The Client List Screen

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

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

Use this screen to change your ZyXEL Device's static DHCP settings. Click **Network > LAN > Client List** to open the following screen.

Figure 38 Network > LAN > Client List

The following table describes the labels in this screen.

Table 23 Network > LAN > Client List

LABEL	DESCRIPTION
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.
MAC Address	Enter the MAC address of a computer on your LAN.
Add	Click this to add a static DHCP entry.
#	This is the index number of the static IP table entry (row).
Status	This field displays whether the client is connected to the ZyXEL Device.
Host Name	This field displays the computer host name.
IP Address	This field displays the IP address relative to the # field listed above.
MAC Address	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.
Remove	Select the check box and then click Apply to remove the client from the list.
Modify	Click the modify icon to have the IP address field editable and change it.
Apply	Click this to save your changes.

7.5 The IP Alias Screen

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The ZyXEL Device supports two logical LAN interface via its physical Ethernet interface with the ZyXEL Device itself as the gateway for the LAN network.

When you use IP alias, you can also configure firewall rules to control access to the LAN's logical network (subnet).

7.5.1 Configuring the LAN IP Alias Screen

Use this screen to change your ZyXEL Device's IP alias settings. Click **Network > LAN > IP Alias** to open the following screen.

Figure 39 Network > LAN > IP Alias

The following table describes the labels in this screen.

Table 24 Network > LAN > IP Alias

LABEL	DESCRIPTION
IP Alias	Select the check box to configure a LAN network for the ZyXEL Device.
IP Address	Enter the IP address of your ZyXEL Device in dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address.
IP Subnet Mask	Your ZyXEL Device will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyXEL Device.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

7.6 The IPv6 Screen

Use this screen to configure the IPv6 settings for your P-660HN-Tx's LAN interface. See [Appendix E on page 295](#) for background information about IPv6.

Figure 40 Network > LAN > IPv6

The following table describes the labels in this screen.

Table 25 Network > LAN > IPv6

LABEL	DESCRIPTION
IPv6	
IPv6 Address	Enter the LAN IPv6 address you want to assign to your ZyXEL Device in hexadecimal notation, for example, fe80::1 (factory default).
Prefix	Enter the address prefix to specify how many most significant bits in an IPv6 address compose the network address.
MLD Snooping	Multicast Listener Discovery (MLD) allows an IPv6 switch or router to discover the presence of MLD hosts who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network. Select Enabled to activate MLD Snooping on the ZyXEL Device. This allows the ZyXEL device to check MLD packets passing through it and learn the multicast group membership. It helps reduce multicast traffic.
LAN IPv6 Address Setting	
Delegate Prefix from WAN	Select this option to automatically obtain an IPv6 network prefix from the service provider or an uplink router.
Static	Select this option to configure a fixed IPv6 network prefix for the ZyXEL device's LAN interface.
Static IPv6 Address	If you select static IPv6 address, enter the IPv6 prefix that the ZyXEL Device uses to generate its LAN IPv6 address.

LABEL	DESCRIPTION
Prefix length	An IPv6 prefix length specifies how many most significant bits (starting from the left) in the address compose the network address. This field displays the bit number of the IPv6 subnet mask.
Preferred Lifetime	Enter the preferred lifetime for the prefix.
Valid Lifetime	Enter the valid lifetime for the prefix.
DHCPv6 Configuration	
IPv6 DNS	Configure the IPv6 DNS information the ZyXEL device passes to clients when it acts as a DHCPv6 server. Select Auto if your ISP dynamically assigns DNS server information. Select Manual to configure DNS server addresses manually.
IPv6 DNS Server1	Enter the first DNS server IP address the ZyXEL Device passes to the DHCP clients.
IPv6 DNS Server2	Enter the second DNS server IP address the ZyXEL Device passes to the DHCP clients.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

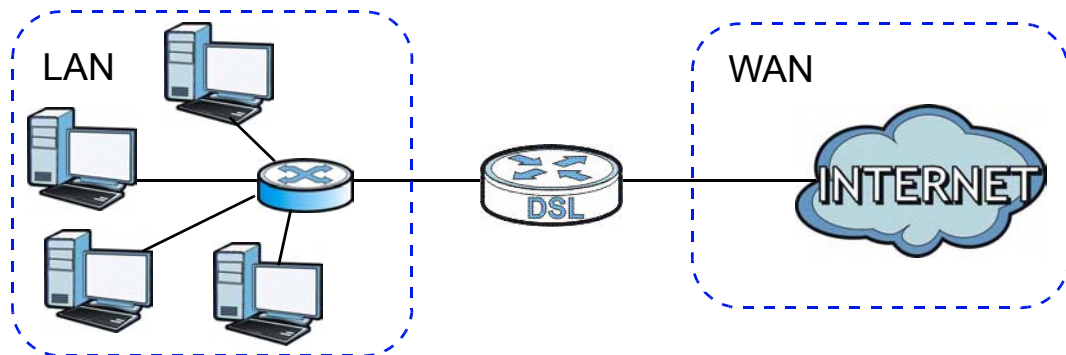
7.7 LAN Technical Reference

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

7.7.1 LANs, WANs and the ZyXEL Device

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

Figure 41 LAN and WAN IP Addresses



7.7.2 DHCP Setup

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

IP Pool Setup

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

7.7.3 DNS Server Addresses

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.

There are two ways that an ISP disseminates the DNS server addresses.

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields in the **DHCP Setup** screen.
- Some ISPs choose to disseminate the DNS server addresses using the DNS server extensions of IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The ZyXEL Device supports the IPCP DNS server extensions through the DNS proxy feature.

Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the **DHCP Setup** screen.

7.7.4 LAN TCP/IP

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

IP Address and Subnet Mask

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.

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

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the ZyXEL Device. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

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

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

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".

7.7.5 RIP Setup

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. When set to:

- **Both** - the ZyXEL Device will broadcast its routing table periodically and incorporate the RIP information that it receives.
- **In Only** - the ZyXEL Device will not send any RIP packets but will accept all RIP packets received.
- **Out Only** - the ZyXEL Device will send out RIP packets but will not accept any RIP packets received.
- **None** - the ZyXEL Device will not send any RIP packets and will ignore any RIP packets received.

The **Version** field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). RIP-1 is universally supported; but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

Both RIP-2B and RIP-2M sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.

7.7.6 Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP

version 1 is still in wide use. IGMP version 3 supports source filtering, reporting or ignoring traffic from specific source address to a particular host on the network. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

At start up, the ZyXEL Device queries all directly connected networks to gather group membership. After that, the ZyXEL Device periodically updates this information. IP multicasting can be enabled/disabled on the ZyXEL Device LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

Wireless LAN

8.1 Overview

This chapter describes how to perform tasks related to setting up and optimizing your wireless network, including the following.

- Turning the wireless connection on or off.
- Configuring a name, wireless channel and security for the network.
- Using WiFi Protected Setup (WPS) to configure your wireless network.
- Setting up multiple wireless networks.
- Using a MAC (Media Access Control) address filter to restrict access to the wireless network.
- Performing other performance-related wireless tasks.

8.1.1 What You Can Do in the Wireless LAN Screens

This section describes the ZyXEL Device's **Network > Wireless LAN** screens. Use these screens to set up your ZyXEL Device's wireless connection.

