

P-870H/HW Series

VDSL2 4 port gateway/802.11bg Wireless VDSL2 4 port gateway

User's Guide



Default Login Details

IP Address	http://192.168.1.1
User Name	admin
Password	1234

Firmware Version 1.0
Edition 1, 12/2010

www.zyxel.com

ZyXEL

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the ZyXEL Device using the Web Configurator.

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.

Documentation Feedback

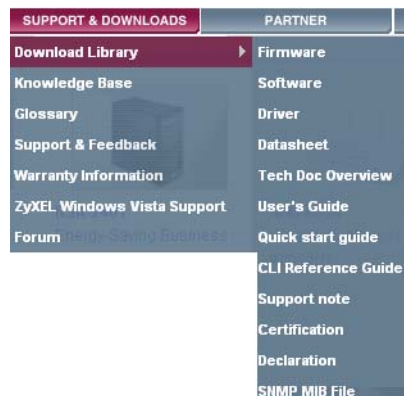
Send your comments, questions or suggestions to: techwriters@zyxel.com.tw

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

Should problems arise that cannot be solved by the methods listed above, 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.

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-870H/HW Series 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 	DSLAM 	Firewall 
Telephone 	Switch 	Router 

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).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

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
Introducing the ZyXEL Device	21
Tutorials	27
Introducing the Web Configurator	37
Status Screens	43
Technical Reference	53
WAN Setup	55
LAN Setup	77
Wireless LAN	85
Network Address Translation (NAT)	117
MAC Filter	131
Firewall	135
Certificate	141
Static Route	153
Policy Forwarding	157
RIP	161
Quality of Service (QoS)	163
Dynamic DNS Setup	177
Remote Management	179
Universal Plug-and-Play (UPnP)	185
Parental Control	199
Interface Group	203
System Settings	209
Logs	213
Tools	217
Diagnostic	225
Troubleshooting	229
Product Specifications	235

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	
Introducing the ZyXEL Device	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	22
1.5 LEDs (Lights)	24
1.6 The RESET Button	25
1.6.1 Using the Reset Button	26
1.7 The WPS WLAN Button (P-870HW Series only)	26
1.7.1 Turn the Wireless LAN Off or On	26
1.7.2 Activate WPS	26
 Chapter 2	
Tutorials.....	27
2.1 How to Set up a Wireless Network	27
2.1.1 Example Parameters	27
2.1.2 Configuring the AP	27
2.1.3 Configuring the Wireless Client	30
 Chapter 3	
Introducing the Web Configurator	37
3.1 Web Configurator Overview	37
3.1.1 Accessing the Web Configurator	37
3.2 Web Configurator Main Screen	38

3.2.1 Navigation Panel	39
3.2.2 Main Window	41
3.2.3 Status Bar	41
Chapter 4	
Status Screens	43
4.1 Status Screen	43
4.1.1 WAN Service Statistics	47
4.1.2 Route Info	48
4.1.3 WLAN Station List	49
4.1.4 LAN Statistics	50
4.1.5 Client List	51
 Part II: Technical Reference	 53
 Chapter 5	
WAN Setup.....	55
5.1 Overview	55
5.1.1 What You Can Do in this Chapter	55
5.2 What You Need to Know	56
5.3 Before You Begin	56
5.4 The Layer 2 Interface Screen	56
5.4.1 Layer 2 Interface Configuration	58
5.5 The Internet Connection Screen	59
5.5.1 WAN Connection Configuration	60
5.6 Technical Reference	71
 Chapter 6	
LAN Setup.....	77
6.1 Overview	77
6.1.1 What You Can Do in this Chapter	77
6.2 What You Need To Know	78
6.3 The LAN IP Screen	79
6.4 Technical Reference	81
 Chapter 7	
Wireless LAN.....	85
7.1 Overview	85
7.1.1 What You Can Do in this Chapter	85
7.2 What You Need to Know	86
7.3 Before You Begin	88

7.4 The General Screen	89
7.4.1 No Security	90
7.4.2 WEP Encryption	91
7.4.3 WPA(2)-PSK	93
7.4.4 WPA(2) Authentication	94
7.4.5 MAC Filter	95
7.4.6 Adding a New MAC Filtering Rule	97
7.5 The More AP Screen	97
7.5.1 More AP Edit	98
7.6 The WPS Screen	98
7.7 The WPS Station Screen	100
7.8 The WDS Screen	101
7.9 The Advanced Setup Screen	103
7.10 Technical Reference	105
7.10.1 Wireless Network Overview	105
7.10.2 Additional Wireless Terms	106
7.10.3 Wireless Security Overview	106
7.10.4 WiFi Protected Setup	109
Chapter 8	
Network Address Translation (NAT).....	117
8.1 Overview	117
8.1.1 What You Can Do in this Chapter	117
8.2 What You Need to Know	117
8.3 The Port Forwarding Screen	118
8.3.1 The Port Forwarding Edit Screen	120
8.4 The Address Mapping Screen	121
8.4.1 The Address Mapping Rule Edit Screen	123
8.5 The Trigger Port Screen	124
8.5.1 Trigger Port Configuration	126
8.6 The DMZ Host Screen	128
8.7 The ALG Screen	128
8.8 Technical Reference	129
Chapter 9	
MAC Filter	131
9.1 Overview	131
9.1.1 What You Can Do in this Chapter	131
9.2 The MAC Filter Screen	131
9.2.1 Creating MAC Filtering Rules	133
Chapter 10	
Firewall.....	135

10.1 Overview	135
10.1.1 What You Can Do in this Chapter	135
10.2 What You Need to Know	135
10.3 The Firewall Screen	136
10.3.1 Creating Incoming Firewall Rules	138
Chapter 11	
Certificate	141
11.1 Overview	141
11.1.1 What You Can Do in this Chapter	141
11.2 What You Need to Know	141
11.3 The Local Certificates Screen	142
11.3.1 Create Certificate Request	143
11.3.2 Import Certificate	144
11.3.3 Certificate Details	146
11.3.4 Load Signed Certificate	148
11.4 The Trusted CA Screen	149
11.4.1 View Trusted CA Certificate	151
11.4.2 Import Trusted CA Certificate	152
Chapter 12	
Static Route	153
12.1 Overview	153
12.1.1 What You Can Do in this Chapter	153
12.2 The Static Route Screen	154
12.2.1 Static Route Edit	155
Chapter 13	
Policy Forwarding	157
13.1 Overview	157
13.1.1 What You Can Do in this Chapter	157
13.2 The Static Route Screen	157
13.2.1 Policy Forwarding Setup	158
Chapter 14	
RIP	161
14.1 Overview	161
14.1.1 What You Can Do in this Chapter	161
14.2 The RIP Screen	161
Chapter 15	
Quality of Service (QoS)	163
15.1 Overview	163

15.1.1 What You Can Do in this Chapter	163
15.2 What You Need to Know	164
15.3 The Quality of Service General Screen	164
15.4 The Queue Setup Screen	166
15.4.1 Adding a QoS Queue	167
15.5 The Class Setup Screen	168
15.5.1 QoS Class Edit	170
15.6 The QoS Monitor Screen	174
15.7 Technical Reference	175
Chapter 16	
Dynamic DNS Setup	177
16.1 Overview	177
16.1.1 What You Can Do in this Chapter	177
16.2 What You Need To Know	177
16.3 The Dynamic DNS Screen	178
Chapter 17	
Remote Management.....	179
17.1 Overview	179
17.1.1 What You Can Do in this Chapter	179
17.2 The TR-069 Screen	179
17.3 The TR-064 Screen	181
17.4 The Service Control Screen	182
17.5 The IP Address Screen	183
17.5.1 Adding an IP Address	184
Chapter 18	
Universal Plug-and-Play (UPnP).....	185
18.1 Overview	185
18.1.1 What You Can Do in this Chapter	185
18.2 What You Need to Know	185
18.3 The UPnP Screen	186
18.4 Installing UPnP in Windows Example	187
18.5 Using UPnP in Windows XP Example	191
Chapter 19	
Parental Control	199
19.1 Overview	199
19.1.1 What You Can Do in this Chapter	199
19.2 The Time Restriction Screen	199
19.2.1 Adding a Schedule	200
19.3 The URL Filter Screen	201

19.3.1 Adding URL Filter	202
Chapter 20	
Interface Group	203
20.1 Overview	203
20.1.1 What You Can Do in this Chapter	203
20.2 The Interface Group Screen	203
20.2.1 Interface Group Configuration	204
20.2.2 Interface Grouping Criteria	206
Chapter 21	
System Settings	209
21.1 Overview	209
21.1.1 What You Can Do in this Chapter	209
21.2 The General Screen	209
21.3 The Time Setting Screen	210
Chapter 22	
Logs	213
22.1 Overview	213
22.1.1 What You Can Do in this Chapter	213
22.2 The View Log Screen	213
22.3 The Log Settings Screen	214
Chapter 23	
Tools.....	217
23.1 Overview	217
23.1.1 What You Can Do in this Chapter	217
23.2 The Firmware Screen	218
23.3 The Configuration Screen	220
23.4 The Restart Screen	222
Chapter 24	
Diagnostic.....	225
24.1 Overview	225
24.1.1 What You Can Do in this Chapter	225
24.2 What You Need to Know	225
24.3 The General Diagnostic Screen	226
24.4 The 802.1ag Screen	227
Chapter 25	
Troubleshooting.....	229
25.1 Power, Hardware Connections, and LEDs	229

25.2 ZyXEL Device Access and Login	230
25.3 Internet Access	231
Chapter 26	
Product Specifications	235
26.1 Hardware Specifications	235
26.2 Firmware Specifications	235
26.3 Wireless Features (for P-870HW Series only)	238
Appendix A Setting Up Your Computer's IP Address	241
Appendix B Pop-up Windows, JavaScript and Java Permissions	271
Appendix C IP Addresses and Subnetting	281
Appendix D Wireless LANs	293
Appendix E Common Services	309
Appendix F Open Software Announcements	313
Appendix G Legal Information	325
Index	329

PART I

User's Guide

Introducing the ZyXEL Device

This chapter introduces the main applications and features of the ZyXEL Device. It also introduces the ways you can manage the ZyXEL Device.

1.1 Overview

The ZyXEL Device is a VDSL2 gateway that allows super-fast, secure Internet access.

you can use Quality of Service (QoS) to efficiently manage traffic on your network by giving priority to certain types of traffic and/or to particular computers.

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

- “H” denotes an integrated 4-port hub (switch).
- “W” denotes wireless functionality. There is an embedded mini-PCI module for IEEE 802.11g wireless LAN connectivity.

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

- Models ending in “1”, for example P-870HW-51a v2, denote a device that works over the analog telephone system, POTS (Plain Old Telephone Service). Models ending in “3”, for example P-870H-53a v2, denote a device that works over ISDN (Integrated Services Digital Network) or T-ISDN (UR-2).

See [Chapter 26 on page 235](#) 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.

- **SNMP.** The device can be monitored by an SNMP manager. See the SNMP chapter in this User's Guide.
- **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.

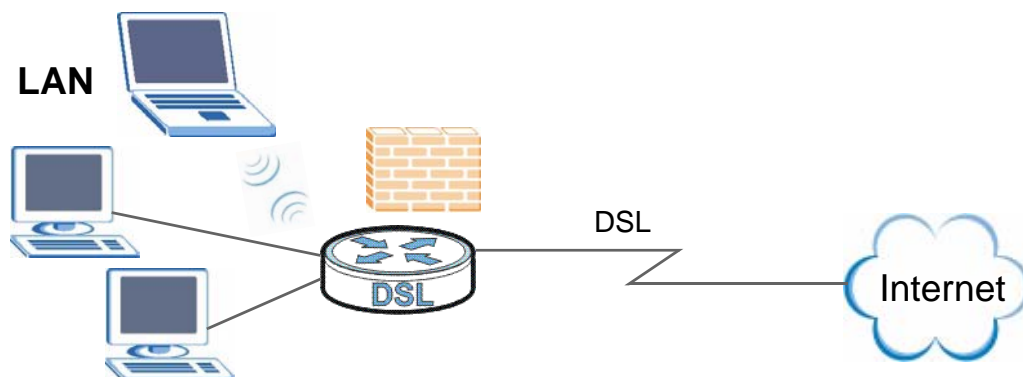
1.4 Applications for the ZyXEL Device

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 IP filtering on the ZyXEL Device for secure Internet access. When the IP filter is on, all incoming traffic from the Internet to your network is blocked by default 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.

1.5 LEDs (Lights)

The following graphic displays the labels of the LEDs. Not all LEDs are available on all models.

Figure 2 LEDs on the Top of the Device: P-870HW Series

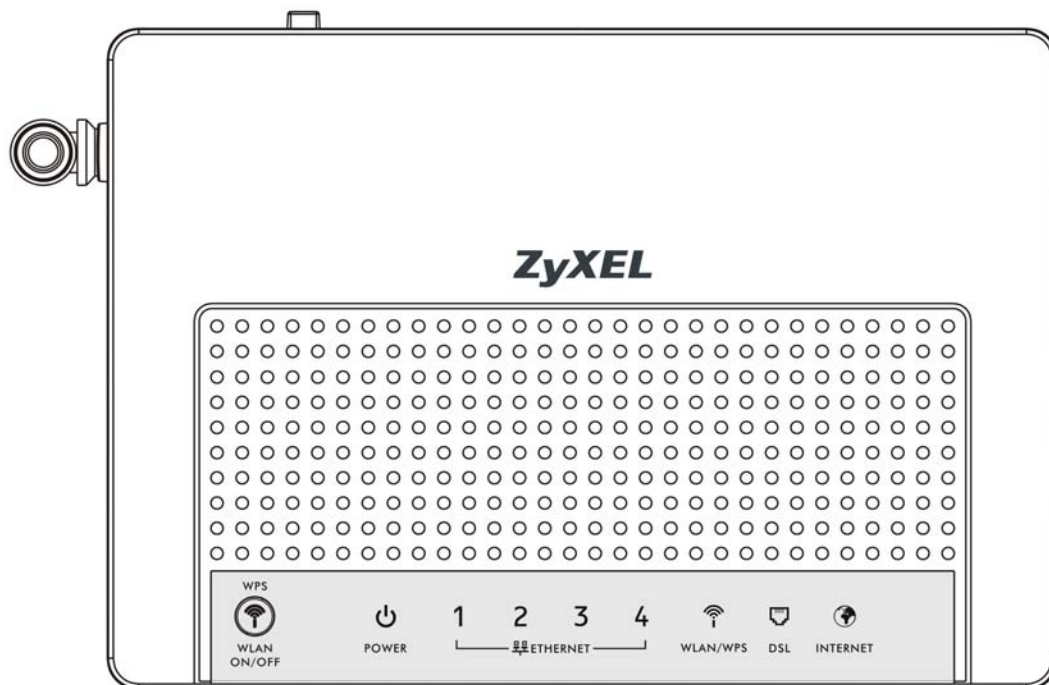
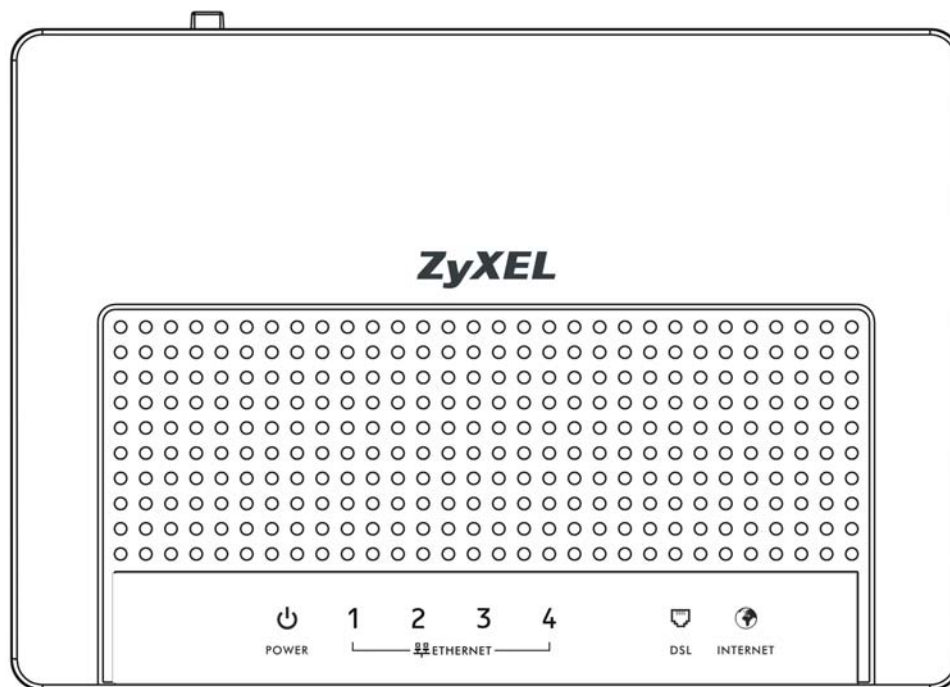


Figure 3 LEDs on the Top of the Device: P-870H Series



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 not receiving power.
ETHERNET 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 sending/receiving data to /from the LAN.
		Off	The ZyXEL Device does not have an Ethernet connection with the LAN.
WLAN/WPS	Green	On	The wireless network is activated and is operating in IEEE 802.11b/g mode.
		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.
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 DHCP server), PPP negotiation was successfully completed (if used) and the DSL connection is up.
		Red	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.
		Off	The ZyXEL Device does not have an IP connection.

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


1.6 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 password will be reset to "1234".

1.6.1 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.

1.7 The WPS WLAN Button (P-870HW Series only)

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

1.7.1 Turn the Wireless LAN Off or On

- 1 Make sure the **POWER** LED is on (not blinking).
- 2 Press the **WPS WLAN ON/OFF** button for one second and release it. The **WLAN/WPS** LED should change from on to off or vice versa.

1.7.2 Activate WPS

- 1 Make sure the **POWER** LED is on (not blinking).
- 2 Press the **WPS WLAN ON/OFF** button for more than five seconds and release it. Press the WPS button on another WPS -enabled device within range of the ZyXEL Device. The **WLAN/WPS** LED should flash while the ZyXEL Device sets up a WPS connection with the wireless device.

Note: You must activate WPS in the ZyXEL Device and in another wireless device within two minutes of each other. See [Section 7.10.4 on page 109](#) for more information.

Tutorials

This chapter describes how to set up a wireless network.

2.1 How to Set up a Wireless Network

This tutorial gives you examples of how to set up an access point and wireless client for wireless communication using the following parameters. The wireless clients can access the Internet through an AP wirelessly.

2.1.1 Example Parameters

SSID	SSID_Example3
Security	WPA-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)
802.11 mode	IEEE 802.11b/g

An access point (AP) or wireless router is referred to as "AP" and a computer with a wireless network card or USB/PCI adapter is referred to as "wireless client" here.

We use the ZyXEL Device web screens and M-302 utility screens as an example. The screens may vary slightly for different models.

2.1.2 Configuring the AP

Follow the steps below to configure the wireless settings on your AP.

- 1 Open the **Network > Wireless LAN** screen in the AP's Web Configurator.

Figure 4 AP: Wireless LAN

The screenshot displays the 'General' tab of the AP's Web Configurator. The 'Wireless Setup' section is visible, showing the 'Active Wireless LAN' checkbox checked and 'Channel Selection' set to 6. Below this, the 'Common Setup' section contains the following fields:

- Network Name(SSID): SSID_Example3
- Auto Generate Key: ☐
- Hide Network Name(SSID): ☐
- Disable WMM Advertise: ☐
- BSSID: 00:23:F8:0C:89:65
- Security Mode: WPA-PSK
- Encryption: TKIP
- Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey
- Group Key Update Timer: 1800 sec
- MAC Filter: Edit

At the bottom of the form, there are 'Apply' and 'Reset' buttons.

- 2 Make sure the **Active Wireless LAN** check box is selected.
- 3 Enter "SSID_Example3" as the SSID and select a channel which is not used by another AP.
- 4 Set security mode to **WPA-PSK** and enter "ThisismyWPA-PSKpre-sharedkey" in the **Pre-Shared Key** field. Click **Apply**.

- 5 Click the **Advanced Setup** tab and select **802.11b/g Mixed** in the **802.11 Mode** field. Click **Apply**.

Figure 5 AP: Wireless LAN > Advanced Setup

Wireless Advanced Setup

RTS/CTS Threshold: 2347

Fragmentation Threshold: 2346

Number of Wireless Stations Allowed: 16

Output Power: 100%

Multicast Rate: 18 Mbps

802.11 Mode: 802.11b/g Mixed

802.11 Protection: Auto

Preamble: Long

Apply Reset

- 6 Open the **Status** screen. Verify your wireless and wireless security settings under **Device Information** and check if the WLAN connection is up under **Interface Status**.

Figure 6 AP: Status

ZyXEL

Status

Host Name: 1234

Model Number: P-870HW-51a V2

MAC Address: 00:19:cb:d1:79:04

ZYNOS Firmware Version: 1.00(AW2.0)b4

DSL Firmware Version: AvC010a.d21i3

WAN 1 Information

- Mode: ENET ENCAP
- IP Address: 0.0.0.0
- IP Subnet Mask: 0.0.0.0

LAN Information

- IP Address: 192.168.1.1
- IP Subnet Mask: 255.255.255.0
- DHCP: Server

WLAN Information

- ESSID: SSID_Example3
- Channel: 6
- WPS Status: Unconfigured

System Uptime: 0: 0:20

Current Date/Time: 1 Jan 2000 00:20:59

System Mode: Routing / Bridging

CPU Usage: 3%

Memory Usage: 70%

Interface Status

Interface	Status	Rate
DSL	NoSignal	kbps / kbps
LAN 0	Up	100M/ Full
LAN 1	Disabled	100M/ Full
LAN 2	Disabled	100M/ Full
LAN 3	Disabled	100M/ Full
WLAN	Up	54M

More Status

[WAN Service Statistics](#)
[LAN Statistics](#)
[Route Info](#)
[Client List](#)
[WLAN Station List](#)

Message Ready

- 7 Click the **WLAN Station List** hyperlink in the AP's **Status** screen. You can see if any wireless client has connected to the AP.

Figure 7 AP: Status: WLAN Station List

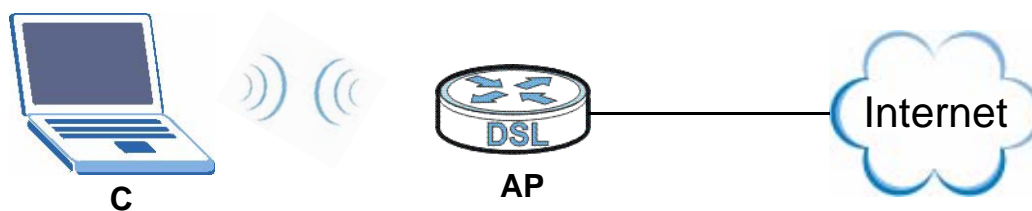
WLAN Station List				
MAC	Associated	Authorized	SSID	Interface
00:03:7F:BF:16:8C	Yes	Yes	SSID_Example3	wl0
Refresh Interval : <input type="text"/> sec <input type="button" value="Set Interval"/> <input type="button" value="Stop"/>				

2.1.3 Configuring the Wireless Client

This section describes how to connect the wireless client to a network.

2.1.3.1 Connecting to a Wireless LAN

The following sections show you how to join a wireless network using the ZyXEL utility, as in the following diagram. The wireless client is labeled **C** and the access point is labeled **AP**.



There are three ways to connect the client to an access point.

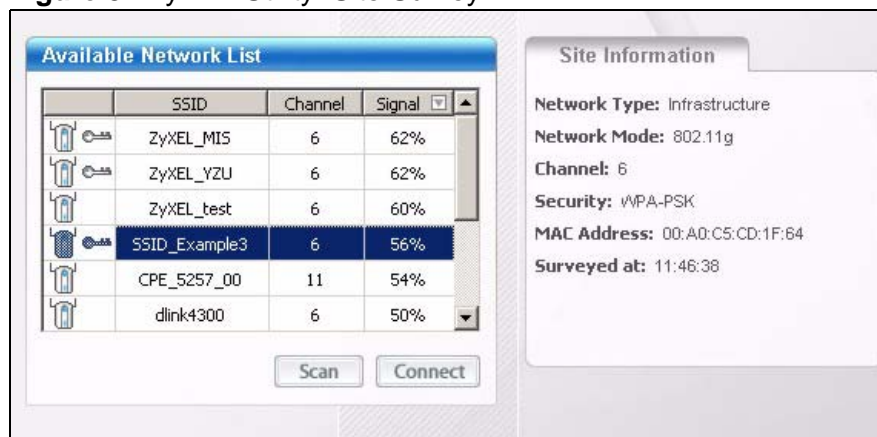
- Configure nothing and leave the wireless client to automatically scan for and connect to any available network that has no wireless security configured.
- Manually connect to a network.
- Configure a profile to have the wireless client automatically connect to a specific network or peer computer.

This example illustrates how to manually connect your wireless client to an access point (AP) which is configured for WPA-PSK security and connected to the Internet. Before you connect to the access point, you must know its Service Set IDentity (SSID) and WPA-PSK pre-shared key. In this example, the SSID is "SSID_Example3" and the pre-shared key is "ThisismyWPA-PSKpre-sharedkey".

After you install the ZyXEL utility and then insert the wireless client, follow the steps below to connect to a network using the **Site Survey** screen.

- 1 Open the ZyXEL utility and click the **Site Survey** tab to open the screen shown next.

Figure 8 ZyXEL Utility: Site Survey

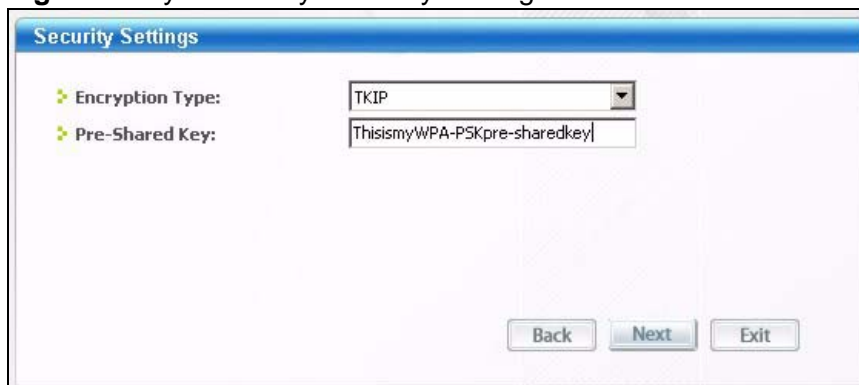


- 2 The wireless client automatically searches for available wireless networks. Click **Scan** if you want to search again. If no entry displays in the **Available Network List**, that means there is no wireless network available within range. Make sure the AP or peer computer is turned on or move the wireless client closer to the AP or peer computer.

- 3 When you try to connect to an AP with security configured, a window will pop up prompting you to specify the security settings. Enter the pre-shared key and leave the encryption type at the default setting.

Use the **Next** button to move on to the next screen. You can use the **Back** button at any time to return to the previous screen, or the **Exit** button to return to the **Site Survey** screen.

Figure 9 ZyXEL Utility: Security Settings



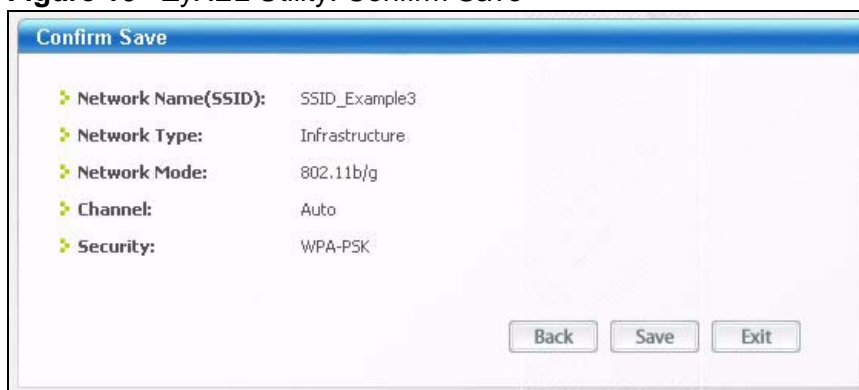
The 'Security Settings' window displays two configuration fields. The 'Encryption Type' is set to 'TKIP' via a dropdown menu. The 'Pre-Shared Key' field contains the text 'ThisismyWPA-PSKpre-sharedkey'. At the bottom right, there are three buttons: 'Back', 'Next', and 'Exit'.

Encryption Type:	TKIP
Pre-Shared Key:	ThisismyWPA-PSKpre-sharedkey

Back Next Exit

- 4 The **Confirm Save** window appears. Check your settings and click **Save** to continue.

Figure 10 ZyXEL Utility: Confirm Save



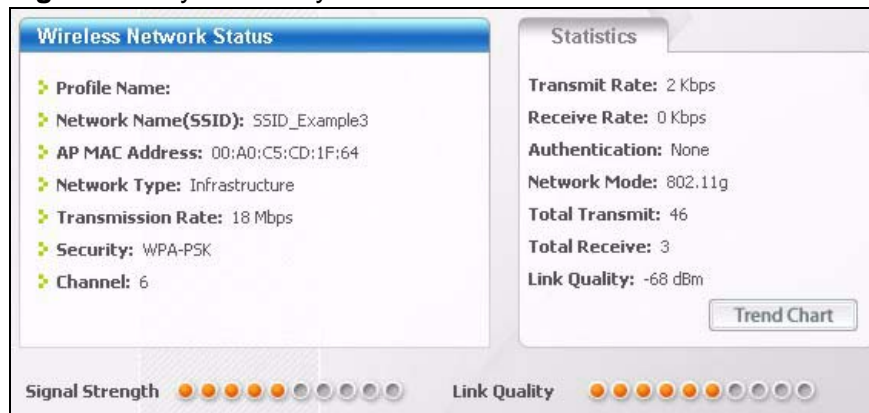
The 'Confirm Save' window displays a summary of the network configuration. The settings listed are: Network Name (SSID): SSID_Example3, Network Type: Infrastructure, Network Mode: 802.11b/g, Channel: Auto, and Security: WPA-PSK. At the bottom right, there are three buttons: 'Back', 'Save', and 'Exit'.

Network Name(SSID):	SSID_Example3
Network Type:	Infrastructure
Network Mode:	802.11b/g
Channel:	Auto
Security:	WPA-PSK

Back Save Exit

- 5 The ZyXEL utility returns to the **Link Info** screen while it connects to the wireless network using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection. Check the network information in the **Link Info** screen to verify that you have successfully connected to the selected network. If the wireless client is not connected to a network, the fields in this screen remain blank.

Figure 11 ZyXEL Utility: Link Info



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

If you cannot access the web site, try changing the encryption type in the **Security Settings** screen, check the Troubleshooting section of this User's Guide or contact your network administrator.

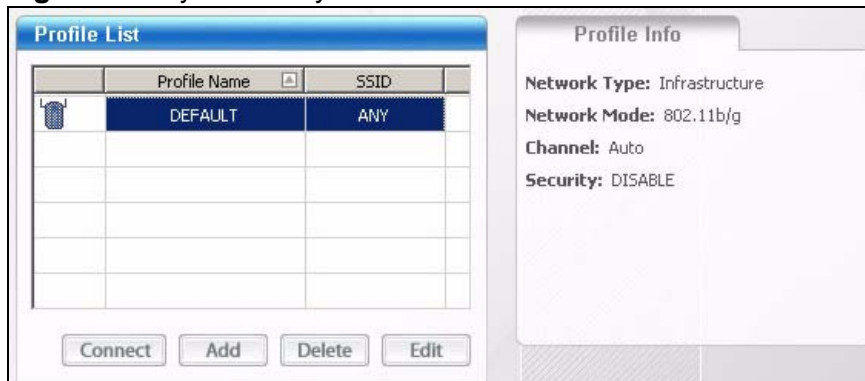
2.1.3.2 Creating and Using a Profile

A profile lets you automatically connect to the same wireless network every time you use the wireless client. You can also configure different profiles for different networks, for example if you connect a notebook computer to wireless networks at home and at work.

This example illustrates how to set up a profile and connect the wireless client to an access point configured for WPA-PSK security. In this example, the SSID is "SSID_Example3", the profile name is "PN_Example3" and the pre-shared key is "ThisismyWPA-PSKpre-sharedkey". You have chosen the profile name "PN_Example3".

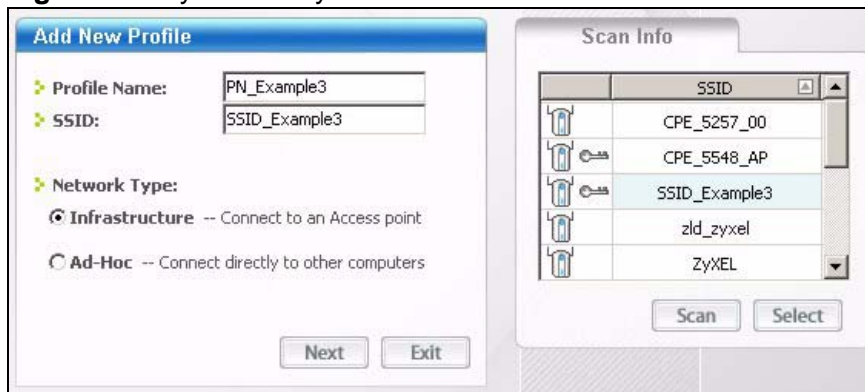
- 1 Open the ZyXEL utility and click the **Profile** tab to open the screen shown next. Click **Add** to configure a new profile.

Figure 12 ZyXEL Utility: Profile



- 2 The **Add New Profile** screen appears. The wireless client automatically searches for available wireless networks, which are displayed in the **Scan Info** box. Click on **Scan** if you want to search again. You can also configure your profile for a wireless network that is not in the list.

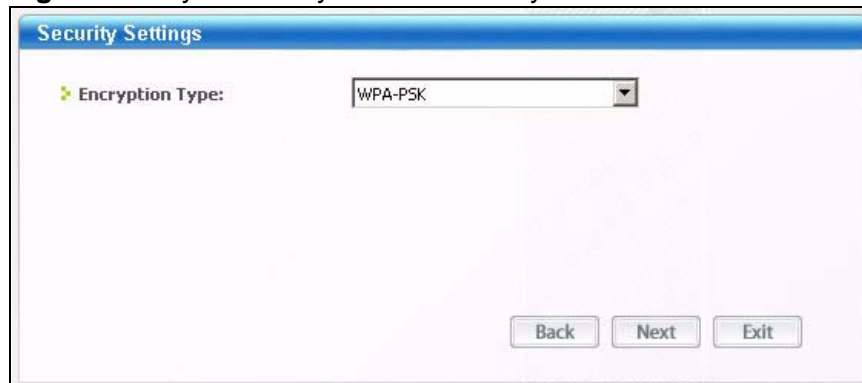
Figure 13 ZyXEL Utility: Add New Profile



- 3 Give the profile a descriptive name (of up to 32 printable ASCII characters). Select **Infrastructure** and either manually enter or select the AP's SSID in the **Scan Info** table and click **Select**.