- Use the **AP** screen (see [Section 8.2 on page 105](#)) to turn the wireless connection on or off, set up wireless security, configure the MAC filter, and make other basic configuration changes.
- Use the **More AP** screen (see [Section 8.3 on page 111](#)) to set up multiple wireless networks on your ZyXEL Device.
- Use the **WPS** screen (see [Section 8.4 on page 113](#)) to enable or disable WPS, generate a security PIN (Personal Identification Number) and see information about the ZyXEL Device's WPS status.
- Use the **WPS Station** (see [Section 8.5 on page 114](#)) screen to set up WPS by pressing a button or using a PIN.

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

8.1.2 What You Need to Know About Wireless

Wireless Basics

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

SSID

Each network must have a name, referred to as the SSID - “Service Set Identifier”. The “service set” is the network, so the “service set identifier” is the network’s name. This helps you identify your wireless network when wireless networks’ coverage areas overlap and you have a variety of networks to choose from.

MAC Address Filter

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address consists of twelve hexadecimal characters (0-9, and A to F), and it is usually written in the following format: “0A:A0:00:BB:CC:DD”.

The MAC address filter controls access to the wireless network. You can use the MAC address of each wireless client to allow or deny access to the wireless network.

Finding Out More

See [Section 8.6 on page 115](#) for advanced technical information on wireless networks.

8.1.3 Before You Start

Before you start using these screens, ask yourself the following questions. See [Section 8.1.2 on page 104](#) if some of the terms used here are not familiar to you.

- What wireless standards do the other wireless devices in your network support (IEEE 802.11g, for example)? What is the most appropriate standard to use?

- What security options do the other wireless devices in your network support (WPA-PSK, for example)? What is the strongest security option supported by all the devices in your network?
- Do the other wireless devices in your network support WPS (Wi-Fi Protected Setup)? If so, you can set up a well-secured network very easily.

Even if some of your devices support WPS and some do not, you can use WPS to set up your network and then add the non-WPS devices manually, although this is somewhat more complicated to do.

- What advanced options do you want to configure, if any? If you want to configure advanced options such as Quality of Service, ensure that you know precisely what you want to do. If you do not want to configure advanced options, leave them as they are.

8.2 The AP Screen

Use this screen to configure the wireless settings of your ZyXEL Device. Click **Network > Wireless LAN** to open the **AP** screen.

Figure 42 Network > Wireless LAN > AP

The following table describes the labels in this screen.

Table 26 Network > Wireless LAN > AP

LABEL	DESCRIPTION
Wireless Setup	
Enable Wireless LAN	Click the check box to activate wireless LAN.

Table 26 Network > Wireless LAN > AP

LABEL	DESCRIPTION
Channel Selection	Set the operating channel manually by selecting a channel from the Channel Selection list or use Auto Channel Select to have it automatically configured.
Common Setup	
Network Name (SSID)	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. Note: If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's SSID or WEP settings, you will lose your wireless connection when you press Apply to confirm. You must then change the wireless settings of your computer to match the ZyXEL Device's new settings.
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.
Security Mode	See the following sections for more details about this field.
MAC Filter	This shows whether the wireless devices with the MAC addresses listed are allowed or denied to access the ZyXEL Device using this SSID.
Edit	Click this to go to the MAC Filter screen to configure MAC filter settings. See Section 8.2.5 on page 110 for more details.
QoS	Select this check box to activate Quality of Service (QoS).
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.
Advanced Setup	Click this to display the Wireless Advanced Setup screen and edit more details of your WLAN setup. See Section 8.2.4 on page 109 for more details.

8.2.1 No Security

In the **Network > Wireless LAN > AP** screen, select **No Security** from the **Security Mode** list to allow wireless devices to communicate with the ZyXEL Device without any data encryption or authentication.

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

Figure 43 Network > Wireless LAN > AP: No Security

The following table describes the labels in this screen.

Table 27 Network > Wireless LAN > AP: No Security

LABEL	DESCRIPTION
Security Mode	Choose No Security from the drop-down list box.

8.2.2 WEP Encryption

Use this screen to configure and enable WEP encryption. Click **Network > Wireless LAN** to display the **AP** screen. Select **Static WEP** from the **Security Mode** list.

Note: WEP is extremely insecure. Its encryption can be broken by an attacker, using widely-available software. It is strongly recommended that you use a more effective security mechanism. Use the strongest security mechanism that all the wireless devices in your network support. For example, use WPA-PSK or WPA2-PSK if all your wireless devices support it. If your wireless devices support nothing stronger than WEP, use the highest encryption level available.

Figure 44 Network > Wireless LAN > AP: Static WEP

Note:
 The different WEP key lengths configure different strength security, 40/64-bit, or 128-bit respectively. Your wireless client must match the security strength set on the router
 -Please type exactly 5, or 13 characters.
 or
 -Please type exactly 10, or 26 characters using only the numbers 0-9 and the letters A-F

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

Table 28 Network > Wireless LAN > AP: Static WEP

LABEL	DESCRIPTION
Security Mode	Choose Static WEP from the drop-down list box.
Passphrase	Enter a passphrase (up to 32 printable characters) and click Generate . The ZyXEL Device automatically generates a WEP key.
WEP Key	The WEP key is used to encrypt data. Both the ZyXEL Device and the wireless stations must use the same WEP key for data transmission. If you want to manually set the WEP key, enter any 5 or 13 characters (ASCII string) or 10 or 26 hexadecimal characters ("0-9", "A-F") for a 64-bit or 128-bit WEP key respectively.

8.2.3 WPA(2)-PSK

Use this screen to configure and enable WPA(2)-PSK authentication. Click **Network > Wireless LAN** to display the **AP** screen. Select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 45 Network > Wireless LAN > AP: WPA(2)-PSK

The screenshot shows the configuration interface for WPA(2)-PSK. The 'Common Setup' section includes the following fields:

- Name(SSID): ZyXEL_0000
- Hide SSID:
- Security Mode: WPA-PSK (selected from a dropdown menu)
- Pre-Shared Key: 12345678
- WPA Group Key Update Timer: 3600 (seconds)

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

Table 29 Network > Wireless LAN > AP: WPA(2)-PSK

LABEL	DESCRIPTION
Security Mode	Choose WPA-PSK or WPA2-PSK from the drop-down list box.
WPA Compatible	This check box is available only when you select WPA2-PSK in the Security Mode field. Select the check box to have both WPA-PSK wireless clients be able to communicate with the ZyXEL Device even when the ZyXEL Device is using WPA2-PSK.

Table 29 Network > Wireless LAN > AP: WPA(2)-PSK

LABEL	DESCRIPTION
Pre-Shared Key	The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
WPA Group Key Update Timer	The Group Key Update Timer is the rate at which the AP (if using WPA(2)-PSK key management) sends a new group key out to all clients. The re-keying process is the WPA(2) equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis.

8.2.4 Wireless LAN Advanced Setup

Use this screen to configure advanced wireless settings. Click the **Advanced Setup** button in the **AP** screen. The screen appears as shown.

See [Section 8.6.2 on page 117](#) for detailed definitions of the terms listed in this screen.

Figure 46 Network > Wireless LAN > AP: Advanced Setup

The following table describes the labels in this screen.

Table 30 Network > Wireless LAN > AP: Advanced Setup

LABEL	DESCRIPTION
RTS/CTS Threshold	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: 100% , 75% , 50% or 25% .

Table 30 Network > Wireless LAN > AP: Advanced Setup

LABEL	DESCRIPTION
Preamble	Select a preamble type from the drop-down list menu. Choices are Long or Short . See the Appendix D on page 283 for more information.
802.11 Mode	<p>Select 802.11b Only to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyXEL Device.</p> <p>Select 802.11g Only to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device.</p> <p>Select 802.11b+g 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.</p> <p>Select 802.11n to allow only IEEE 802.11n compliant WLAN devices to associate with the ZyXEL Device.</p> <p>Select 802.11g+n to allow either IEEE 802.11g or IEEE 802.11n compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced.</p> <p>Select 802.11b+g+n to allow IEEE 802.11b, IEEE 802.11g or IEEE802.11n compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced.</p>
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

8.2.5 MAC Filter

Use this screen to change your ZyXEL Device's MAC filter settings. Click the **Edit** button in the **AP** screen. The screen appears as shown.

Figure 47 Network > Wireless LAN > AP: MAC Address Filter

Mac Filter

Enable MAC Filter

Association Allow Deny

Set	Mac Address	Set	MAC Address
1	<input type="text"/>	2	<input type="text"/>
3	<input type="text"/>	4	<input type="text"/>
5	<input type="text"/>	6	<input type="text"/>
7	<input type="text"/>	8	<input type="text"/>
9	<input type="text"/>	10	<input type="text"/>
11	<input type="text"/>	12	<input type="text"/>
13	<input type="text"/>	14	<input type="text"/>
15	<input type="text"/>	16	<input type="text"/>

Back Apply Reset

The following table describes the labels in this screen.

Table 31 Network > Wireless LAN > AP: MAC Address Filter

LABEL	DESCRIPTION
Enable MAC Filter	Select the check box to enable MAC address filtering.
Filter Action	Define the filter action for the list of MAC addresses in the MAC Address table. 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.
Set	This is the index number of the MAC address.
MAC Address	Enter the MAC addresses of the wireless 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.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

8.3 The More AP Screen

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

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

Figure 48 Network > Wireless LAN > More AP

#	Status	SSID	Security	Modify
1	InActive	N/A	N/A	
2	InActive	N/A	N/A	
3	InActive	N/A	N/A	

The following table describes the labels in this screen.

Table 32 Network > Wireless LAN > More AP

LABEL	DESCRIPTION
#	This is the index number of each SSID profile.
Active	This field indicates whether this SSID is active.

Table 32 Network > Wireless LAN > More AP

LABEL	DESCRIPTION
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. This field displays the name of the wireless profile on the network. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
Security	This field indicates the security mode of the SSID profile.
Modify	Click the Edit icon to configure the SSID profile. Click the Remove icon to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.

8.3.1 More AP Edit

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

Figure 49 Network > Wireless LAN > More AP: Edit

The screenshot shows the 'Common Setup' configuration page for an SSID profile. The page has a light gray header with the title 'Common Setup'. Below the header, there are several configuration options:

- Active
- Name(SSID) [Text Input Field]
- Hide SSID
- Security Mode [No Security ▼]
- MAC Filter [Text Input Field]
- QoS Enable QoS

At the bottom of the page, there are three buttons: Back, Apply, and Cancel. The 'Allow Association' button is highlighted with a gray background and contains an 'Edit' icon.

The following table describes the fields in this screen.

Table 33 Network > Wireless LAN > More AP: Edit

LABEL	DESCRIPTION
Active	Select this check box to make this SSID active.
Network Name (SSID)	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. Note: If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's SSID or security settings, you will lose your wireless connection when you press Apply to confirm. You must then change the wireless settings of your computer to match the ZyXEL Device's new settings.
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.
Security Mode	See Section 8.2 on page 105 for more details about this field.
MAC Filter	This shows whether the wireless devices with the MAC addresses listed are allowed or denied to access the ZyXEL Device using this SSID.
Edit	Click this to go to the MAC Filter screen to configure MAC filter settings. See Section 8.2.5 on page 110 for more details.
QoS	Select this check box to activate Quality of Service (QoS).
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

8.4 The WPS Screen

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

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Set up each WPS connection between two devices. Both devices must support WPS.

Click **Network > Wireless LAN > WPS**. The following screen displays.

Figure 50 Network > Wireless LAN > WPS

The following table describes the labels in this screen.

Table 34 Network > Wireless LAN > WPS

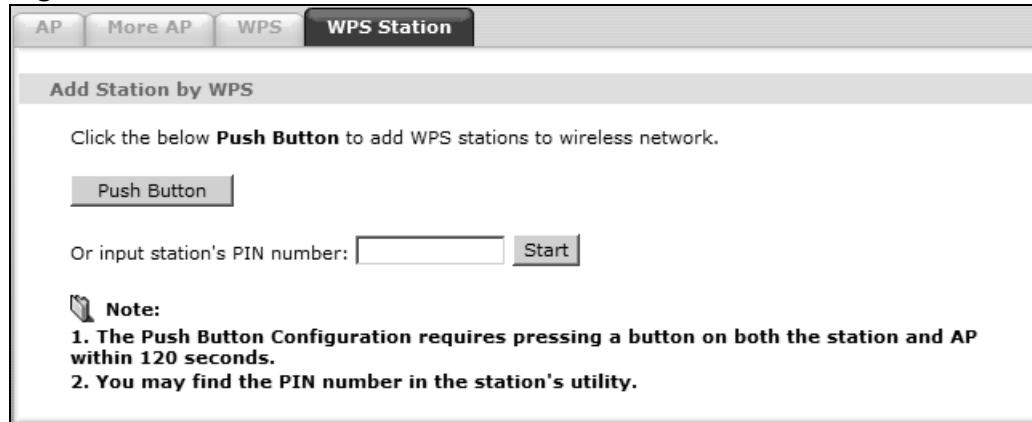
LABEL	DESCRIPTION
WPS Setup	
WPS Setup	Select the check box to activate WPS on the ZyXEL Device.
WPS Status	This displays Configured when the ZyXEL Device has connected to a wireless network using WPS or Enable WPS is selected and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the screen. This displays Unconfigured if WPS is disabled and there is no wireless or wireless security changes on the ZyXEL Device or you click Release to remove the configured wireless and wireless security settings.
Release	This button is available when the WPS status is Configured . Click this button to remove all configured wireless and wireless security settings for WPS connections on the ZyXEL Device.
Apply	Click this to save your changes.
Refresh	Click this to restore your previously saved settings.

8.5 The WPS Station Screen

Use this screen to set up a WPS wireless network using either Push Button Configuration (PBC) or PIN Configuration.

Click **Network > Wireless LAN > WPS Station**. The following screen displays.

Figure 51 Network > Wireless LAN > WPS Station



The following table describes the labels in this screen.

Table 35 Network > Wireless LAN > WPS Station

LABEL	DESCRIPTION
Push Button	<p>Click this to add another WPS-enabled wireless device (within wireless range of the ZyXEL Device) to your wireless network. This button may either be a physical button on the outside of device, or a menu button similar to the Push Button on this screen.</p> <p>Note: You must press the other wireless device's WPS button within two minutes of pressing this button.</p>
Or input station's PIN number	<p>Enter the PIN of the device that you are setting up a WPS connection with and click Start to authenticate and add the wireless device to your wireless network.</p> <p>You can find the PIN either on the outside of the device, or by checking the device's settings.</p> <p>Note: You must also activate WPS on that device within two minutes to have it present its PIN to the ZyXEL Device.</p>

8.6 Wireless LAN Technical Reference

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

8.6.1 Wireless Network Overview

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

- A wireless client is a radio connected to a user's computer.