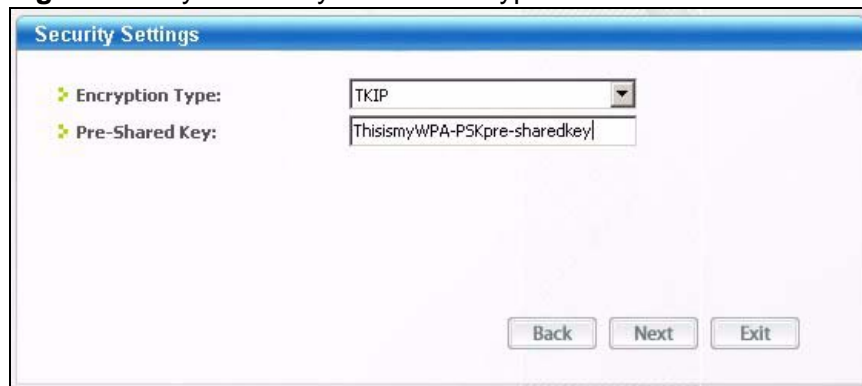
- 4 Choose the same encryption method as the AP to which you want to connect (In this example, WPA-PSK).

Figure 14 ZyXEL Utility: Profile Security



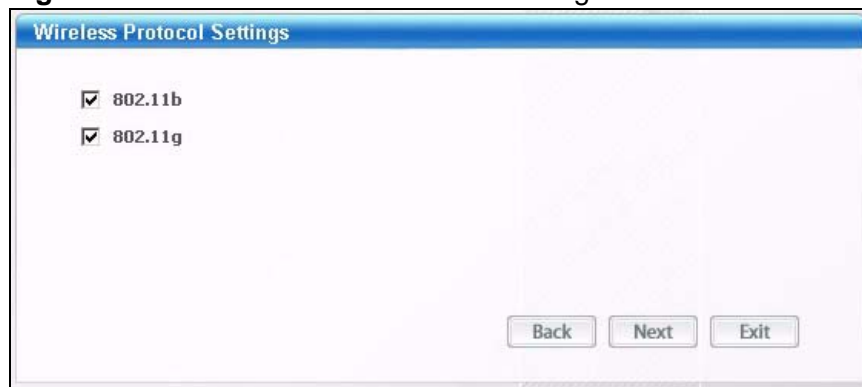
- 5 This screen varies depending on the encryption method you selected in the previous screen. Enter the pre-shared key and leave the encryption type at the default setting.

Figure 15 ZyXEL Utility: Profile Encryption



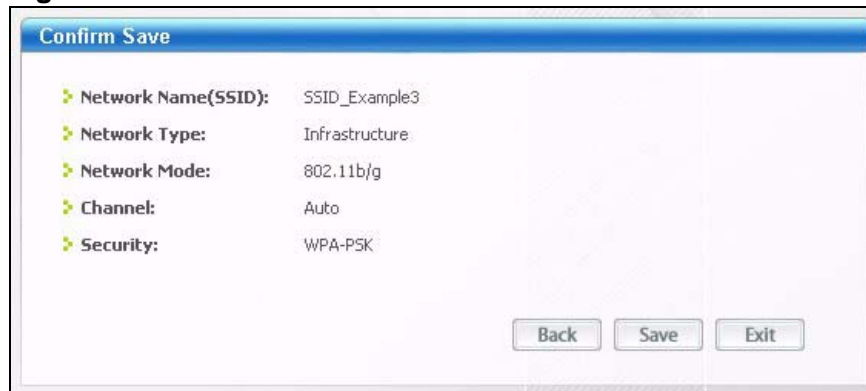
- 6 In the next screen, leave both boxes checked.

Figure 16 Profile: Wireless Protocol Settings.



- 7 Verify the profile settings in the read-only screen. Click **Save** to save and go to the next screen.

Figure 17 Profile: Confirm Save



- 8 Click **Activate Now** to use the new profile immediately. Otherwise, click the **Activate Later** button.

If you clicked **Activate Later**, you can select the profile from the list in the **Profile** screen and click **Connect** to activate it.

Note: Only one profile can be activated and used at any given time.

Figure 18 Profile: Activate



- 9 When you activate the new profile, the ZyXEL utility returns to the **Link Info** screen while it connects to the AP using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection.
- 10 Open your Internet browser, enter <http://www.zyxel.com> or the URL of any other web site in the address bar and press ENTER. If you are able to access the web site, your new profile is successfully configured.
- 11 If you cannot access the Internet go back to the **Profile** screen, select the profile you are using and click **Edit**. Check the details you entered previously. Also, refer to the Troubleshooting section of this User's Guide or contact your network administrator if necessary.

Introducing the Web Configurator

This chapter describes how to access and navigate the Web Configurator.

3.1 Web Configurator 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.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

See [Appendix B on page 271](#) if you need to make sure these functions are allowed in Internet Explorer.

3.1.1 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. Enter the default user name **admin** and default password **1234**. The password displays in non-readable characters. If you have changed the password, enter your password and click **Login**. Click **Cancel** to revert to the default password in the password field.

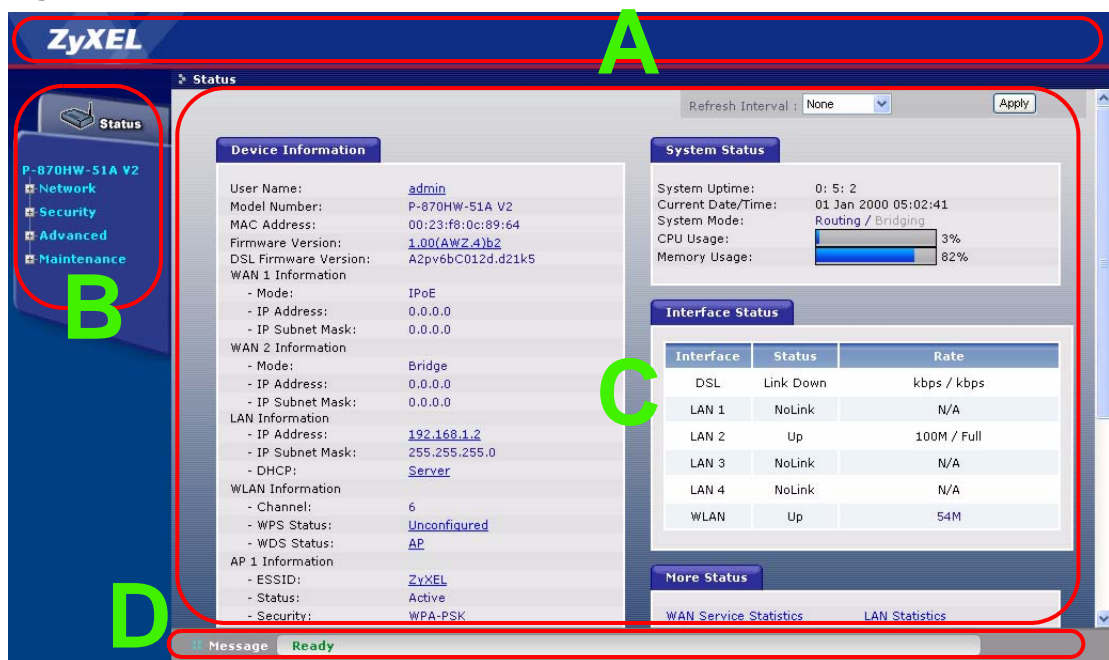
Figure 19 Password Screen



3.2 Web Configurator Main Screen

This guide uses the P-870HW-51a v2 screenshots as an example. The screens may vary slightly for different ZyXEL Device models.

Figure 20 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

3.2.1 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 2 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	Layer 2 Interface	Use this screen to add or remove a DSL PTM (Packet Transfer Mode) interface.
	Internet Connection	Use this screen to configure ISP parameters, WAN IP address assignment, and other advanced properties.
LAN	IP	Use this screen to configure LAN TCP/IP, DHCP and IP alias settings.
Wireless LAN	General	Use this screen to configure the wireless LAN settings, WLAN authentication/security settings and MAC filtering rules.
	More AP	Use this screen to configure multiple BSSs on the ZyXEL Device.
	WPS	Use this screen to enable WPS (Wi-Fi Protected Setup) and view the WPS status.
	WPS Station	Use this screen to use WPS to set up your wireless network.
	WDS	Use this screen to set up Wireless Distribution System links to other access points.
	Advanced Setup	Use this screen to configure the advanced wireless LAN settings.
NAT	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	Address Mapping	Use this screen to configure network address translation mapping rules.
	Trigger Port	Use this screen to change your ZyXEL Device's port triggering settings.
	DMZ Host	Use this screen to configure a default server which receives packets from ports that are not specified in the Port Forwarding screen.
	ALG	Use this screen to allow SIP sessions to pass through the ZyXEL Device.

Table 2 Navigation Panel Summary

LINK	TAB	FUNCTION
Security		
MAC Filter		Use this screen to configure filtering rule(s) that blocks or allows traffic according to its destination and/or source MAC address in bridge mode.
Firewall	Incoming	This screen shows a summary of the IP filtering rules, and allows you to add or remove an incoming IP filtering rule that allows incoming traffic from the WAN.
Certificate	Local Certificates	Use this screen to view a summary list of certificates and manage certificates and certification requests.
	Trusted CA	Use this screen to view and manage the list of the trusted CAs.
Advanced		
Static Route	IP Static Route	Use this screen to configure IP static routes to tell your device about networks beyond the directly connected remote nodes.
Policy Forwarding		Use this screen to configure policy routing on the ZyXEL Device.
RIP		Use this screen to configure RIP (Routing Information Protocol) settings.
QoS	General	Use this screen to enable QoS.
	Queue Setup	Use this screen to configure QoS queues.
	Class Setup	Use this screen to define a classifier.
	Monitor	Use this screen to view QoS packets statistics.
Dynamic DNS		This screen allows you to use a static hostname alias for a dynamic IP address.
Remote MGMT	TR069	Use this screen to configure the ZyXEL Device to be managed by an ACS (Auto Configuration Server).
	TR064	Use this screen to enable management via TR-064 on the LAN.
	ServiceControl	Use this screen to configure which services/protocols can access which ZyXEL Device interface.
	IPAddress	Use this screen to configure from which IP address(es) users can manage the ZyXEL Device.
UPnP	General	Use this screen to turn UPnP on or off.
Parental Control	Time Restriction	Use this screen to configure the days and times when the restrictions are enforced.
	URL Filter	Use this screen to prevent users of your network from viewing inappropriate web content.
Interface Group		Use this screen to map a port to a PVC or bridge group.
Maintenance		
System	General	Use this screen to configure your device's name, domain name, management inactivity timeout and password.
	Time Setting	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.

Table 2 Navigation Panel Summary

LINK	TAB	FUNCTION
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.
	802.1ag	Use this screen to configure CFM (Connectivity Fault Management) MD (maintenance domain) and MA (maintenance association), perform connectivity tests and view test reports.

3.2.2 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 4 on page 43](#) for more information about the **Status** screen.

3.2.3 Status Bar

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

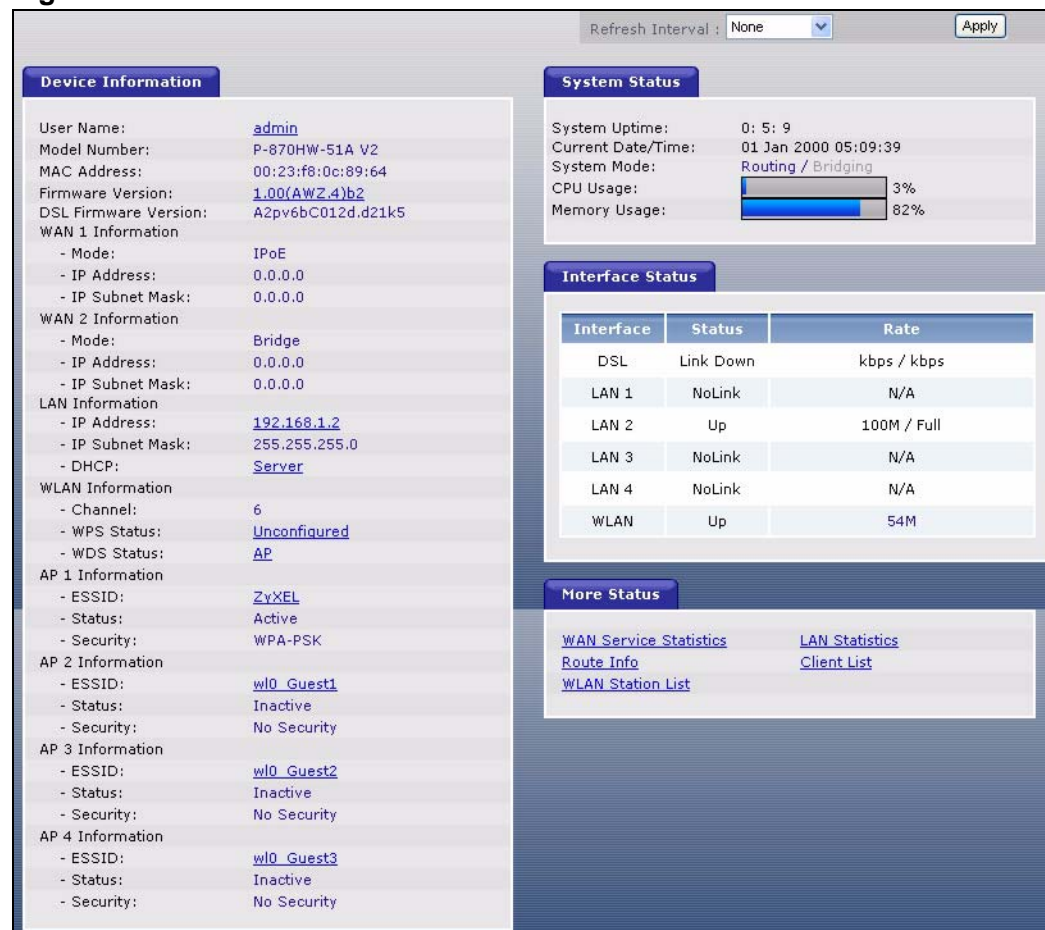
Status Screens

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 traffic.

4.1 Status Screen

Click **Status** to open this screen.

Figure 21 Status Screen



Each field is described in the following table.

Table 3 Status Screen

LABEL	DESCRIPTION
Refresh Interval	Enter 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. Click this to go to the screen where you can change it.
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 field displays the current version of the firmware inside the device. It also shows the date the firmware version was created. Click this to go to the screen where you can change it.
DSL Firmware Version	This field displays the current version of the device's DSL modem code.
WAN Information	
Mode	This is the method of encapsulation used by your ISP.
IP Address	This field displays the current IP address of the ZyXEL Device in the WAN.
IP Subnet Mask	This field displays the current subnet mask in the WAN.
LAN Information	
IP Address	This field displays 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 field displays the current subnet mask in the LAN.
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	
Channel	This is the channel number used by the ZyXEL Device now.

Table 3 Status Screen

LABEL	DESCRIPTION
WPS Status	This field displays the status of WPS (Wi-Fi Protected Setup). Click this to go to the screen where you can change it.
WDS Status	<p>This field displays</p> <ul style="list-style-type: none"> • AP when WDS is disabled. • Bridge when the ZyXEL Device functions as a wireless network bridge only to use WDS (Wireless Distribution System) to establish wireless links with other APs. • AP+Bridge when WDS is enabled and the ZyXEL Device acts as a bridge and access point simultaneously. <p>Click this to go to the screen where you can change it</p>
AP Information	
ESSID	This is the descriptive name used to identify the ZyXEL Device in this wireless network. Click this to go to the screen where you can change it.
Status	This shows the current status of the wireless network.
Security	This shows the level of wireless security the ZyXEL Device is using in this wireless network.
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 (see Section 1.6 on page 25).
Current Date/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 15 on page 163).
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 23.4 on page 222 , 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 3 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 LinkDown (line is down) or Up (line is up or connected).</p> <p>For the LAN interface, this field displays Up when the ZyXEL Device is using the interface and NoLink when the line is disconnected.</p> <p>For the WLAN interface, it displays Up when WLAN is enabled or Disabled when WLAN is not active.</p>
Rate	<p>For the DSL interface, it displays the downstream and upstream transmission rate.</p> <p>For the LAN interface, this displays the port speed and duplex setting.</p> <p>For the WLAN interface, it displays the maximum transmission rate.</p>
More Status	
WAN Service Statistics	Click this link to view packet specific statistics of the WAN connection(s). See Section 4.1.1 on page 47 .
Route Info	Click this link to view the internal routing table on the ZyXEL Device. See Section 4.1.2 on page 48 .
WLAN Station List	Click this link to display the MAC address(es) of the wireless stations that are currently associating with the ZyXEL Device. See Section 4.1.3 on page 49 .
LAN Statistics	Click this link to view packet specific statistics on the LAN and WLAN interfaces. See Section 4.1.4 on page 50 .
Client List	Click this link to view current DHCP client information. See Section 4.1.5 on page 51 .

4.1.1 WAN Service Statistics

Click **Status > WLAN Service Statistics** to access this screen. Use this screen to view the WAN statistics.

Figure 22 Status > WAN Service Statistics

Interface	Description	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
ptm0_1	ipoe_0_0_1_1	0	0	0	0	1494108	5082	0	0
ptm0_2	br_0_0_1_2	0	0	0	0	0	0	0	0

Refresh Interval : 5 sec Set Interval Stop

The following table describes the labels in this screen.

Table 4 Status > WAN Service Statistics

LABEL	DESCRIPTION
Interface	This shows the name of the WAN interface used by this connection. The default name ptm0 indicates the DSL port. The last number represents the index number of connections over the same PVC or the VLAN ID number assigned to traffic sent through this connection.
Description	This shows the descriptive name of this connection.
Received	
Bytes	This indicates the number of bytes received on this interface.
Pkts	This indicates the number of transmitted packets on this interface.
Errs	This indicates the number of frames with errors received on this interface.
Drops	This indicates the number of received packets dropped on this interface.
Transmitted	
Bytes	This indicates the number of bytes transmitted on this interface.
Pkts	This indicates the number of transmitted packets on this interface.
Errs	This indicates the number of frames with errors transmitted on this interface.
Drops	This indicates the number of outgoing packets dropped on this interface.

Table 4 Status > WAN Service Statistics (continued)

LABEL	DESCRIPTION
Refresh Interval	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the Refresh Interval field.
Stop	Click Stop to stop refreshing statistics.

4.1.2 Route Info

Routing is based on the destination address only and the ZyXEL Device takes the shortest path to forward a packet. Click **Status > Route Info** to access this screen. Use this screen to view the internal routing table on the ZyXEL Device.

Figure 23 Status > Route Info

Route Info						
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate, D - dynamic (redirect), M - modified (redirect).						
Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
172.16.31.0	0.0.0.0	255.255.255.0	U	0	ipoe_0_0_1_1	ptm0_1
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
0.0.0.0	172.16.31.254	0.0.0.0	UG	0	ipoe_0_0_1_1	ptm0_1

The following table describes the labels in this screen.

Table 5 Status > Route Info

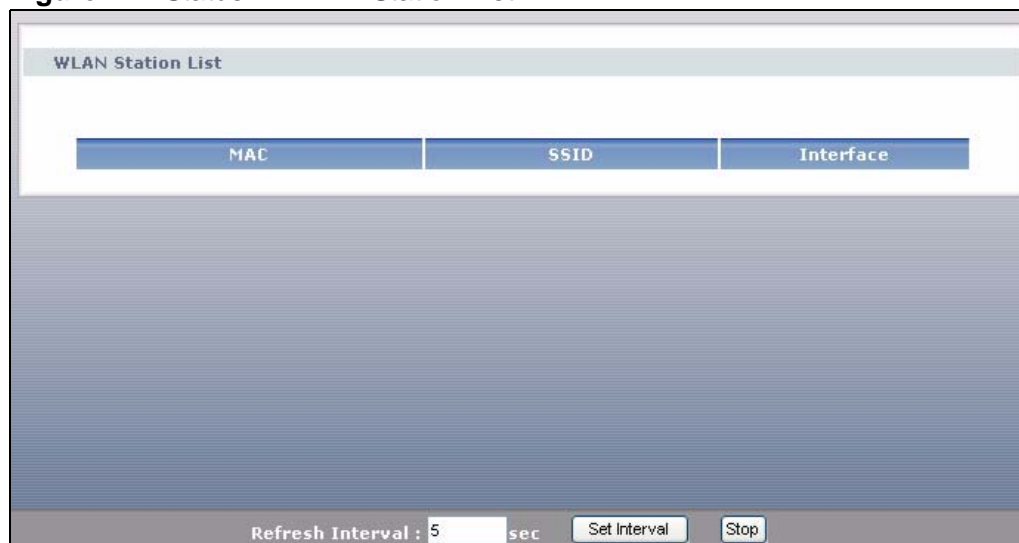
LABEL	DESCRIPTION
Destination	This indicates the destination IP address of this route.
Gateway	This indicates the IP address of the gateway that helps forward this route's traffic.
Subnet Mask	This indicates the destination subnet mask of this route.
Flag	<p>This indicates the route status.</p> <p>Up: The route is up.</p> <p>!(Reject): The route is blocked and will force a route lookup to fail.</p> <p>Gateway: The route uses a gateway to forward traffic.</p> <p>Host: The target of the route is a host.</p> <p>Reinstate: The route is reinstated for dynamic routing.</p> <p>Dynamic (redirect): The route is dynamically installed by a routing daemon or redirect</p> <p>Modified (redirect): The route is modified from a routing daemon or redirect.</p>

Table 5 Status > Route Info (continued)

LABEL	DESCRIPTION
Metric	The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". The smaller the number, the lower the "cost".
Service	This indicates the name of the service used to forward the route.
Interface	This indicates the name of the interface through which the route is forwarded. br0 indicates the LAN interface. ptm0 indicates the WAN interface using IPoE or in bridge mode. ppp0 indicates the WAN interface using PPPoE.

4.1.3 WLAN Station List

Click **Status > WLAN Station List** to access this screen. Use this screen to view the wireless stations that are currently associated to the ZyXEL Device.

Figure 24 Status > WLAN Station List

The following table describes the labels in this screen.

Table 6 Status > WLAN Station List

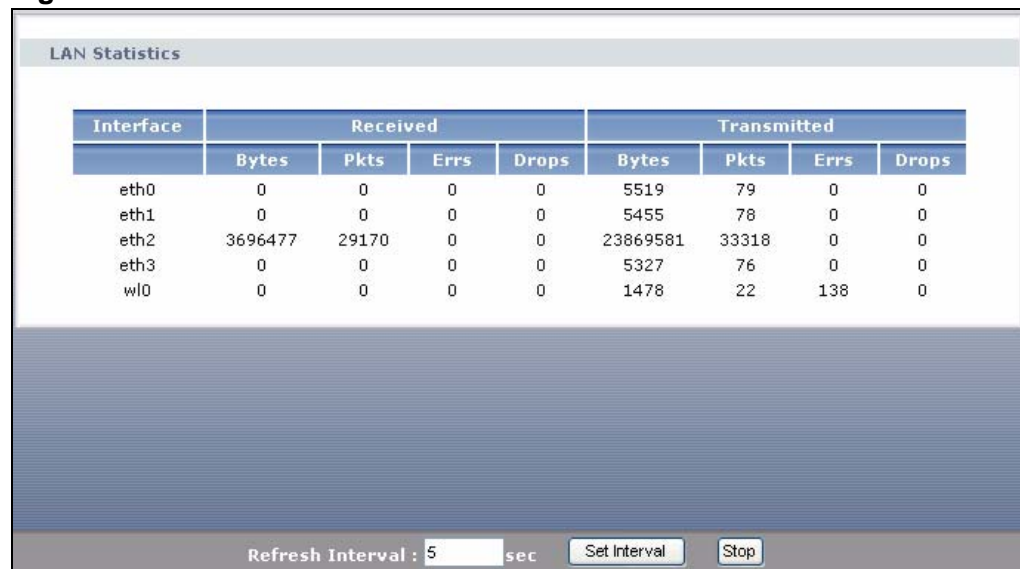
LABEL	DESCRIPTION
MAC	This field shows the MAC (Media Access Control) address of an associated wireless station.
SSID	This field shows the SSID to which the wireless station is connected.
Interface	This field shows the wireless interface to which the wireless station is connected.
Refresh Interval	Enter the time interval for refreshing statistics in this field.

Table 6 Status > WLAN Station List (continued)

LABEL	DESCRIPTION
Set Interval	Click this button to apply the new poll interval you entered in the Refresh Interval field.
Stop	Click Stop to stop refreshing statistics.

4.1.4 LAN Statistics

Click **Status > LAN Statistics** to access this screen. Use this screen to view the LAN statistics.

Figure 25 Status > LAN Statistics


The screenshot shows the 'LAN Statistics' screen. It features a table with columns for Interface, Received (Bytes, Pkts, Errs, Drops), and Transmitted (Bytes, Pkts, Errs, Drops). The data is as follows:

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth0	0	0	0	0	5519	79	0	0
eth1	0	0	0	0	5455	78	0	0
eth2	3696477	29170	0	0	23869581	33318	0	0
eth3	0	0	0	0	5327	76	0	0
wl0	0	0	0	0	1478	22	138	0

At the bottom of the screen, there is a 'Refresh Interval : 5 sec' label, a 'Set Interval' button, and a 'Stop' button.

The following table describes the labels in this screen.

Table 7 Status > LAN Statistics

LABEL	DESCRIPTION
Interface	This shows the LAN or WLAN interface. eth0~3 represent the physical Ethernet ports 1 ~ 4.
Received	
Bytes	This indicates the number of bytes received on this interface.
Pkts	This indicates the number of transmitted packets on this interface.
Errs	This indicates the number of frames with errors received on this interface.
Drops	This indicates the number of received packets dropped on this interface.
Transmitted	
Bytes	This indicates the number of bytes transmitted on this interface.
Pkts	This indicates the number of transmitted packets on this interface.
Errs	This indicates the number of frames with errors transmitted on this interface.

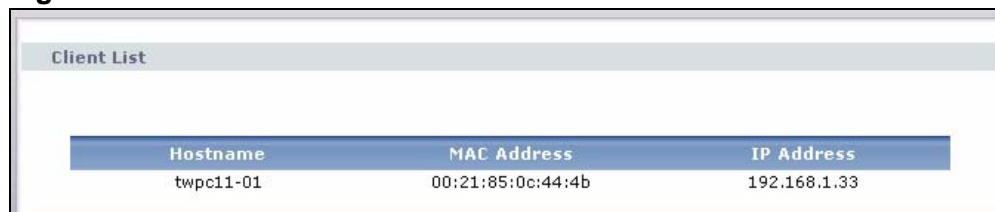
Table 7 Status > LAN Statistics (continued)

LABEL	DESCRIPTION
Drops	This indicates the number of outgoing packets dropped on this interface.
Refresh Interval	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the Refresh Interval field.
Stop	Click Stop to stop refreshing statistics.

4.1.5 Client List

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 DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

Click **Status > Client List** to open the following screen. The read-only DHCP table shows current DHCP client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the ZyXEL Device's DHCP server.

Figure 26 Status > Client List


Client List		
Hostname	MAC Address	IP Address
twpc11-01	00:21:85:0c:44:4b	192.168.1.33

The following table describes the labels in this screen.

Table 8 Status > Client List

LABEL	DESCRIPTION
Host Name	This indicates the computer host name.
MAC Address	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. This indicates the MAC address of the client computer.
IP Address	This indicates the IP address assigned to this client computer.

PART II

Technical Reference

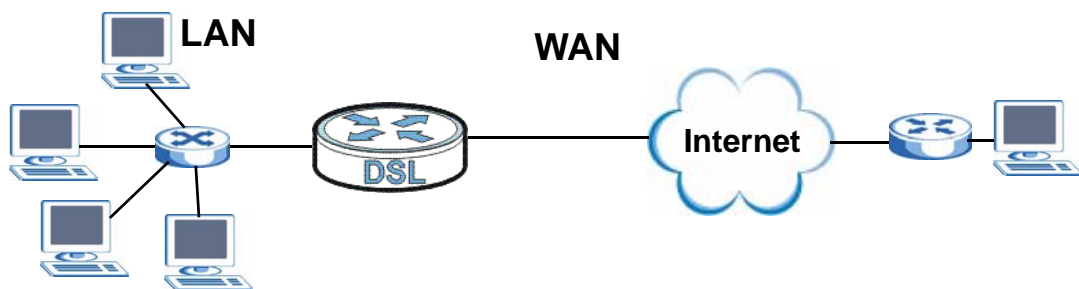
WAN Setup

5.1 Overview

This chapter discusses the ZyXEL Device's **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 27 LAN and WAN



- See [Section 5.6 on page 71](#) for advanced technical information on WAN.

5.1.1 What You Can Do in this Chapter

- The **Layer 2 Interface** screen lets you view, remove or add a DSL PTM interface ([Section 5.4 on page 56](#)).
- The **Internet Connection** screen lets you view and configure the WAN settings on the ZyXEL Device for Internet access ([Section 5.5 on page 59](#)).

5.2 What You Need to Know

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).

PTM

Packet Transfer Mode (PTM) is packet-oriented and supported by the VDSL2 standard. In PTM, packets are encapsulated directly in the High-level Data Link Control (HDLC) frames. It is designed to provide a low-overhead, transparent way of transporting packets over DSL links, as an alternative to ATM.

5.3 Before You Begin

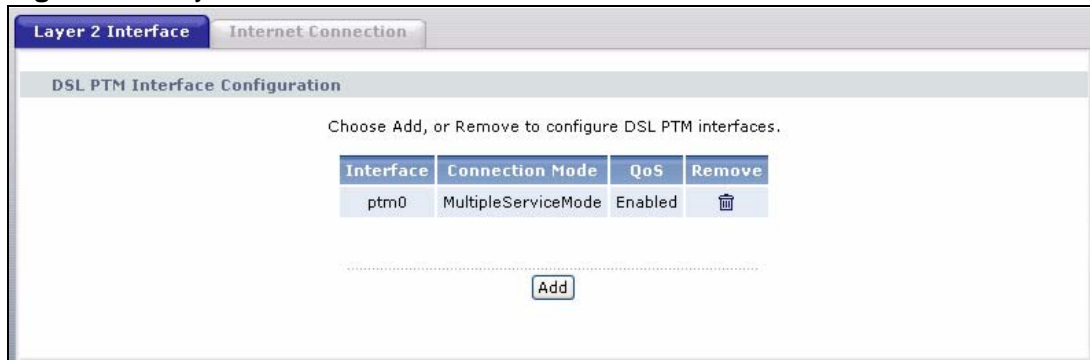
You need to know your Internet access settings such as encapsulation and WAN IP address. Get this information from your ISP.

5.4 The Layer 2 Interface Screen

The ZyXEL Device must have a DSL PTM interface to allow users to use the DSL port to access the Internet.

Note: At the time of writing, you can have only one DSL PTM interface on the ZyXEL Device.

Figure 28 Layer 2 Interface



The following table describes the fields in this screen.

Table 9 Layer 2 Interface

LABEL	DESCRIPTION
Interface	This is the name of the interface.
Connection Mode	This shows the connection mode of the DSL interface.
QoS	This shows whether QoS (Quality of Service) is enabled on the ZyXEL Device.
Remove	Click the Remove button to delete this interface from the ZyXEL Device. A window displays asking you to confirm that you want to delete the interface. You cannot remove the DSL interface when a service is associated with it.
Add	Click this button to create a new DSL interface.

5.4.1 Layer 2 Interface Configuration

Click the **Add** button in the **Layer 2 Interface** screen to open the following screen. Use this screen to create a new DSL PTM interface. At the time of writing, you can configure only one DSL interface on the ZyXEL Device.

Figure 29 DSL PTM Interface Configuration

The following table describes the fields in this screen.

Table 10 DSL PTM Interface Configuration

LABEL	DESCRIPTION
Select Connection Mode	<p>Select MSC Mode to allow multiple WAN services over a single virtual circuit.</p> <p>Select VLAN MUX Mode to allow multiplexing of multiple protocols over a single virtual circuit. You need to assign a VLAN ID and priority level to traffic through each WAN connection.</p>
Enable Quality Of Service	<p>Select this option to activate QoS (Quality of Service) on this interface to group and prioritize traffic. Traffic is grouped according to the VLAN group.</p> <p>The QoS setting applies to all WAN connections over the same PVC.</p>
Back	Click this button to return to the previous screen without saving any changes.
Apply/Save	Click this button to save your changes and go back to the previous screen.

5.5 The Internet Connection Screen

Use this screen to change your ZyXEL Device's WAN settings. Click **Network > WAN > Internet Connection**. The summary table shows you the configured WAN connection(s) on the ZyXEL Device.

To use NAT, firewall or IGMP proxy in the ZyXEL Device, you need to configure a WAN connection with PPPoE or IPoE.

Note: When the DSL PTM interface is in VLAN MUX mode, you can configure up to eight connections over a DSL PTM interface on the ZyXEL Device. All WAN connections share one MAC address.

When the DSL PTM interface is in MSC mode, you can have up to four WAN connections and only one bridge connection. Each WAN connection has its own MAC address.

Figure 30 Internet Connection

Interface	Description	Type	Rate	Vlan8021p	VlanMuxId	ConnId	IGMP	NAT	Firewall	Modify
ptm0_1	ipoe_0_0_1_1	IPoE	N/A	N/A	N/A	1	Disabled	Enabled	Enabled	

Add

The following table describes the labels in this screen.

Table 11 Internet Connection

LABEL	DESCRIPTION
Interface	<p>This shows the name of the interface used by this connection.</p> <p>The default name ptm0_ or ppp0_ indicates the DSL port. The last number represents the index number of connections over the same PVC or the VLAN ID number assigned to traffic sent through this connection.</p>
Description	<p>This is the service name of this connection.</p> <p>0 and 1 are the default VPI and VCI numbers. The last number represents the index number of connections over the same PVC or the VLAN ID number assigned to traffic sent through this connection.</p>
Type	This shows the method of encapsulation used by this connection.
Rate	This shows the maximum data rate (in Kbps) allowed for traffic sent through this connection. This displays N/A when there is no limit on transmission rate.

Table 11 Internet Connection

LABEL	DESCRIPTION
Vlan8021p	This indicates the 802.1P priority level assigned to traffic sent through this connection. This displays N/A when there is no priority level assigned.
VlanMuxId	This indicates the VLAN ID number assigned to traffic sent through this connection. This displays N/A when there is no VLAN ID number assigned.
ConnId	This shows the index number of each connection.
IGMP	This shows whether IGMP (Internet Group Multicast Protocol) is activated or not for this connection. IGMP is not available when the connection uses the bridging service.
NAT	This shows whether NAT is activated or not for this interface. NAT is not available when the connection uses the bridging service.
Firewall	This shows whether the firewall is activated or not for this connection. The firewall is not available when the connection uses the bridging service.
Modify	Click the Edit icon to configure the WAN connection. Click the Remove icon to delete the WAN connection.
Add	Click Add to create a new connection.

5.5.1 WAN Connection Configuration

Click the **Edit** or **Add** button in the **WAN Service** screen to configure a WAN connection.

5.5.1.1 WAN Interface

This screen displays when you add a new WAN connection.

Figure 31 WAN Configuration: WAN Interface

WAN Service Interface Configuration

Select a layer 2 interface for this service

ptm0/(0_0_1)

Back Next

The following table describes the labels in this screen.

Table 12 WAN Configuration: WAN Interface

LABEL	DESCRIPTION
Select a layer 2 interface for this service	Select ptm0 to use the DSL port as the WAN port for this connection.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

5.5.1.2 Service Type

Figure 32 WAN Configuration: Service Type

The following table describes the labels in this screen.