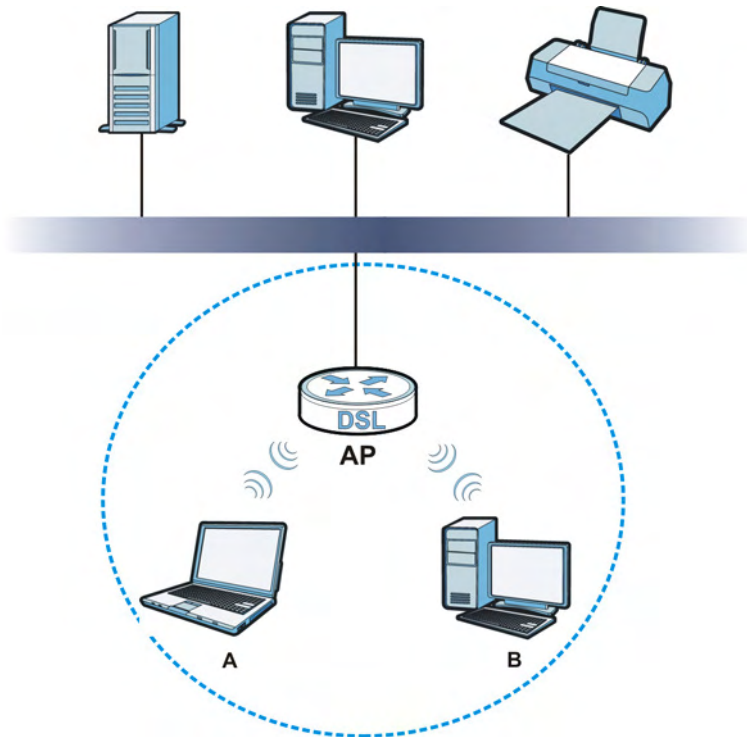
- An access point is a radio with a wired connection to a network, which can connect with numerous wireless clients and let them access the network.
- A bridge is a radio that relays communications between access points and wireless clients, extending a network's range.

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

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

The following figure provides an example of a wireless network.

Figure 52 Example of a Wireless Network



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

Every wireless network must follow these basic guidelines.

- Every device in the same wireless network must use the same SSID.
The SSID is the name of the wireless network. It stands for Service Set Identifier.

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

Radio Channels

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

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

8.6.2 Additional Wireless Terms

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

Table 36 Additional Wireless Terms

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

8.6.3 Wireless Security Overview

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

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

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

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

A good way to come up with effective security keys, passwords and so on is to use obscure information that you personally will easily remember, and to enter it in a way that appears random and does not include real words. For example, if your mother owns a 1970 Dodge Challenger and her favorite movie is Vanishing Point (which you know was made in 1971) you could use "70dodchal71vanpoi" as your security key.

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

8.6.3.1 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 wireless devices to get the SSID. In addition, unauthorized wireless devices can still see the information that is sent in the wireless network.

8.6.3.2 MAC Address Filter

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

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

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

8.6.3.3 User Authentication

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

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

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

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

8.6.3.4 Encryption

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

The types of encryption you can choose depend on the type of authentication. (See [Section 8.6.3.3 on page 119](#) for information about this.)

Table 37 Types of Encryption for Each Type of Authentication

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

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

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

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

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

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

8.6.4 Signal Problems

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

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

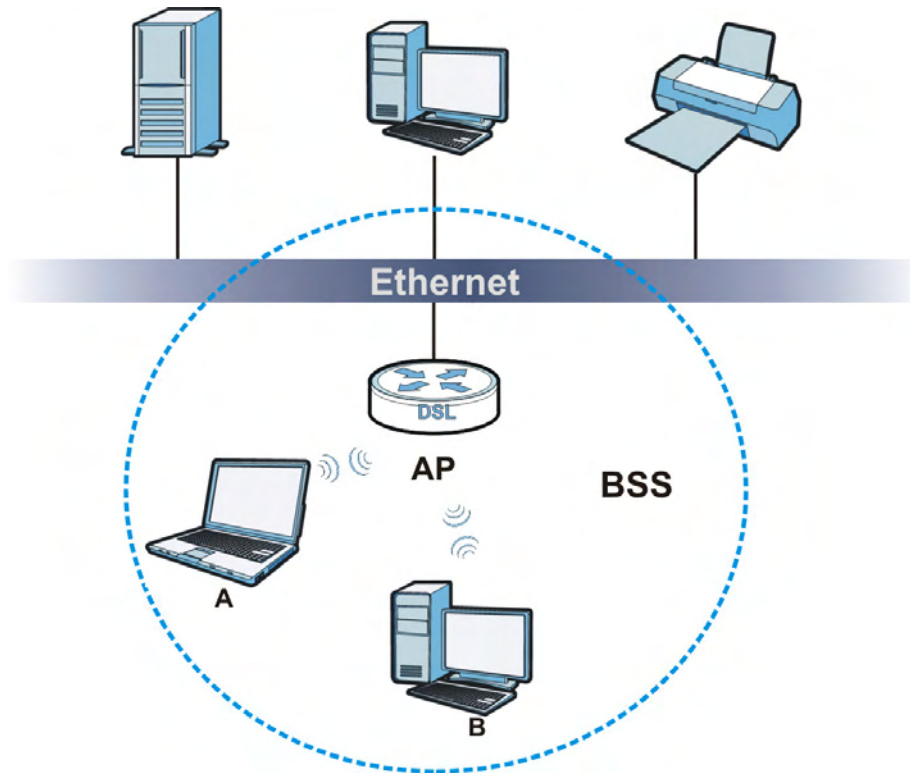
8.6.5 BSS

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

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS traffic blocking is disabled, wireless station A and B can access the wired network and communicate with each other. When Intra-BSS traffic blocking is enabled,

wireless station A and B can still access the wired network but cannot communicate with each other.

Figure 53 Basic Service set



8.6.6 MBSSID

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

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

8.6.6.1 Notes on Multiple BSSs

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

8.6.7 WiFi Protected Setup (WPS)

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

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

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

8.6.7.1 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 8.5 on page 114](#)).
- 3 Press the button on one of the devices (it doesn't matter which). For the ZyXEL Device you must press the WPS button for more than three seconds.
- 4 Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through an secure connection to the enrollee.