Table 13 WAN Configuration: Service Type

LABEL	DESCRIPTION
Select WAN service type	Select the method of encapsulation used by your ISP. Choices are PPP over Ethernet (PPPoE) , IP over Ethernet and Bridging .
Enter Service Description	Specify a name for this connection or use the automatically generated one.
Rate Limit	Enter the maximum transmission rate in Kbps for traffic sent through the WAN connection. Otherwise, leave this field blank to disable the rate limit.
Tag VLAN ID for egress packets	Select this option to add the VLAN tag (specified below) to the outgoing traffic through this connection. This field is available when the PTM interface is in VLANMUX mode.

Table 13 WAN Configuration: Service Type

LABEL	DESCRIPTION
Enter 802.1P Priority	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Type the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level. This field is available when the PTM interface is in VLANMUX mode.
Enter 802.1Q VLAN ID	Type the VLAN ID number (from 1 to 4094) for traffic through this connection. This field is available when the PTM interface is in VLANMUX mode.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

5.5.1.3 WAN IP Address and DNS Server

The screen differs by the encapsulation you selected in the previous screen. See [Section 5.6 on page 71](#) for more information.

PPPoE

This screen displays when you select **PPP over Ethernet (PPPoE)** in the **WAN Service Configuration** screen.

Figure 33 WAN Configuration: PPPoE

PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method: AUTO

☒ Enable Fullcone NAT

☒ Dial on demand (with idle timeout timer)

Inactivity Timeout (minutes) [1-4320]:

☒ Use Static IPv4 Address

IPv4 Address:

☐ Enable PPP Debug Mode

☐ Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

☐ Enable IGMP Multicast Proxy

Back Next

The following table describes the labels in this screen.

Table 14 WAN Configuration: PPPoE

LABEL	DESCRIPTION
PPP 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.
PPP Password	Enter the password associated with the user name above.
PPPoE Service Name	Type the name of your PPPoE service here.

Table 14 WAN Configuration: PPPoE

LABEL	DESCRIPTION
Authentication Method	<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> <p>MSCHAP - Your ZyXEL Device accepts MSCHAP only. MS-CHAP is the Microsoft version of the CHAP.</p>
Enable Fullcone NAT	Select this option to enable full cone NAT on the ZyXEL Device.
Dial on Demand	Select this check box when you do not want the connection up all the time and specify an idle time-out in the Inactivity Timeout field.
Inactivity Timeout	Specify an idle time-out when you select Dial on Demand . The default setting is 0, which means the Internet session will not timeout.
Use Static IPv4 Address	A static IPv4 address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you do not have a dynamic IP address.
IPv4 Address	Enter the static IP address provided by your ISP.
Enable PPP Debug Mode	Select this option to display PPP debugging messages on the console.
Bridge PPPoE Frames Between WAN and Local Ports	<p>Select this option to forward PPPoE packets from the WAN port to the LAN ports and from the LAN ports to the WAN port.</p> <p>In addition to the ZyXEL Device's built-in PPPoE client, you can select this to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the ZyXEL Device. Each host can have a separate account and a public WAN IP address.</p> <p>This is an alternative to NAT for application where NAT is not appropriate.</p> <p>Clear this if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.</p>
Enable IGMP Multicast Proxy	Select this check box to have the ZyXEL Device act as an IGMP proxy on this connection. This allows the ZyXEL Device to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

IPoE

This screen displays when you select **IP over Ethernet** in the **WAN Service Configuration** screen.

Figure 34 WAN Configuration: IPoE

DSL PTM Interface Configuration

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
 Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in MER mode.
 If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.

☒ Obtain an IP address automatically

☐ Enable DHCP Option 60
 Vendor class Identifier: 0023f80c8964

☐ Enable DHCP Option 61
 IAID:
 DUID type: DUID-EN
 Enterprise Number: 890
 Identifier: 3daf2f5b

☐ Enable DHCP Option 125
 Manufacturer OUI: 0023f8
 Product class: P-870HW-51A V2
 Model name: P-870HW-51A V2
 Serial number: 0023f80c8964

☐ Use the following Static IP address:
 WAN IP Address:
 WAN Subnet Mask:
 WAN gateway IP Address:

The following table describes the labels in this screen.

Table 15 WAN Configuration: IPoE

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 this if you have a dynamic IP address.
Enable DHCP Option 60	Select this to identify the vendor and functionality of the ZyXEL Device in DHCP requests that the ZyXEL Device sends to a DHCP server when getting a WAN IP address.
Vendor Class Identifier	Enter the Vendor Class Identifier (Option 60), such as the type of the hardware or firmware.
Enable DHCP Option 61	Select this to identify the ZyXEL Device in DHCP requests that the ZyXEL Device sends to a DHCP server when getting a WAN IP address.
IAID	Enter the Identity Association Identifier (IAID) of the ZyXEL Device. For example, the WAN connection index number.

Table 15 WAN Configuration: IPoE

LABEL	DESCRIPTION
DUID Type	<p>Select Other to enter any string that identifies the ZyXEL Device in the DUID field.</p> <p>Select DUID-LL (DUID Based on Link-layer Address) to enter the ZyXEL Device's hardware address, that is the MAC address in the DUID field.</p> <p>Select DUID-EN (DUID Assigned by Vendor Based on Enterprise Number) to enter the vendor's registered private enterprise number.</p>
DUID	Enter the DHCP Unique Identifier (DUID) of the ZyXEL Device.
Enterprise number	<p>Enter the vendor's 32-bit enterprise number registered with the IANA (Internet Assigned Numbers Authority).</p> <p>This field is available when you select DUID-EN in the DUID Type field.</p>
Identifier	<p>Enter a unique identifier assigned by the vendor.</p> <p>This field is available when you select DUID-EN in the DUID Type field.</p>
Enable DHCP Option 125	Select this to add vendor specific information to DHCP requests that the ZyXEL Device sends to a DHCP server when getting a WAN IP address.
Manufacturer OUI	Specify the vendor's OUI (Organization Unique Identifier). It is usually the first three bytes of the MAC address.
Product Class	Enter the product class of the ZyXEL Device.
Model Name	Enter the model name of the ZyXEL Device.
Serial Number	Enter the serial number of the ZyXEL Device.
Use the following Static IP address	Select this if you have a static IP address.
WAN IP Address	Enter the static IP address provided by your ISP.
WAN Subnet Mask	Enter the subnet mask provided by your ISP.
WAN gateway IP Address	Enter the gateway IP address provided by your ISP.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

5.5.1.4 NAT, IGMP Multicast and Firewall Activation

The screen is available only when you select **IP over Ethernet** in the **WAN Service Configuration** screen.

Figure 35 WAN Configuration: NAT, IGMP Multicast and Firewall Activation: IPoE

Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

☒ Enable NAT

☐ Enable Fullcone NAT

☐ Enable Address Mapping

Address Mapping Set 1

☒ Enable Firewall

IGMP Multicast

☐ Enable IGMP Multicast Proxy

Back Next

The following table describes the labels in this screen.

Table 16 WAN Configuration: NAT, IGMP Multicast and Firewall Activation: IPoE

LABEL	DESCRIPTION
Enable NAT	Select this check box to activate NAT on this connection.
Enable Fullcone NAT	Select this check box to activate full cone NAT on this connection. This field is available only when you select Enable NAT .
Enable Address Mapping	Select this check box to activate NAT address mapping on this connection. There is no default address mapping rule. You need to configure the address mapping rules manually in the NAT > Address Mapping screen. This field is available only when you configure a static IP address in the previous screen and select Enable NAT .
Address Mapping Set	Select the index number of the address mapping set that you want to use on this connection. This field is available only when you configure a static IP address in the previous screen and select Enable NAT .
Enable Firewall	Select this check box to activate Firewall on this connection.
Enable IGMP Multicast Proxy	Select this check box to have the ZyXEL Device act as an IGMP proxy on this connection. This allows the ZyXEL Device to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.

Table 16 WAN Configuration: NAT, IGMP Multicast and Firewall Activation: IPoE

LABEL	DESCRIPTION
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

5.5.1.5 Default Gateway

The screen is available when you select **PPP over Ethernet** or **IP over Ethernet** in the **WAN Service Configuration** screen.

Figure 36 WAN Configuration: Default Gateway: PPPoE or IPoE

The following table describes the labels in this screen.

Table 17 WAN Configuration: Default Gateway: PPPoE or IPoE

LABEL	DESCRIPTION
Selected WAN Interface	Select a WAN interface through which you want to forward the traffic.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

5.5.1.6 DNS Server

The screen is available when you select **PPP over Ethernet** or **IP over Ethernet** in the **WAN Service Configuration** screen.

Figure 37 WAN Configuration: DNS Server: PPPoE or IPoE

DNS Server Configuration

Get DNS server information from the selected WAN interface OR enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.

☒ Obtain DNS info from a WAN interface:
 WAN Interface selected: pppoe_0_0_1_2/ppp0_1

☐ Use the following Static DNS IP address:
 Primary DNS server:
 Secondary DNS server:

Back Next

The following table describes the labels in this screen.

Table 18 WAN Configuration: DNS Server: PPPoE or IPoE

LABEL	DESCRIPTION
Obtain DNS info from a WAN interface	Select this to have the ZyXEL Device get the DNS server addresses from the ISP automatically.
WAN interface selected	This displays the WAN interface you selected in the previous screen.
Use the following Static DNS IP address	Select this to have the ZyXEL Device use the DNS server addresses you configure manually.
Primary DNS server	Enter the first DNS server address assigned by the ISP.
Secondary DNS server	Enter the second DNS server address assigned by the ISP.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

5.5.1.7 Configuration Summary

This read-only screen shows the current WAN connection settings.

Figure 38 WAN Configuration: Configuration Summary

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	PPPoE
Service Name:	pppoe_0_0_1_2
Service Category:	
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Full Cone NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

[Back](#) [Apply/Save](#)

The following table describes the labels in this screen.

Table 19 WAN Configuration: Configuration Summary

LABEL	DESCRIPTION
Connection Type	This is the encapsulation method used by this connection.
Service Name	This is the name of the service.
IP Address	This shows whether the WAN IP address is assigned by the ISP, manually configured or not configurable.
Service State	This shows whether this service is active or not.
NAT	This shows whether NAT is active or not for this connection.
Full Cone NAT	This shows whether full cone NAT is active or not for this connection.
Firewall	This shows whether Firewall is active or not for this connection.
IGMP Multicast	This shows whether IGMP multicasting is active or not for this connection.
Quality Of Service	This shows whether QoS is active or not for this connection.
Back	Click this button to return to the previous screen.
Apply/Save	Click this button to save your changes.

5.6 Technical Reference

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

Encapsulation

Be sure to use the encapsulation method required by your ISP. The ZyXEL Device can work in bridge mode or routing mode. When the ZyXEL Device is in routing mode, it supports the following methods.

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.

PPP over Ethernet

Point-to-Point Protocol over Ethernet (PPPoE) provides access control and billing functionality in a manner similar to dial-up services using PPP. PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection.

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.

IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the

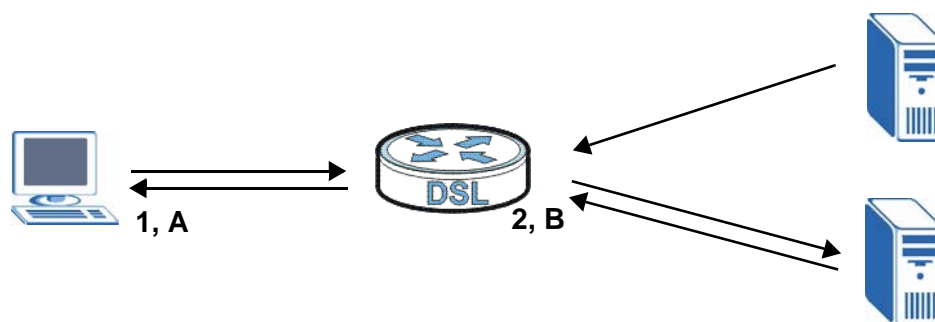
encapsulation method assigned influences your choices for IP address and default gateway.

Full Cone NAT

In full cone NAT, the NAT router maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. The NAT router also maps packets coming to that external IP address and port to the internal IP address and port.

In the following example, the ZyXEL Device maps the source address of all packets sent from the internal IP address **1** and port **A** to IP address **2** and port **B** on the external network. The ZyXEL Device also performs NAT on all incoming packets sent to IP address **2** and port **B** and forwards them to IP address **1**, port **A**.

Figure 39 Full Cone NAT Example



Symmetric NAT

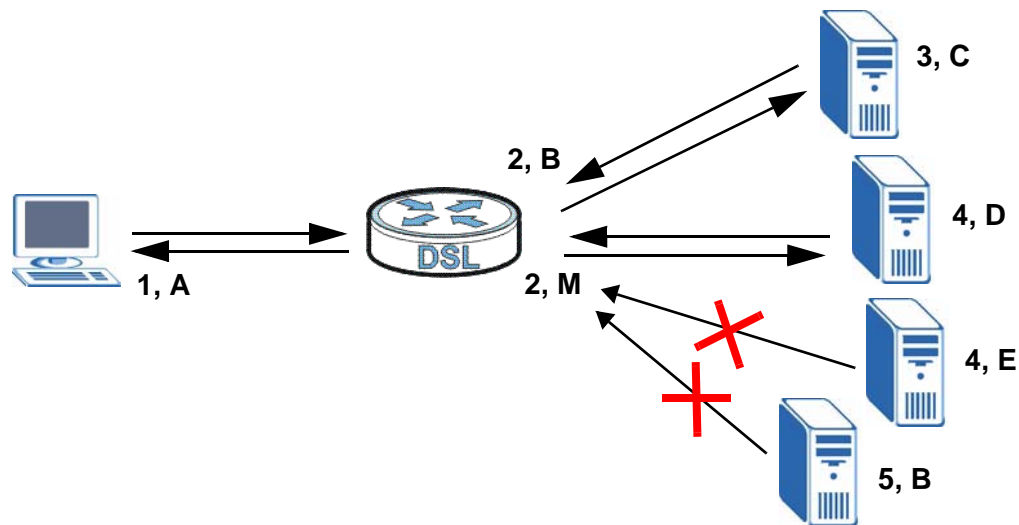
The full, restricted and port restricted cone NAT types use the same mapping for an outgoing packet's source address regardless of the destination IP address and port. In symmetric NAT, the mapping of an outgoing packet's source address to a source address in another network is different for each different destination IP address and port.

In the following example, the ZyXEL Device maps the source address IP address **1** and port **A** to IP address **2** and port **B** on the external network for packets sent to IP address **3** and port **C**. The ZyXEL Device uses a different mapping (IP address **2** and port **M**) for packets sent to IP address **4** and port **D**.

A host on the external network (IP address **3** and port **C** for example) can only send packets to the internal host via the external IP address and port that the NAT router used in sending a packet to the external host's IP address and port. So in

the example, only **3, C** is allowed to send packets to **2, B** and only **4, D** is allowed to send packets to **2, M**.

Figure 40 Symmetric NAT



Introduction to VLANs

A Virtual Local Area Network (VLAN) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In Multi-Tenant Unit (MTU) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

Introduction to IEEE 802.1Q Tagged VLAN

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and

contains two bytes of TPID (Tag Protocol Identifier), residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information), starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID	User Priority	CFI	VLAN ID
2 Bytes	3 Bits	1 Bit	12 Bits

Multicast

IP packets are transmitted in either one of 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.

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

DNS Server Address Assignment

Use Domain Name System (DNS) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is

204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

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

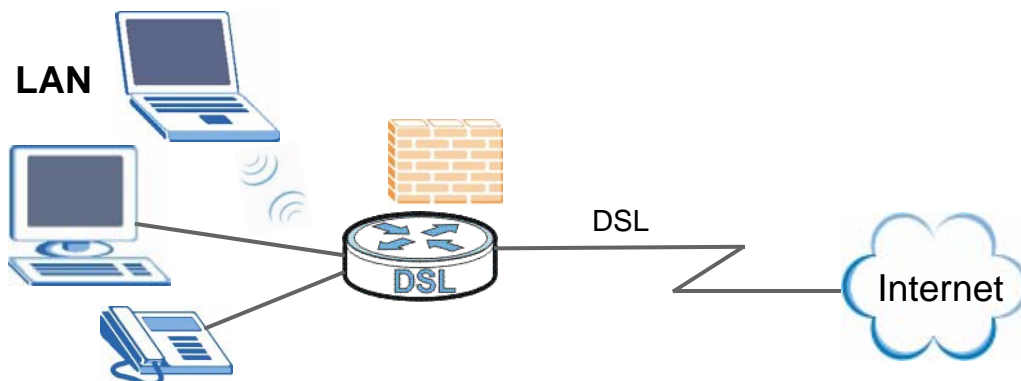
- 1** The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
- 2** If your ISP dynamically assigns the DNS server IP addresses (along with the ZyXEL Device's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

LAN Setup

6.1 Overview

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

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



- See [Section 6.4 on page 81](#) for more information on LANs.
- See [Appendix D on page 293](#) for more information on IP addresses and subnetting.

6.1.1 What You Can Do in this Chapter

The **LAN IP** screen lets you set the LAN IP address and subnet mask of your ZyXEL device and configure other LAN TCP/IP settings ([Section 6.3 on page 79](#)).

6.2 What You Need To Know

IP Address

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

Subnet Mask

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

DHCP

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

DHCP Relay

You can also configure the ZyXEL Device to relay client DHCP requests to a DHCP server and the server's responses back to the clients.

RIP

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

Multicast and IGMP

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. There are two versions 1 and 2. IGMP version 2 is an improvement over version 1 but IGMP version 1 is still in wide use.

DNS

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

6.3 The LAN IP Screen

Click **Network > LAN** to open the **IP** screen. See [Section 6.4 on page 81](#) for background information. Use this screen to set the Local Area Network IP address and subnet mask of your ZyXEL Device.

Figure 41 LAN > IP

IP

LAN TCP/IP

GroupName

Default

IP Address

192.168.1.2

IP Subnet Mask

255.255.255.0

DHCP Setup

☒ Active DHCP

☒ DHCP Server

IP Pool Starting Address

192.168.1.33

Pool Size

100

☐ DHCP Relay

Relay Server

DNS Server

DNS Servers Assigned by DHCP Server

First DNS Server

0.0.0.0

Second DNS Server

0.0.0.0

IGMP Snooping

☐ Active IGMP Snooping

☒ Standard Mode

☐ Blocking Mode

IP Alias

☐ Active IP Alias

IP Address

IP Subnet Mask

Apply

The following table describes the fields in this screen.

Table 20 LAN > IP

LABEL	DESCRIPTION
LAN TCP/IP	
Group Name	Select the interface group for which you want to configure the LAN TCP/IP settings. See Chapter 20 on page 203 for how to create a new interface group.
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).
DHCP Setup	
Active DHCP	Select this to have the ZyXEL Device act as a DHCP server or DHCP relay agent. Otherwise, deselect this to not have the ZyXEL Device provide any DHCP services. The DHCP server will be disabled.
DHCP Server	Select this option to have the ZyXEL Device assign IP addresses and provide subnet mask, gateway, and DNS server information to the network. The ZyXEL Device is the DHCP server for the network. When the ZyXEL Device acts as a DHCP server, the following items need to be set:
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
DHCP Relay	Select this option to have the ZyXEL Device forward DHCP request to the DHCP server.
Relay Server	If you select DHCP Relay , enter the IP address of the DHCP server.
DNS Servers Assigned by DHCP Server	
If you do not configure DNS servers, the ZyXEL Device uses its LAN IP address and tells the DHCP clients on the LAN that itself is the DNS server. When a LAN client sends a DNS query to the ZyXEL Device, the ZyXEL Device forwards the query to its system DNS server you configured in the WAN screen.	
First DNS Server	Enter the first DNS (Domain Name System) server IP address the ZyXEL Device passes to the DHCP clients.
Second DNS Server	Enter the second DNS (Domain Name System) server IP address the ZyXEL Device passes to the DHCP clients.
IGMP Snooping	
Active IGMP Snooping	Select this option to enable IGMP snooping. This allows the ZyXEL Device to passively learn multicast group.
Standard Mode	Select this to have the ZyXEL Device forward multicast packets to a port that joins the multicast group and broadcast unknown multicast packets from the WAN to all LAN ports.
Blocking Mode	Select this to have the ZyXEL Device block all unknown multicast packets from the WAN.

Table 20 LAN > IP

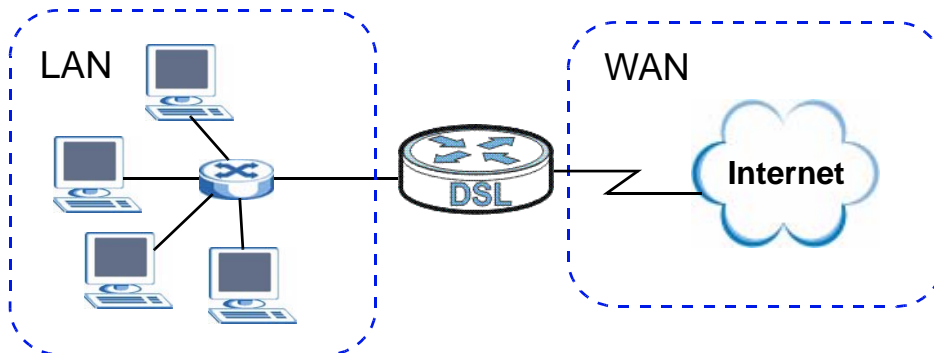
LABEL	DESCRIPTION
Active IP Alias	Select the check box to configure another LAN network for the ZyXEL Device.
IP Address	Enter the IP address of your ZyXEL Device in dotted decimal notation.
IP Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default).
Apply	Click Apply to save your changes back to the ZyXEL Device.

6.4 Technical Reference

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

LANs, WANs and the ZyXEL Device

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

Figure 42 LAN and WAN IP Addresses

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.

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".

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. 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.

The ZyXEL Device supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). 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.

IP Alias

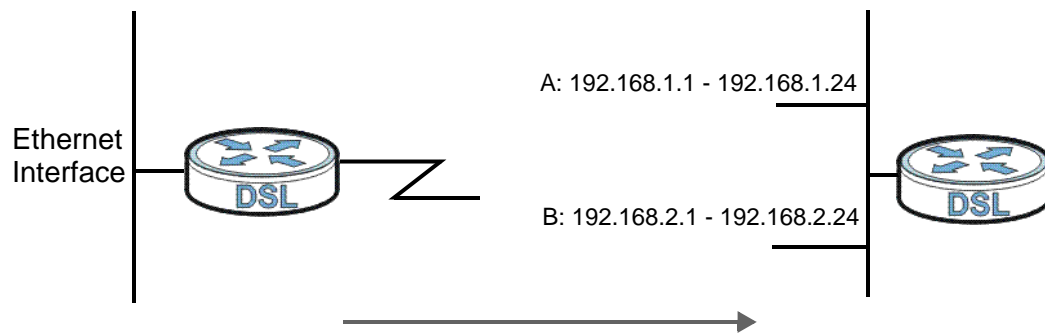
IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The ZyXEL Device supports three logical LAN interfaces via its single physical Ethernet interface with the ZyXEL Device itself as the gateway for each LAN network.

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

Note: Make sure that the subnets of the logical networks do not overlap.

The following figure shows a LAN divided into subnets A and B.

Figure 43 Physical Network & Partitioned Logical Networks



Wireless LAN

7.1 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.
- Using a MAC (Media Access Control) address filter to restrict access to the wireless network.

See [Chapter 2 on page 27](#) for a tutorial showing how to set up your wireless connection in an example scenario.

See [Section 7.10 on page 105](#) for advanced technical information on wireless networks.

7.1.1 What You Can Do in this Chapter

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

- The **General** screen lets you turn the wireless connection on or off, set up wireless security and make other basic configuration changes ([Section 7.4 on page 89](#)). You can also configure the MAC filter to allow or block access to the ZyXEL Device based on the MAC addresses of the wireless stations.
- The **More AP** screen lets you set up multiple wireless networks on your ZyXEL Device ([Section 7.5 on page 97](#)).
- Use the **WPS** screen and the **WPS Station** screen to use WiFi Protected Setup (WPS). WPS lets you set up a secure network quickly, when connecting to other WPS-enabled devices.

Use the **WPS** screen (see [Section 7.6 on page 98](#)) 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 7.7 on page 100](#)) screen to set up WPS by pressing a button or using a PIN.

- The **WDS** screen lets you set up a Wireless Distribution System, in which the ZyXEL Device acts as a bridge with other ZyXEL access points ([Section 7.8 on page 101](#)).
- The **Advanced Setup** screen lets you change the wireless mode, and make other advanced wireless configuration changes ([Section 7.9 on page 103](#)).

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

7.2 What You Need to Know

Wireless Basics

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

Wireless Network Construction

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.

Network Names

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.

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.

Wireless Security

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 s/he can either 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 perfectly 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.

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.

7.3 Before You Begin

Before you start using these screens, ask yourself the following questions. See [Section 7.2 on page 86](#) if some of the terms used here do not make sense to you.

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

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

- What advanced options do you want to configure, if any? If you want to configure advanced options, ensure that you know precisely what you want to do. If you do not want to configure advanced options, leave them alone.

7.4 The General Screen

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.

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

Figure 44 Network > Wireless LAN > General

The following table describes the labels in this screen.

Table 21 Network > Wireless LAN > General

LABEL	DESCRIPTION
Active Wireless LAN	Click the check box to activate wireless LAN.
Channel Selection	Set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box.
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.

Table 21 Network > Wireless LAN > General

LABEL	DESCRIPTION
Hide Network Name (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.
Disable WMM Advertise	WMM (Wi-Fi MultiMedia) QoS (Quality of Service) allows you to prioritize wireless traffic according to the delivery requirements of individual services. To do this, you must enable WMM QoS on all wireless devices in your network. Select this option to not broadcast the WMM information in beacon frames and disable WMM QoS on the ZyXEL Device.
BSSID	This shows the MAC address of the wireless interface on the ZyXEL Device when wireless LAN is enabled.
Security Mode	See the following sections for more details about this field.
MAC Filter	Click this button to go to the MAC Filter screen to configure whether the wireless devices with the MAC addresses listed are allowed or denied to access the ZyXEL Device using this SSID.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to reload the previous configuration for this screen.

7.4.1 No Security

Select **No Security** to allow wireless devices to communicate with the access points 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 45 Wireless LAN > General: No Security

The screenshot shows the 'General' tab of the 'Wireless LAN' configuration page. The 'Wireless Setup' section has 'Active Wireless LAN' checked and 'Channel Selection' set to 6. The 'Common Setup' section shows 'Network Name(SSID)' as 'ZyXEL', 'Hide Network Name(SSID)' unchecked, 'Disable WMM Advertise' unchecked, 'BSSID' as '00:23:F8:0C:89:65', 'Security Mode' set to 'No Security', and a 'MAC Filter' button labeled 'Edit'. At the bottom are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 22 Wireless LAN > General: No Security

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

7.4.2 WEP Encryption

In order to configure and enable WEP encryption; click **Network > Wireless LAN** to display the **General** screen. Select **WEP** from the **Security Mode** list.

Figure 46 Wireless LAN > General: Static WEP Encryption

General More AP WPS WPS Station WDS Advanced Setup

Wireless Setup

☒ Active Wireless LAN

Channel Selection 6

Common Setup

Network Name(SSID) ZyXEL

☐ Auto Generate Key

☐ Hide Network Name(SSID)

☐ Disable WMM Advertise

BSSID 00:23:F8:0C:89:65

Security Mode WEP

WEP Encryption 128-bit

Note:
 64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key (1-4).
 128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each Key (1-4).
 (Select one WEP key as an active key to encrypt wireless data transmission.)

☒ Key 1 1234567890123

☐ Key 2 1234567890123

☐ Key 3 1234567890123

☐ Key 4 1234567890123

MAC Filter Edit

Apply Reset

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

Table 23 Network > Wireless LAN > General: Static WEP Encryption

LABEL	DESCRIPTION
Auto Generate Key	Select this option to have the ZyXEL Device automatically generate an SSID and WEP key. The SSID , WEP Encryption and key fields will not be configurable when you select this option.
Security Mode	Choose WEP from the drop-down list box.
WEP Encryption	WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network. Select 64-bit WEP or 128-bit WEP to enable data encryption.
Key 1 to Key 4	The WEP key is used to secure your data from eavesdropping by unauthorized wireless users. Both the ZyXEL Device and the wireless stations must use the same WEP key for data transmission. Only one key can be activated at any one time. Select a default key to use for data encryption. If you chose 64-bit WEP in the WEP Encryption field, then enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. If you chose 128-bit WEP in the WEP Encryption field, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.

7.4.3 WPA(2)-PSK

In order to configure and enable WPA(2)-PSK authentication; click **Network > Wireless LAN** to display the **General** screen. Select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 47 Wireless LAN > General: WPA(2)-PSK

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

Table 24 Wireless LAN > General: WPA(2)-PSK

LABEL	DESCRIPTION
Auto Generate Key	This field is only available for WPA-PSK. Select this option to have the ZyXEL Device automatically generate an SSID and pre-shared key. The SSID and Pre-Shared Key fields will not be configurable when you select this option.
Security Mode	Choose WPA-PSK or WPA2-PSK from the drop-down list box.
Active Compatible	This field is only available for WPA2-PSK. Select this if you want the ZyXEL Device to support WPA-PSK and WPA2-PSK simultaneously.
Encryption	Select the encryption type (TKIP , AES or TKIP+AES) for data encryption.

Table 24 Wireless LAN > General: 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).
Group Key Update Timer	The Group Key Update Timer is the rate at which the AP (if using WPA(2)-PSK key management) or RADIUS server (if using WPA(2) 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. Setting of the Group Key Update Timer is also supported in WPA(2)-PSK mode. The ZyXEL Device default is 1800 seconds (30 minutes).

7.4.4 WPA(2) Authentication

Use this screen to configure and enable WPA or WPA2 authentication; click the **Wireless LAN** link under **Network** to display the **General** screen. Select **WPA** or **WPA2** from the **Security Mode** list.

Figure 48 Wireless LAN > General: WPA(2)

General More AP WPS WPS Station WDS Advanced Setup

Wireless Setup

☒ Active Wireless LAN

Channel Selection 6

Common Setup

Network Name(SSID) ZyXEL

☐ Hide Network Name(SSID)

☐ Disable WMM Advertise

BSSID 00:23:F8:0C:89:65

Security Mode WPA2

☐ Active Compatible WPA Compatible

Encryption TKIP

WPA2 Preauthentication Disabled

Network Re-auth Interval 36000 sec

Group Key Update Timer 1800 sec

Authentication Server

IP Address 0.0.0.0

Port Number 1812

Shared Secret

MAC Filter Edit

Apply Reset

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

Table 25 Wireless LAN > General: WPA(2)

LABEL	DESCRIPTION
Security Mode	Choose WPA or WPA2 from the drop-down list box.
Active Compatible	This field is only available for WPA2. Select this if you want the ZyXEL Device to support WPA and WPA2 simultaneously.
Encryption	Select the encryption type (TKIP , AES or TKIP+AES) for data encryption.
WPA2 Preauthentication	This field is available only when you select WPA2 . Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it. Select Enabled to turn on preauthentication in WPA2. Otherwise, select Disabled .
Network Re-auth Interval	This field is available only when you select WPA2 . Specify how often wireless clients have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 2147483647 seconds. Note: If wireless client authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Group Key Update Timer	The Group Key Update Timer is the rate at which the AP (if using WPA(2)-PSK key management) or RADIUS server (if using WPA(2) 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. Setting of the Group Key Update Timer is also supported in WPA(2)-PSK mode. The ZyXEL Device default is 1800 seconds (30 minutes).
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is 1812 . You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the ZyXEL Device. The key must be the same on the external authentication server and your ZyXEL Device. The key is not sent over the network.

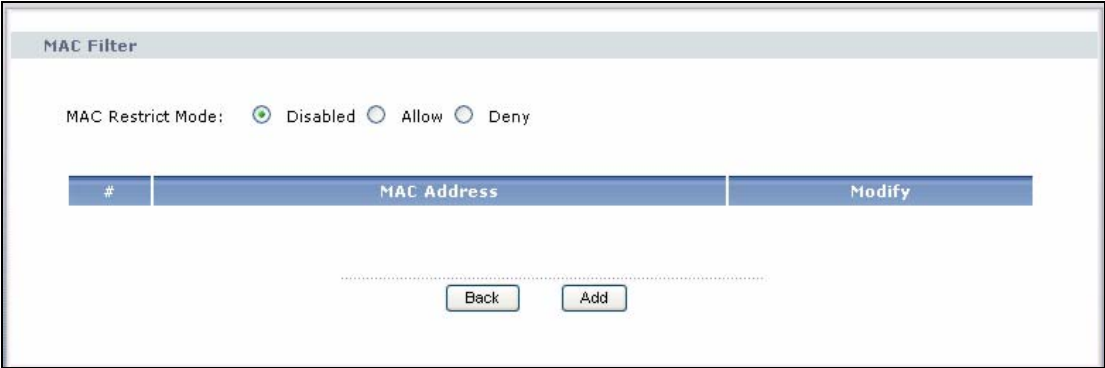
7.4.5 MAC Filter

This screen allows you to configure the ZyXEL Device to give exclusive access to specific devices (**Allow**) or exclude specific devices from accessing the ZyXEL

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

Use this screen to change your ZyXEL Device's MAC filter settings. Click the **Edit** button in the **Wireless LAN > General** screen. The following screen displays.

Figure 49 Wireless LAN > MAC Filter



The following table describes the labels in this screen.

Table 26 Wireless LAN > MAC Filter

LABEL	DESCRIPTION
MAC Restrict Mode	Define the filter action for the list of MAC addresses in the table below. Select Disabled to turn off MAC address filtering. Select Allow to permit access to the ZyXEL Device, MAC addresses not listed will be denied access to the ZyXEL Device. Select Deny to block access to the ZyXEL Device, MAC addresses not listed will be allowed to access the ZyXEL Device
#	This is the index number of the MAC address.
MAC Address	This is the MAC addresses of the wireless devices that are allowed or denied access to the ZyXEL Device.
Modify	Click the Remove icon to delete the entry.
Back	Click this to return to the previous screen without saving changes.
Add	Click this to create a new MAC filtering rule.

7.4.6 Adding a New MAC Filtering Rule

Click the **Add** button in the **MAC Filter** screen. The following screen displays.

Figure 50 Wireless LAN > MAC Filter > Add

The following table describes the labels in this screen.

Table 27 Wireless LAN > MAC Filter > Add

LABEL	DESCRIPTION
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 changes.
Apply	Click this to save your changes and go back to the previous screen.

7.5 The More AP Screen

This screen allows you to enable and configure multiple wireless networks on the ZyXEL Device.

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

Figure 51 Network > Wireless LAN > More AP

#	Active	SSID	Security	Modify
1	<input checked="" type="checkbox"/>	wl0_Guest1	No Security	
2	<input type="checkbox"/>	wl0_Guest2	No Security	
3	<input type="checkbox"/>	wl0_Guest3	No Security	

The following table describes the labels in this screen.

Table 28 Network > Wireless LAN > More AP

LABEL	DESCRIPTION
#	This is the index number of each SSID profile.
Active	Select the check box to activate an SSID profile.
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.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Reset	Click Reset to reload the previous configuration for this screen.

7.5.1 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 52 Network > Wireless LAN > More AP: Edit

The screenshot shows the 'Common Setup' configuration page for a wireless LAN. It includes the following elements:

- Active:** A checked checkbox.
- Network Name(SSID):** A text field containing 'wl0_Guest1'.
- Hide Network Name(SSID):** An unchecked checkbox.
- Disable WMM Advertise:** An unchecked checkbox.
- BSSID:** A text field displaying the MAC address '72:23:F8:0C:89:66'.
- Security Mode:** A dropdown menu currently set to 'No Security'.
- MAC Filter:** A button labeled 'Edit'.
- Navigation:** At the bottom, there are three buttons: 'Back', 'Apply', and 'Reset'.