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

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

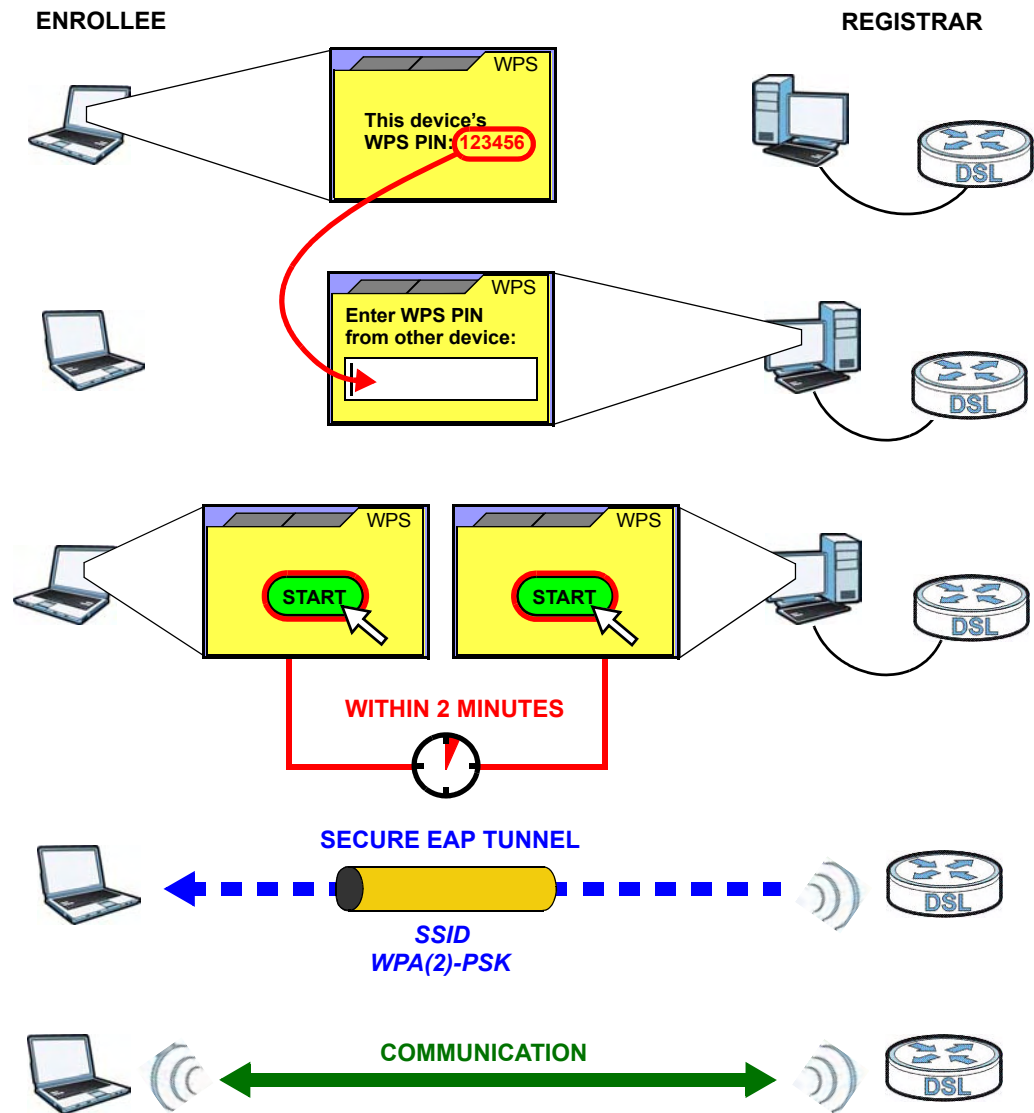
Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

- 1 Ensure WPS is enabled on both devices.
- 2 Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this.
- 3 Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide for how to find the WPS PIN - for the ZyxEL Device, see [Section 8.4 on page 113](#)).
- 4 Enter the client's PIN in the AP's configuration interface.
- 5 If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client - it does not matter which.
- 6 Start WPS on both devices within two minutes.
- 7 Use the configuration utility to activate WPS, not the push-button on the device itself.
- 8 On a computer connected to the wireless client, try to connect to the Internet. If you can connect, WPS was successful.

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

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

Figure 54 Example WPS Process: PIN Method

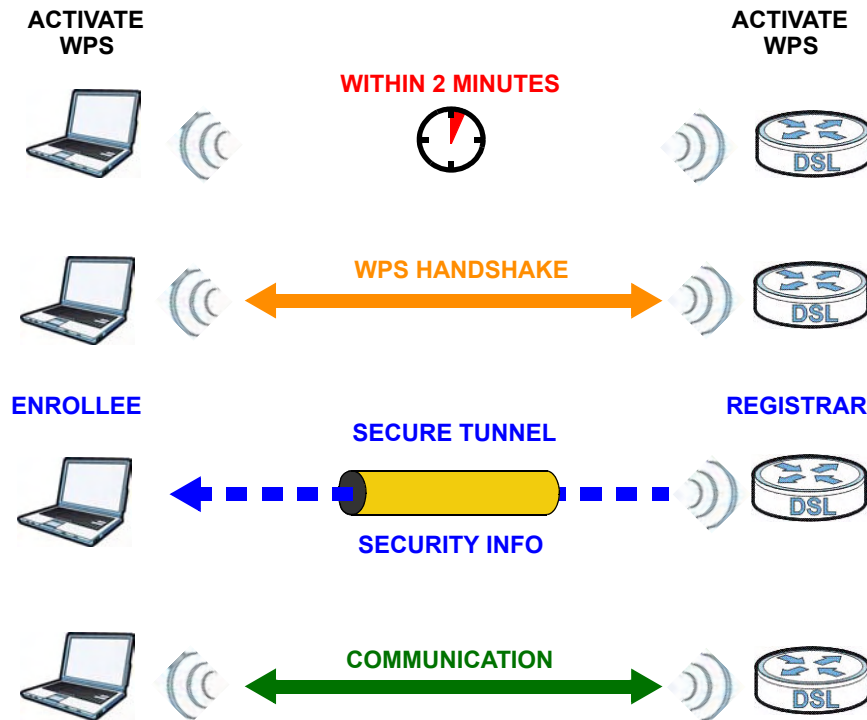


8.6.7.3 How WPS Works

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

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

Figure 55 How WPS works



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

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

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

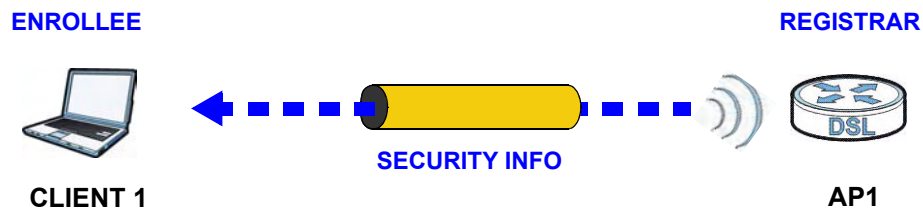
By default, a WPS device is "unconfigured". This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled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

8.6.7.4 Example WPS Network Setup

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

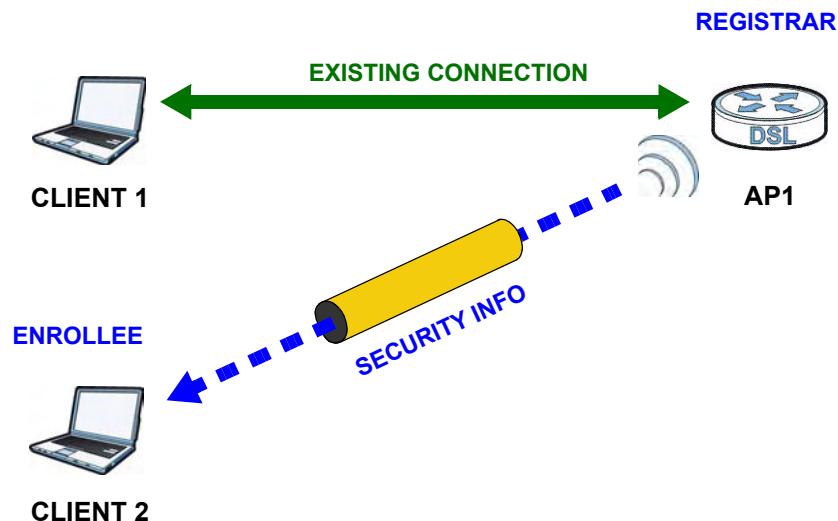
The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information.

Figure 56 WPS: Example Network Step 1



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

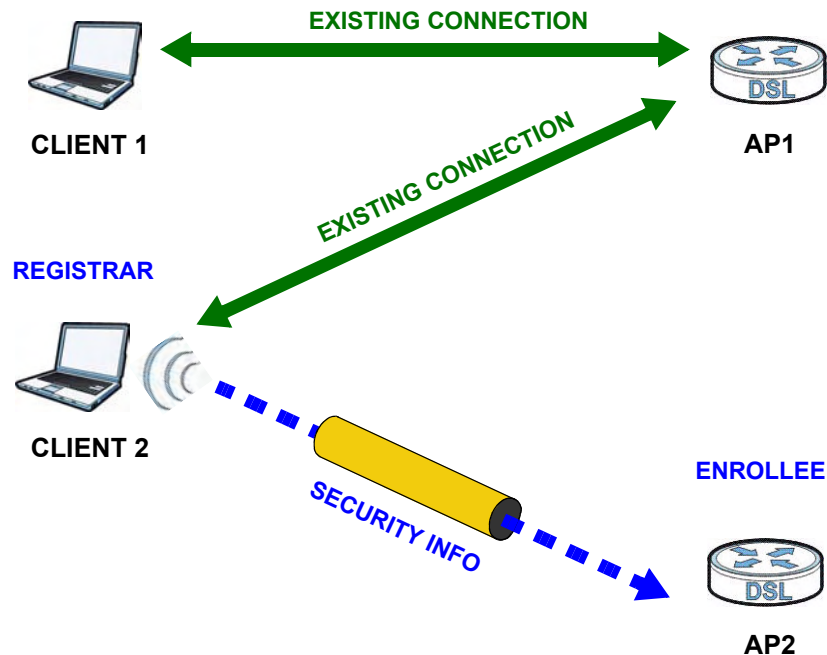
Figure 57 WPS: Example Network Step 2



In step **3**, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access

point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

Figure 58 WPS: Example Network Step 3



8.6.7.5 Limitations of WPS

WPS has some limitations of which you should be aware.

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

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

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

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

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

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

Network Address Translation (NAT)

9.1 Overview

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

9.1.1 What You Can Do in the NAT Screens

- Use the **NAT General Setup** screen ([Section 9.2 on page 132](#)) to configure the NAT setup settings.
- Use the **Port Forwarding** screen ([Section 9.3 on page 133](#)) to configure forward incoming service requests to the server(s) on your local network.
- Use the **ALG** screen ([Section 9.4 on page 137](#)) to enable and disable the SIP (VoIP) ALG in the ZyXEL Device.

9.1.2 What You Need To Know About NAT

Inside/Outside

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

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

NAT

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

Port Forwarding

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

Finding Out More

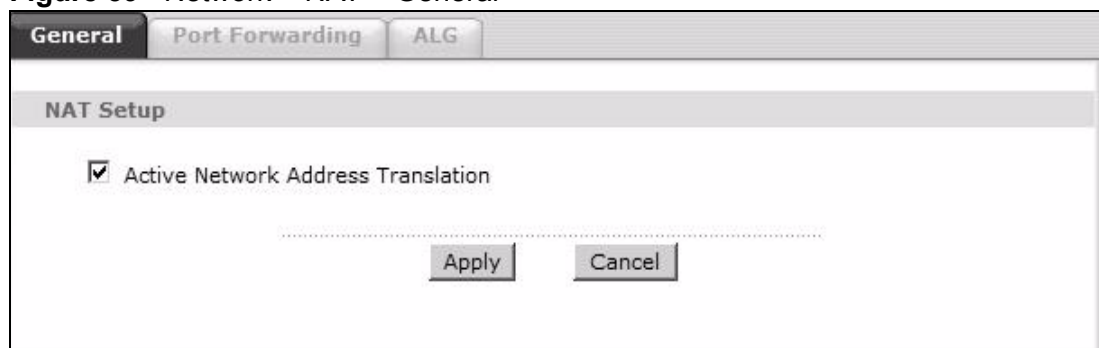
See [Section 9.5 on page 137](#) for advanced technical information on NAT.

9.2 The NAT General Setup Screen

Use this screen to activate NAT. Click **Network > NAT** to open the following screen.

Note: You must create an IP filter rule in addition to setting up NAT, to allow traffic from the WAN to be forwarded through the ZyXEL Device.

Figure 59 Network > NAT > General



The screenshot shows a web interface for NAT configuration. At the top, there are three tabs: 'General' (selected), 'Port Forwarding', and 'ALG'. Below the tabs is a section titled 'NAT Setup'. Inside this section, there is a checkbox labeled 'Active Network Address Translation' which is checked. At the bottom of the section, there are two buttons: 'Apply' and 'Cancel'.

The following table describes the labels in this screen.

Table 38 Network > NAT > General

LABEL	DESCRIPTION
Active Network Address Translation	Select this check box to enable NAT.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

9.3 The Port Forwarding Screen

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

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

The most often used port numbers and services are shown in [Appendix F on page 305](#). 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.

Default Server IP Address

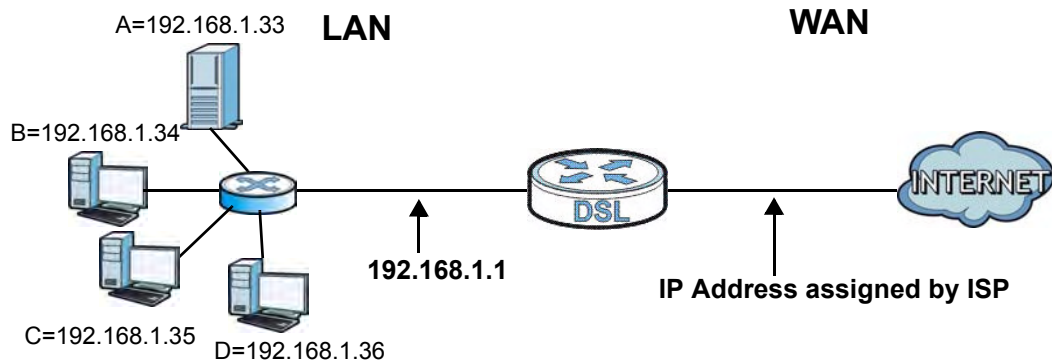
In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in this screen.

Note: If you do not assign a **Default Server** IP address, the ZyXEL Device discards all packets received for ports that are not specified here or in the remote management setup.

Configuring Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 60 Multiple Servers Behind NAT Example



9.3.1 Configuring the Port Forwarding Screen

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

See [Appendix F on page 305](#) for port numbers commonly used for particular services.

Figure 61 Network > NAT > Port Forwarding

The screenshot shows the configuration interface for Port Forwarding. It includes a 'Default Server Setup' section with a 'Default Server' field set to '0.0.0.0'. Below that is the 'Port Forwarding' section, which has a 'Service Name' dropdown menu set to 'WWW' and a 'Server IP Address' field set to '0.0.0.0'. There is an 'Add' button next to the IP address field. Below these fields is a table with the following columns: '#', 'Active', 'Service Name', 'Start Port', 'End Port', 'Server IP Address', and 'Modify'. At the bottom of the screen are three buttons: 'Back', 'Apply', and 'Cancel'.