See [Section 7.4 on page 89](#) for more details about the fields in this screen.

7.6 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 53 Network > Wireless LAN > WPS

The screenshot shows the 'WPS Setup' and 'WPS Status' configuration interface. The 'WPS Setup' section has a tabbed interface with 'WPS' selected. It includes a checked 'Enable WPS' checkbox, a 'PIN Number' field containing '40757841' with a 'Generate' button next to it. Below this is a 'Note' section with two points: '1. This feature is available only when WPA-PSK, WPA2-PSK or No Security mode is configured.' and '2. The "Auto Generate Key" would deactivate when "Unconfigured" status.' The 'WPS Status' section displays 'WPS Status: Configured' with a 'Release_Configuration' button, '802.11 Mode: 802.11bg', 'SSID: ZyXEL', and 'Security: No Security'. An 'Apply' button is located at the bottom of the status section.

The following table describes the labels in this screen.

Table 29 Network > Wireless LAN > WPS

LABEL	DESCRIPTION
WPS Setup	
Enable WPS	Select the check box to activate WPS on the ZyXEL Device.
PIN Number	This shows the PIN (Personal Identification Number) of the ZyXEL Device. Enter this PIN in the configuration utility of the device you want to connect to using WPS. The PIN is not necessary when you use WPS push-button method.
Generate	Click this button to have the ZyXEL Device create a new PIN.
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_Configuration to remove the configured wireless and wireless security settings.

Table 29 Network > Wireless LAN > WPS

LABEL	DESCRIPTION
Release_Configuration	This button is available when the WPS status is Configured but not configurable if you disable WPS. Click this button to remove all configured wireless and wireless security settings for WPS connections on the ZyXEL Device.
Apply	Click Apply to save your changes back to the ZyXEL Device.

7.7 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 54 Network > Wireless LAN > WPS Station

The screenshot shows the 'WPS Station' configuration screen. At the top, there are tabs: 'General', 'More AP', 'WPS', 'WPS Station' (selected), 'WDS', and 'Advanced Setup'. Below the tabs is a section titled 'Add Station by WPS'. It contains the instruction: 'Click the below Push Button to add WPS stations to wireless network.' There is a 'Push-Button' button. Below that, it says 'Or input station's PIN number:' followed by a text input field and a 'Start' button. A 'Note' section follows, with a yellow notepad icon. The note contains three points: 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. This feature is available only when WPA-PSK, WPA2 PSK or No Security mode is configured.

The following table describes the labels in this screen.

Table 30 Network > Wireless LAN > WPS Station

LABEL	DESCRIPTION
Push Button	<p>Click this button 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>

7.8 The WDS Screen

A Wireless Distribution System (WDS) is a wireless connection between two or more APs. Use this screen to set up your WDS links between the ZyXEL Devices. You need to know the MAC address of the peer device. Once the security settings of peer sides match one another, the connection between the devices is made.

Note: You can use WDS only when wireless security is set to “No Security” or “WEP”. The wireless security settings apply to both WDS links and the connections between the ZyXEL Device and any wireless clients.

Note: At the time of writing, WDS is only compatible with other ZyXEL Devices of the same model.

Click **Network > Wireless LAN > WDS**. The following screen displays. WDS is turned on and this screen is configurable when the ZyXEL Device's wireless security mode is **No Security** or **WEP**.

Figure 55 Network > Wireless LAN > WDS

WDS

Operating Mode: Access Point + Bridge

Bridge Restrict: Enabled(Scan)

Remote Bridges MAC Address:

	SSID	BSSID
<input type="checkbox"/>	ZyXEL	00:19:CB:0A:E0:7A
<input type="checkbox"/>	ZyXEL	00:19:CB:0A:E0:88
<input type="checkbox"/>	ZyXEL	00:13:49:18:90:1A
<input type="checkbox"/>	ZyXEL	00:19:CB:00:00:02

Note :

1. The WDS function only works on the No Security and WEP security mode.
2. The WDS function only works on the basic SSID.

Refresh Apply

The following table describes the labels in this screen.

Table 31 Network > Wireless LAN > WDS

LABEL	DESCRIPTION
WDS	
Operating Mode	<p>Select the operating mode for your ZyXEL Device.</p> <ul style="list-style-type: none"> • Access Point + Bridge - The ZyXEL Device functions as a bridge and access point simultaneously. • Wireless Bridge - The ZyXEL Device acts as a wireless network bridge and establishes wireless links with other APs. In this mode, clients cannot connect to the ZyXEL Device wirelessly. <p>You need to know the MAC address of the peer device, which must be of the same model and also WDS-enabled. The ZyXEL Device can establish up to four wireless links with other APs.</p>
Bridge Restrict	<p>This field is available only when you set operating mode to Access Point + Bridge.</p> <p>Select Enabled to turn on WDS and enter the peer device's MAC address manually in the table below.</p> <p>Select Enabled(Scan) to turn on WDS, search and display the available APs within range in the table below.</p>
Remote Bridges MAC Address	<p>Enter the MAC address of the peer device that your ZyXEL Device wants to make a bridge connection with.</p> <p>You can connect to up to 4 peer devices.</p>

Table 31 Network > Wireless LAN > WDS

LABEL	DESCRIPTION
	This is available only when you select Enabled(Scan) in the Bridge Restrict field. Select the check box and click Apply to have the ZyXEL Device establish a wireless link with the selected wireless device.
SSID	This is available only when you select Enabled(Scan) in the Bridge Restrict field. This shows the SSID of the available wireless device within range.
BSSID	This is available only when you select Enabled(Scan) in the Bridge Restrict field. This shows the MAC address of the available wireless device within range.
Refresh	Click Refresh to update the Remote Bridges MAC Address table when Bridge Restrict is set to Enabled(Scan) .
Apply	Click Apply to save your changes to ZyXEL Device.

7.9 The Advanced Setup Screen

To configure advanced wireless settings, click **Network > Wireless LAN > Advanced Setup**. The screen appears as shown.

Figure 56 Wireless LAN > Advanced Setup

The screenshot displays the 'Advanced Setup' tab for Wireless LAN configuration. The interface includes a navigation bar at the top with tabs for General, More AP, WPS, WPS Station, WDS, and Advanced Setup. Below the navigation bar, the 'Wireless Advanced Setup' section contains the following settings:

- RTS/CTS Threshold: 2347
- Fragmentation Threshold: 2346
- Number of Wireless Stations Allowed: 16
- Output Power: 100%
- Multicast Rate: 18 Mbps
- 802.11 Mode: 802.11b/g Mixed
- 802.11 Protection: Auto
- Preamble: Long

At the bottom of the configuration area, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 32 Wireless LAN > Advanced Setup

LABEL	DESCRIPTION
RTS/CTS Threshold	Enter a value between 0 and 2432.
Fragmentation Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.
Number of Wireless Stations Allowed	Specify the maximum number (from 1 to 64) of the wireless stations that may connect to the ZyXEL Device.
Output Power	Set the output power of the ZyXEL Device. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs. Select one of the following 20% , 40% , 60% , 80% or 100% .
Multicast Rate	Select a data rate at which the ZyXEL Device transmits wireless multicast traffic. If you select a high rate, multicast traffic may occupy all the bandwidth and cause network congestion.
802.11 Mode	Select 802.11b/g Mixed to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. The ZyXEL Device adjusts the transmission rate automatically according to the wireless standard supported by the wireless devices. Select 802.11g Only to allow IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. IEEE 802.11b compliant WLAN devices can associate with the ZyXEL Device only when they use the short preamble type. Select 802.11b Only to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. In this mode, all wireless devices can only transmit at the data rates supported by IEEE 802.11b.
802.11 Protection	Enabling this feature can help prevent collisions in mixed-mode networks (networks with both IEEE 802.11b and IEEE 802.11g traffic). Select Auto to have the wireless devices transmit data after a RTS/CTS handshake. This helps improve IEEE 802.11g performance. Select Off to disable 54g protection. The transmission rate of your ZyXEL Device might be reduced in a mixed-mode network. This field displays Off and is not configurable when you set 802.11 Mode to 802.11b Only .
Preamble	Select a preamble type from the drop-down list menu. Choices are Long or Short . The default setting is Long . See the appendix for more information. This field is not configurable and the ZyXEL Device uses Short when you set 802.11 Mode to 802.11g Only .
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to reload the previous configuration for this screen.

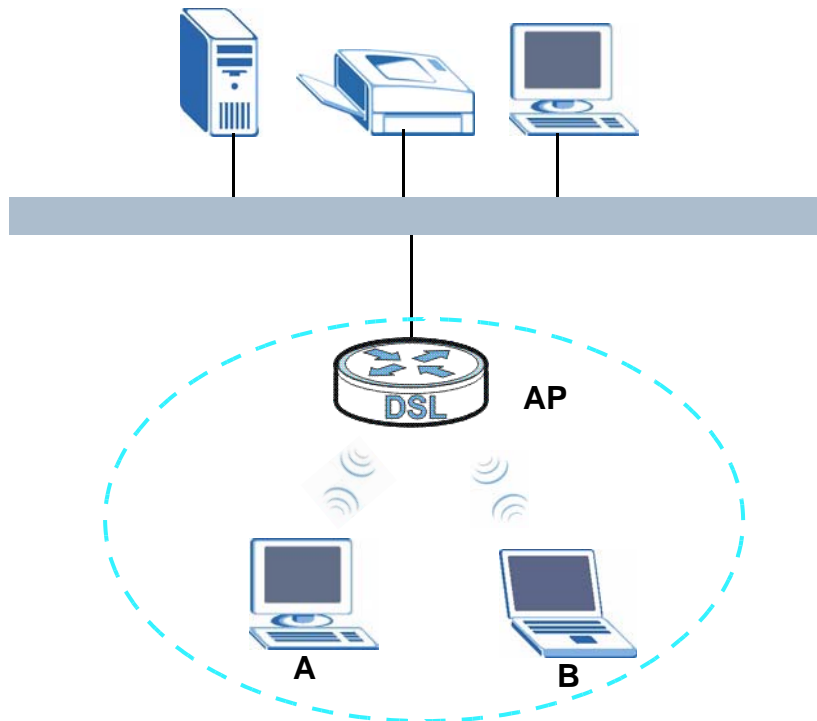
7.10 Technical Reference

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

7.10.1 Wireless Network Overview

The following figure provides an example of a wireless network.

Figure 57 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 IDentity.
- 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.

7.10.2 Additional Wireless Terms

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

Table 33 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	<p>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.</p>
Authentication	<p>The process of verifying whether a wireless device is allowed to use the wireless network.</p>
Fragmentation Threshold	<p>A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.</p>

7.10.3 Wireless Security Overview

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

7.10.3.1 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.

7.10.3.2 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.

7.10.3.3 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 they can use 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.

7.10.3.4 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 7.10.3.3 on page 107](#) for information about this.)

Table 34 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. 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.

7.10.4 WiFi Protected Setup

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.

7.10.4.1 Push Button Configuration

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

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

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

- 1 Ensure that the two devices you want to set up are within wireless range of one another.
- 2 Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the ZyXEL Device, see [Section 7.7 on page 100](#)).
- 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.

7.10.4.2 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 7.6 on page 98](#)).
- 4 Enter the client's PIN in the AP's configuration interface.

Note: 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.

- 5 Start WPS on both devices within two minutes.

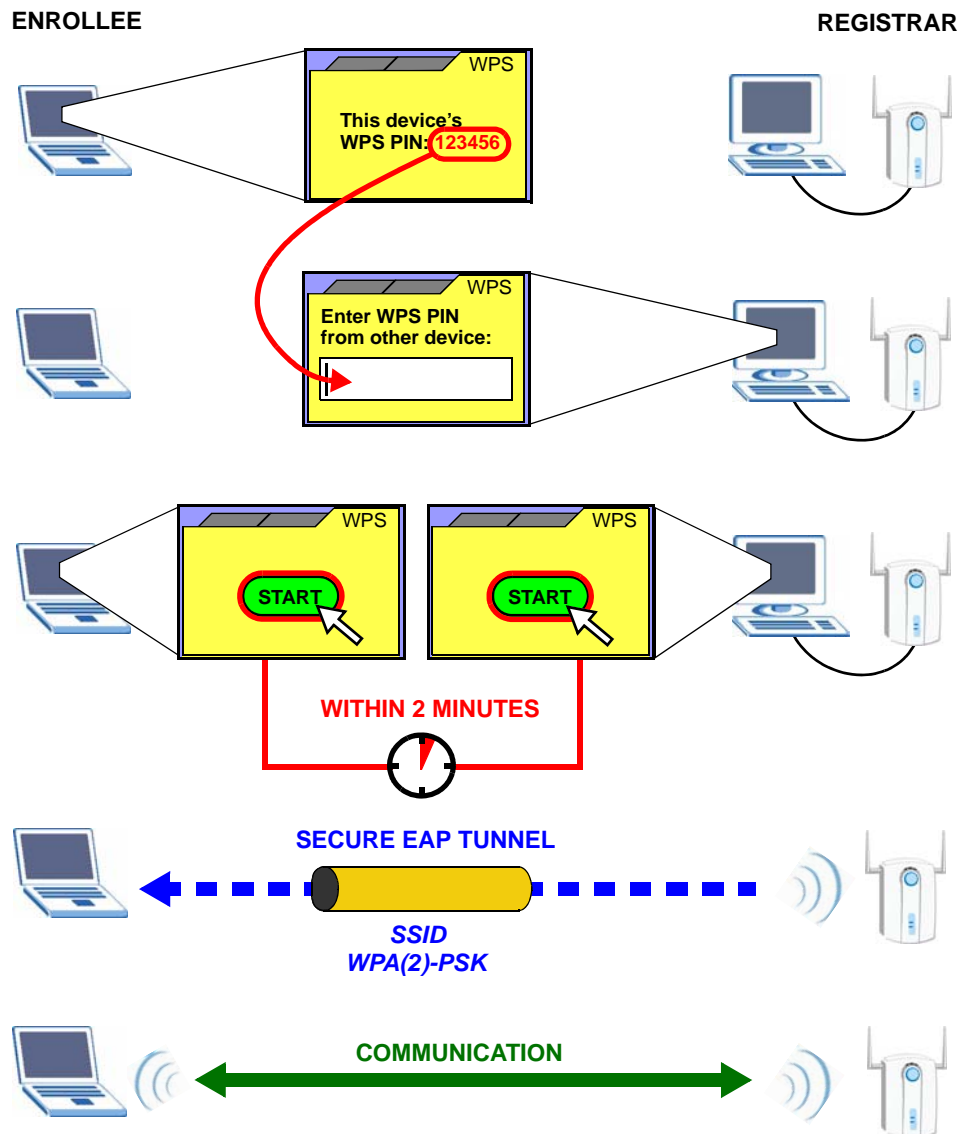
Note: Use the configuration utility to activate WPS, not the push-button on the device itself.

- 6 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 58 Example WPS Process: PIN Method

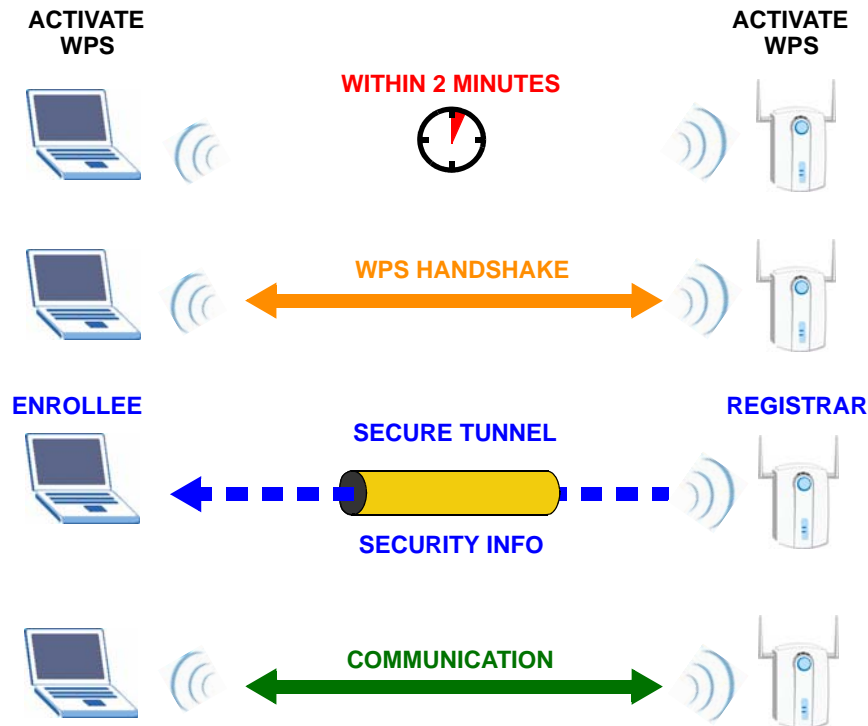


7.10.4.3 How WPS Works

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 59 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.

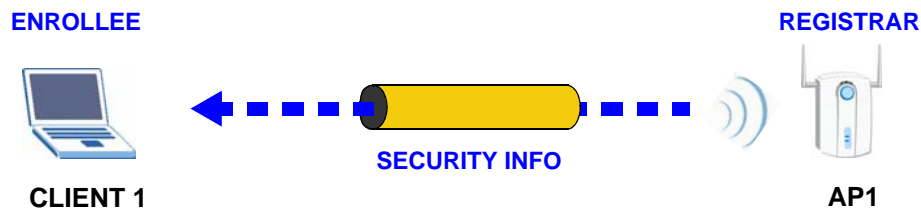
By default, a WPS device is "unconfigured". This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled 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.