The following table describes the fields in this screen.

Table 39 Network > NAT > Port Forwarding

LABEL	DESCRIPTION
Default Server Setup	
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a Default Server IP address, the ZyXEL Device discards all packets received for ports that are not specified here or in the remote management setup.
Port Forwarding	
Service Name	Select a service from the drop-down list box.
Server IP Address	Enter the IP address of the server for the specified service.
Add	Click this button to add a rule to the table below.
#	This is the rule index number (read-only).
Active	This field indicates whether the rule is active or not. Clear the check box to disable the rule. Select the check box to enable it.
Service Name	This is a service's name.
Start Port	This is the first port number that identifies a service.
End Port	This is the last port number that identifies a service.
Server IP Address	This is the server's IP address.
Modify	Click the edit icon to go to the screen where you can edit the port forwarding rule. Click the delete icon to delete an existing port forwarding rule. Note that subsequent address mapping rules move up by one when you take this action.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

9.3.2 The Port Forwarding Rule Edit Screen

Use this screen to edit a port forwarding rule. Click the rule's edit icon in the **Port Forwarding** screen to display the screen shown next.

Figure 62 Network > NAT > Port Forwarding: Edit

The screenshot shows a web-based configuration interface titled "Rule Setup". It contains the following elements:

- Active:** A checked checkbox.
- Service Name:** A text input field containing "WWW".
- Start Port:** A numeric input field containing "80".
- End Port:** A numeric input field containing "80".
- Server IP Address:** A text input field containing "192.168.1.2".
- Buttons:** Three buttons labeled "Back", "Apply", and "Cancel" are positioned at the bottom of the form.

The following table describes the fields in this screen.

Table 40 Network > NAT > Port Forwarding: Edit

LABEL	DESCRIPTION
Rule Setup	
Active	Click this check box to enable the rule.
Service Name	Enter a name to identify this port-forwarding rule.
Start Port	Enter a port number in this field. 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	Enter a port number in this field. To forward only one port, enter the port number again 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.
Server IP Address	Enter the inside IP address of the server here.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

9.4 The ALG Screen

Some NAT routers may include a SIP Application Layer Gateway (ALG). A SIP ALG allows SIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream. When the ZyXEL Device registers with the SIP register server, the SIP ALG translates the ZyXEL Device's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if your ZyXEL Device is behind a SIP ALG.

Use this screen to enable and disable the SIP (VoIP) ALG in the ZyXEL Device. To access this screen, click **Network > NAT > ALG**.

Figure 63 Network > NAT > ALG

The following table describes the fields in this screen.

Table 41 Network > NAT > ALG

LABEL	DESCRIPTION
Enable SIP ALG	Select this to make sure SIP (VoIP) works correctly with port-forwarding and address-mapping rules.
Apply	Click this to save your changes.
Reset	Click this to restore your previously saved settings.

9.5 NAT Technical Reference

This chapter contains more information regarding NAT.

9.5.1 NAT Definitions

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.

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

Table 42 NAT Definitions

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

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

9.5.2 What NAT Does

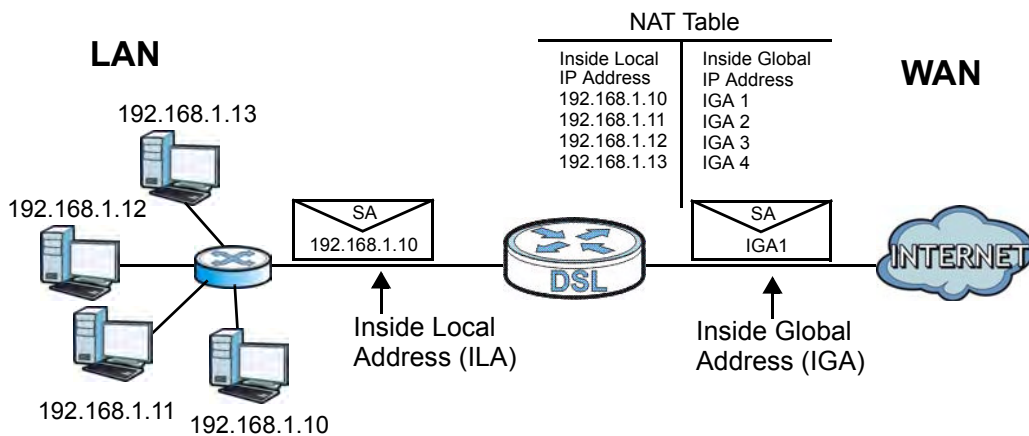
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see [Table 43 on page 141](#)), NAT offers the additional benefit of firewall protection. With no servers defined, your ZyXEL Device filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631, The IP Network Address Translator (NAT)*.

9.5.3 How NAT Works

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

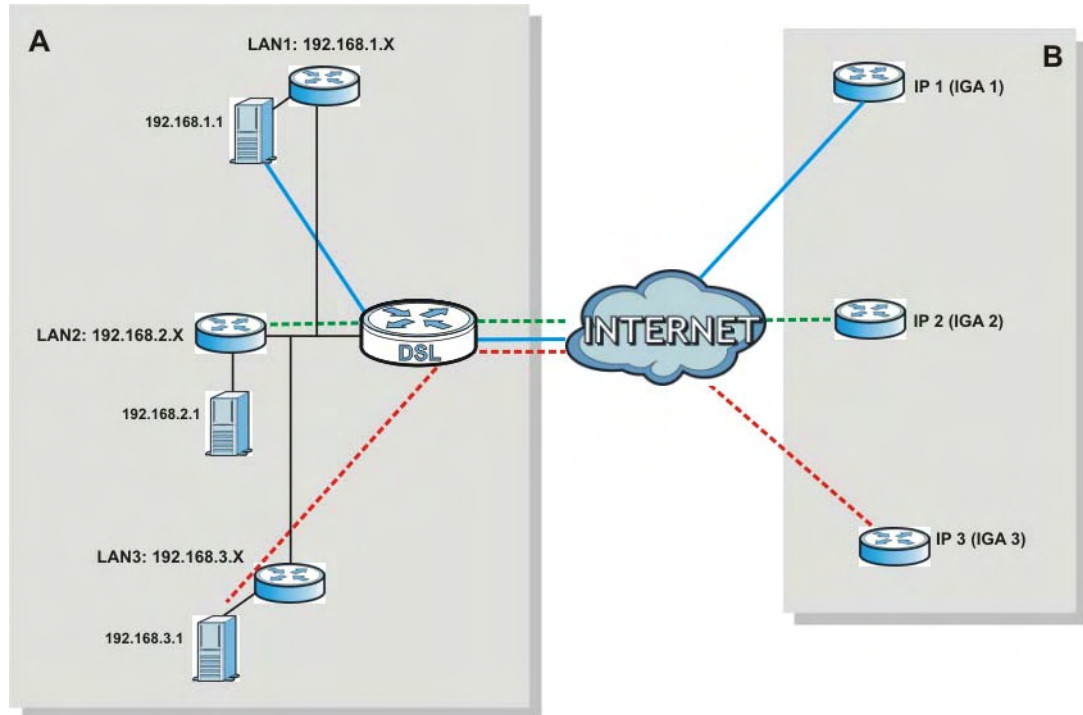
Figure 64 How NAT Works



9.5.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP alias) behind the ZyXEL Device can communicate with three distinct WAN networks.

Figure 65 NAT Application With IP Alias



9.5.5 NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

- **One to One:** In One-to-One mode, the ZyXEL Device maps one local IP address to one global IP address.
- **Many to One:** In Many-to-One mode, the ZyXEL Device maps multiple local IP addresses to one global IP address. This is equivalent to SUA (for instance, PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported (the **SUA Only** option in today's routers).
- **Many to Many Overload:** In Many-to-Many Overload mode, the ZyXEL Device maps the multiple local IP addresses to shared global IP addresses.
- **Many-to-Many No Overload:** In Many-to-Many No Overload mode, the ZyXEL Device maps each local IP address to a unique global IP address.
- **Server:** This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.

Port numbers do NOT change for **One-to-One** and **Many-to-Many No Overload** NAT mapping types.

The following table summarizes these types.

Table 43 NAT Mapping Types

TYPE	IP MAPPING
One-to-One	ILA1 \leftrightarrow IGA1
Many-to-One (SUA/PAT)	ILA1 \leftrightarrow IGA1 ILA2 \leftrightarrow IGA1 ...
Many-to-Many Overload	ILA1 \leftrightarrow IGA1 ILA2 \leftrightarrow IGA2 ILA3 \leftrightarrow IGA1 ILA4 \leftrightarrow IGA2 ...
Many-to-Many No Overload	ILA1 \leftrightarrow IGA1 ILA2 \leftrightarrow IGA2 ILA3 \leftrightarrow IGA3 ...
Server	Server 1 IP \leftrightarrow IGA1 Server 2 IP \leftrightarrow IGA1 Server 3 IP \leftrightarrow IGA1

Firewall

10.1 Overview

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

- allows traffic that originates from your LAN computers to go to all other networks.
- blocks traffic that originates on other networks from going to the LAN.
- blocks SYN and port scanner attacks.

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

10.1.1 What You Can Do in the Firewall Screens

Use the **Firewall** screen ([Section 10.2 on page 145](#)) to enable firewall and/or IPv6 firewall on the ZyXEL Device.

10.1.2 What You Need to Know About Firewall

SYN Attack

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

DoS

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a

device or network so users no longer have access to network resources. The ZyXEL Device is pre-configured to automatically detect and thwart all known DoS attacks.

DDoS

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

LAND Attack

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

Ping of Death

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

SPI

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

RFC 4890 SPEC Traffic

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

10.2 The Firewall Screen

Use this screen to enable firewall and/or SPI. Click **Security > Firewall** to display the following screen.

Figure 66 Security > Firewall

The following table describes the labels in this screen.

Table 44 Security > Firewall

LABEL	DESCRIPTION
Firewall	
Firewall	Use this field to enable or disable firewall on your ZyXEL Device.
SPI	Use this field to enable or disable SPI on your ZyXEL Device.
IPv6 Firewall	
IPv6 Firewall	Use this field to enable or disable IPv6 firewall on your ZyXEL Device.
ICMPv6 Filter Recommendations	Use this field to enable or disable ICMPv6 filter recommendations on your ZyXEL Device.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

Enabling SPI blocks all traffic initiated from the WAN side, including the DMZ, virtual server and ACL on the WAN side.

Enabling IPv6 firewall will filter SYN-Flooding and Ping of Death traffic. Enabling ICMPv6 filter recommendations will filter RFC4890 SPEC traffic.

11.1 Overview

This chapter introduces three types of filters supported by the ZyXEL Device. You can configure rules to restrict traffic by IP addresses, MAC addresses, IPv6 addresses and/or URLs.

11.1.1 What You Can Do in the Filter Screens

- Use the **URL Filter** screen ([Section 11.2 on page 148](#)) to block access to web sites.
- Use the **IP Filter** screen ([Section 11.3 on page 149](#)) to create IP filter rules.
- Use the **IPv6 Filter** screen ([Section 11.4 on page 151](#)) to create IPv6 filter rules.

11.1.2 What You Need to Know About Filtering

URL

The URL (Uniform Resource Locator) identifies and helps locates resources on a network. On the Internet the URL is the web address that you type in the address bar of your Internet browser, for example "http://www.zyxel.com".

URL and IP Filter Structure

The URL, IP and IPv6 filters have individual rule indexes. The ZyXEL Device allows you to configure each type of filter with its own respective set of rules.

11.2 The URL Filter Screen

Use this screen to block websites by URL. Click **Security > Filter > URL Filter**. The screen appears as shown.

Figure 67 Security > Filter > URL Filter

The following table describes the labels in this screen.

Table 45 Security > Filter > URL Filter

LABEL	DESCRIPTION
URL Filter Editing	
Active	Use this field to enable or disable the URL filter.
URL Index	Select the index number of the filter.
Individual active	Select Yes to make the filter active and No to make it inactive.
URL	Enter the URL for the ZyXEL Device to block.
URL Filter Listing	
Index	This is the index number of the filter rule.
Active	This indicates if the filter is active or not.
URL	This is the URL you have configured the ZyXEL Device to block.
Apply	Click this to save your changes.
Delete	Click this to remove the filter rule.
Cancel	Click this to restore your previously saved settings.

11.3 The IP Filter Screen

Use this screen to create and apply IP filters. Click **Security > Filter > IP Filter**. The screen appears as shown.

Figure 68 Security > Filter > IP Filter

The following table describes the labels in this screen.

Table 46 Security > Filter > IP Filter

LABEL	DESCRIPTION
Rule Type	
Rule Type selection	Select White List to specify traffic to allow and Black List to specify traffic to disallow.
IP Filter Rule Editing	
IP Filter Rule Index	Select the index number of the filter rule.
Active	Use this field to enable or disable the filter rule.
Interface	Select the PVC to which to apply the filter.

Table 46 Security > Filter > IP Filter (continued)

LABEL	DESCRIPTION
Direction	Apply the filter to Incoming or Outgoing traffic direction.
Rule Type	Use the IP Filter to block traffic by IP addresses.
Source IP Address	Enter the source IP address of the packets you wish to filter. This field is ignored if it is 0.0.0.0.
Subnet Mask	Enter the IP subnet mask for the source IP address
Port Number	Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.
Destination IP Address	Enter the destination IP address of the packets you wish to filter. This field is ignored if it is 0.0.0.0.
Subnet Mask	Enter the IP subnet mask for the destination IP address.
Port Number	Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.
Protocol	Select ICMP , TCP or UDP for the upper layer protocol.
IP Filter Listing	
IP Filter Rule Index	Select the index number of the filter set from the drop-down list box.
#	This is the index number of the rule in a filter set.
Active	This field shows whether the rule is activated.
Interface	This is the interface that the filter set applies to.
Direction	The filter set applies to this traffic direction.
Src Address/Mask	This is the source IP address and subnet mask when you select IP as the rule type.
Dest IP/Mask	This is the destination IP address and subnet mask.
Mac Address	This is the MAC address of the packets being filtered.
Src Port	This is the source port number.
Dest Port	This is the destination port number.
Protocol	This is the upper layer protocol.
Apply	Click this to apply your changes.
Delete	Click this to remove the filter rule.
Cancel	Click this to restore your previously saved settings.