7.10.4.4 Example WPS Network Setup

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

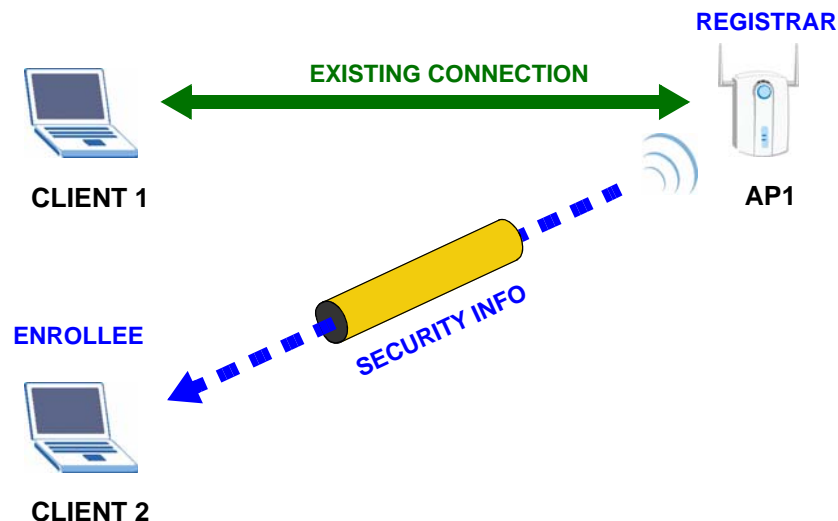
The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information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

Figure 60 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**.

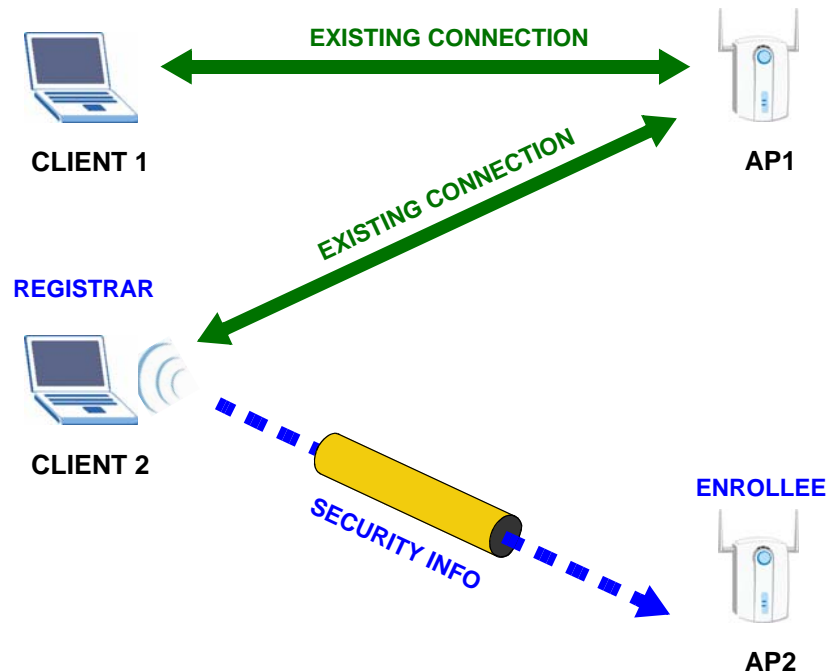
Figure 61 WPS: Example Network Step 2



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 62 WPS: Example Network Step 3



7.10.4.5 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)

8.1 Overview

This chapter discusses how to configure NAT on the ZyXEL Device.

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

8.1.1 What You Can Do in this Chapter

- The **Port Forwarding** screen lets you configure forward incoming service requests to the server(s) on your local network ([Section 8.3 on page 118](#)).
- The **Address Mapping** screen lets you configure the ZyXEL Device's address mapping settings ([Section 8.4 on page 121](#)).
- The **Trigger Port** screen lets you change the ZyXEL Device's trigger port settings ([Section 8.5 on page 124](#)).
- The **DMZ Host** screen lets you configure a default server ([Section 8.6 on page 128](#)).
- The **ALG** screen lets you enable SIP ALG on the ZyXEL Device ([Section 8.7 on page 128](#)).

8.2 What You Need to Know

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

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.

8.3 The Port Forwarding Screen

This summary screen provides a summary of all port forwarding rules and their configuration. In addition, this screen allows you to create new port forwarding rules and delete existing rules.

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.

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.

To access this screen, click **Network > NAT**. The following screen appears.

Figure 63 NAT Port Forwarding

The screenshot shows the 'Port Forwarding' configuration screen. At the top, there are tabs: 'Port Forwarding' (selected), 'Address Mapping', 'Trigger Port', 'DMZ Host', and 'ALG'. Below the tabs is a section titled 'Port Forwarding'. It contains a form to add new rules and a table of existing rules.

Add Rule Form:

- Service Name: WWW (dropdown)
- WAN Interface: ipoe_0_0_1_1/ptm0_1 (dropdown)
- WAN IP: (empty)
- Server IP Address: 192.168.1. (text)
- External port: Start: 80, End: 80
- Internal port: Start: 80, End: 80
- Protocol: TCP (dropdown)
- Buttons: Add, Cancel

Table of Existing Rules:

No.	Active	Service Name	WAN Interface	WAN IP	External Start Port	External End Port	Internal Start Port	Internal End Port	Server IP Address	Modify
1	<input checked="" type="checkbox"/>	FTP	ptm0_1		21	21	21	21	192.168.1.33	

At the bottom of the table are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 35 NAT Port Forwarding

LABEL	DESCRIPTION
Service Name	<p>Select a pre-defined service from the drop-down list box. The pre-defined service port number(s) and protocol will display in the External port, Internal port and Protocol fields.</p> <p>Otherwise, select User Define to open the Rule Setup screen where you can manually enter the port number(s) and select the IP protocol.</p>
WAN Interface	Select the WAN interface through which the service is forwarded.
WAN IP	<p>Enter the WAN IP address for which the incoming service is destined. If the packet's destination IP address doesn't match the one specified here, the port forwarding rule will not be applied.</p> <p>This field is optional.</p>
Server IP Address	Enter the IP address of the server for the specified service.
External Port Start	<p>Enter the original destination port for the packets.</p> <p>To forward only one port, enter the port number again in the External Port End field.</p> <p>To forward a series of ports, enter the start port number here and the end port number in the External Port End field.</p>
External Port End	<p>Enter the last port of the original destination port range.</p> <p>To forward only one port, enter the port number in the External Port Start field above and then enter it again in this field.</p> <p>To forward a series of ports, enter the last port number in a series that begins with the port number in the External Port Start field above.</p>
Internal Port Start	<p>Enter the port number to which you want the ZyXEL Device to translate the incoming port.</p> <p>To forward only one port, enter the port number again in the Internal Port End field.</p> <p>For a range of ports, enter the first number of the range to which you want the incoming ports translated.</p>
Internal Port End	Enter the last port of the translated port range.
Protocol	This is the IP protocol.
Add	Click this button to add a rule to the table below.
No.	This is the rule index number (read-only).
Active	<p>This field indicates whether the rule is active or not.</p> <p>Clear the check box to disable the rule. Select the check box to enable it.</p>
Server Name	This field displays the name of the service used by the packets for this virtual server.
WAN Interface	This field displays the WAN interface through which the service is forwarded.
WAN IP	This field displays the incoming packet's destination IP address.

Table 35 NAT Port Forwarding (continued)

LABEL	DESCRIPTION
External Start Port	This is the first external port number that identifies a service.
External End Port	This is the last external port number that identifies a service.
Internal Start Port	This is the first internal port number that identifies a service.
Internal End Port	This is the last internal port number that identifies a service.
Server IP Address	This field displays the inside IP address of the server.
Modify	Click the Edit icon to go to the screen where you can edit the port forwarding rule. Click the Remove icon to delete an existing port forwarding rule. Note that subsequent rules move up by one when you take this action.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to return to the previous configuration.

8.3.1 The Port Forwarding Edit Screen

This screen lets you create or edit a port forwarding rule. Select **User Define** in the **Service Name** field or click the rule's **Edit** icon in the **Port Forwarding** screen to open the following screen.

Figure 64 Port Forwarding Edit

The screenshot shows the 'Rule Setup' form for editing a port forwarding rule. The form includes the following fields and controls:

- Active:** A checked checkbox.
- Service Name:** An empty text input field.
- WAN Interface:** A dropdown menu with 'ipoe_0_0_1_1/ptm0_1' selected.
- External Start Port:** An empty text input field.
- External End Port:** An empty text input field.
- Internal Start Port:** An empty text input field.
- Internal End Port:** An empty text input field.
- WAN IP Address:** An empty text input field with '(Optional)' text to its right.
- Server IP Address:** A text input field containing '192.168.1.'.
- Protocol:** A dropdown menu with 'TCP' selected.

At the bottom of the form are three buttons: 'Back', 'Apply', and 'Cancel'.

The following table describes the labels in this screen.

Table 36 Port Forwarding Edit

LABEL	DESCRIPTION
Active	Clear the check box to disable the rule. Select the check box to enable it.
Service Name	Enter a name to identify this rule. This field is read-only if you click the Edit icon in the Port Forwarding screen.
WAN Interface	Select a WAN interface for which you want to configure port forwarding rules.
External Start Port	Enter the original destination port for the packets. To forward only one port, enter the port number again in the External End Port field. To forward a series of ports, enter the start port number here and the end port number in the External End Port field.
External End Port	Enter the last port of the original destination port range. To forward only one port, enter the port number in the External Start Port field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the External Start Port field above.
Internal Start Port	Enter the port number here to which you want the ZyXEL Device to translate the incoming port. For a range of ports, enter the first number of the range to which you want the incoming ports translated.
Internal End Port	Enter the last port of the translated port range.
WAN IP Address	Enter the incoming packet's destination IP address. This field is optional.
Server IP Address	Enter the inside IP address of the virtual server here.
Protocol	Select the protocol supported by this virtual server. Choices are TCP , UDP , or TCP/UDP .
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

8.4 The Address Mapping Screen

Ordering your rules is important because the ZyXEL Device applies the rules in the order that you specify. When a rule matches the current packet, the ZyXEL Device takes the corresponding action and the remaining rules are ignored.

To change your ZyXEL Device's address mapping settings, click **Network > NAT > Address Mapping** to open the following screen.

Figure 65 Network > NAT > Address Mapping

Set	Local Start IP	Local End IP	Global Start IP	Global End IP	Type	Modify
1	192.168.1.23		10.1.2.3		One-to-One	

The following table describes the fields in this screen.

Table 37 Network > NAT > Address Mapping

LABEL	DESCRIPTION
Set	This is the index number of the address mapping set.
Local Start IP	This is the starting Inside Local IP Address (ILA).
Local End IP	This is the end Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is blank for One-to-one mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for the Many-to-One mapping type.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is blank for One-to-one and Many-to-One mapping types.
Type	<p>This is the address mapping type.</p> <p>One-to-One: This mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type.</p> <p>Many-to-One: This mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only.</p> <p>Many-to-Many: This mode maps multiple local IP addresses to shared global IP addresses.</p>
Modify	<p>Click the Edit icon to go to the screen where you can edit the address mapping rule.</p> <p>Click the Remove icon to delete an existing address mapping rule. Note that subsequent address mapping rules move up by one when you take this action.</p>

8.4.1 The Address Mapping Rule Edit Screen

To edit an address mapping rule, click the rule's edit icon in the **Address Mapping** screen to display the screen shown next.

Figure 66 Network > NAT > Address Mapping: Edit

The following table describes the fields in this screen.

Table 38 Network > NAT > Address Mapping: Edit

LABEL	DESCRIPTION
Type	<p>Choose the IP/port mapping type from one of the following.</p> <p>One-to-One: This mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type.</p> <p>Many-to-One: This mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only.</p> <p>Many-to-Many: This mode maps multiple local IP addresses to shared global IP addresses.</p>
Local Start IP	This is the starting local IP address (ILA).
Local End IP	<p>This is the end local IP address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address.</p> <p>This field is not configurable for the One-to-One mapping type.</p>
Global Start IP	This is the starting global IP address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending global IP address (IGA). This field is not configurable for One-to-One and Many-to-One mapping types.
Mapping Set	Select the number of the mapping set for which you want to configure.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

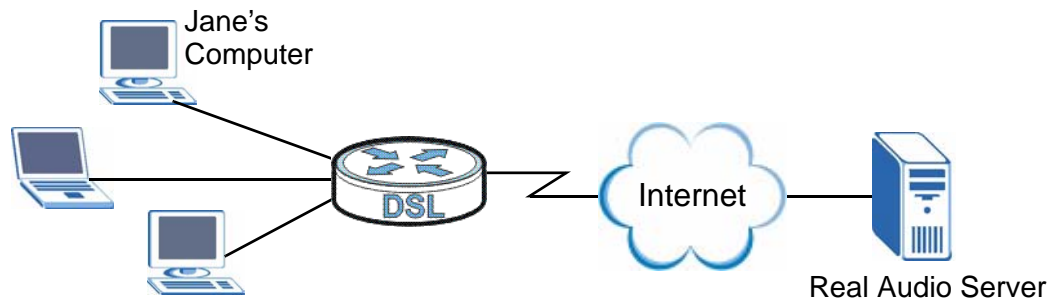
8.5 The Trigger Port Screen

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

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

For example:

Figure 67 Trigger Port Forwarding Process: Example



- 1 Jane requests a file from the Real Audio server (port 7070).
- 2 Port 7070 is a "trigger" port and causes the ZyXEL Device to record Jane's computer IP address. The ZyXEL Device associates Jane's computer IP address with the "open" port range of 6970-7170.
- 3 The Real Audio server responds using a port number ranging between 6970-7170.
- 4 The ZyXEL Device forwards the traffic to Jane's computer IP address.

- 5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The ZyXEL Device times out in three minutes with UDP (User Datagram Protocol) or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

Click **NAT > Trigger Port** to open the following screen. Use this screen to view and configure your ZyXEL Device's trigger port settings.

Figure 68 Trigger Port

The following table describes the labels in this screen.

Table 39 NAT Trigger Port

LABEL	DESCRIPTION
Service Name	Select a pre-defined service from the drop-down list box. The pre-defined service port number(s) and protocol will display in the Trigger port , Open port and Protocol fields. Otherwise, select User Define to open the Rule Setup screen where you can manually enter the port number(s) and select the IP protocol.
WAN Interface	Select the WAN interface through which the service is forwarded.
Trigger Port	The trigger port is a port (or a range of ports) that causes (or triggers) the ZyXEL Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start	This is the first port number that identifies a service.
End	This is the last port number that identifies a service.
Protocol	This is the IP protocol.
Open Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ZyXEL Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start	This is the first port number that identifies a service.
End	This is the last port number that identifies a service.
Protocol	This is the IP protocol.
Add	Click this button to add a rule to the table below.
No.	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.

Table 39 NAT Trigger Port (continued)

LABEL	DESCRIPTION
Server Name	This field displays the name of the service used by the packets for this virtual server.
WAN Interface	This field displays the WAN interface through which the service is forwarded.
Trigger Start Port	This is the first trigger port number that identifies a service.
Trigger End Port	This is the last trigger port number that identifies a service.
Trigger Proto.	This is the trigger IP protocol. 1 means TCP, 2 means UDP and 3 means TCP/UDP.
Open Start Port	This is the first open port number that identifies a service.
Open End Port	This is the last open port number that identifies a service.
Open Proto.	This is the open IP protocol. 1 means TCP, 2 means UDP and 3 means TCP/UDP.
Modify	Click the Edit icon to go to the screen where you can edit the rule. Click the Remove icon to delete an existing rule. Note that subsequent rules move up by one when you take this action.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to return to the previous configuration.

8.5.1 Trigger Port Configuration

This screen lets you create new port triggering rules. Click the **Add** icon in the **NAT - Trigger Port** screen to open the following screen.

Figure 69 NAT > Trigger Port > Add

Rule Setup

☒ Active

Service Name

WAN Interface

Trigger Start Port

Trigger End Port

Trigger Protocol

Open Start Port

Open End Port

Open Protocol

The following table describes the labels in this screen.

Table 40 NAT > Port Triggering > Add

LABEL	DESCRIPTION
Active	Clear the check box to disable the rule. Select the check box to enable it.
Service Name	Enter a name to identify this rule. This field is read-only if you click the Edit icon in the Trigger Port screen.
WAN Interface	Select a WAN interface for which you want to configure port triggering rules.
Trigger Start Port	The trigger port is a port (or a range of ports) that causes (or triggers) the ZyXEL Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN. Type a port number or the starting port number in a range of port numbers.
Trigger End Port	Type a port number or the ending port number in a range of port numbers.
Trigger Protocol	Select the IP protocol from TCP , UDP , or TCP/UDP .
Open Start Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ZyXEL Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. Type a port number or the starting port number in a range of port numbers.
Open End Port	Type a port number or the ending port number in a range of port numbers.
Open Protocol	Select the IP protocol from TCP , UDP , or TCP/UDP .
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

8.6 The DMZ Host Screen

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 the **NAT Port Forwarding Setup** screen.

Figure 70 NAT > DMZ Host

The following table describes the fields in this screen.

Table 41 NAT > DMZ Host

LABEL	DESCRIPTION
Default Server	Enter the IP address of the default server which receives packets from ports that are not specified in the NAT Port Forwarding screen. Note: If you do not assign a Default Server , the ZyXEL Device discards all packets received for ports that are not specified in the NAT Port Forwarding screen.
Apply	Click Apply to save your changes back to the ZyXEL Device.

8.7 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. 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 you enable the SIP ALG.

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

Figure 71 NAT > ALG

Each field is described in the following table.

Table 42 NAT > ALG

LABEL	DESCRIPTION
Active SIP ALG	Select this check box to allow SIP sessions to pass through the ZyXEL Device. SIP is a signaling protocol used in VoIP (Voice over IP), the sending of voice signals over Internet Protocol.
Apply	Click Apply to save your customized settings.

8.8 Technical Reference

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

Port Forwarding: Services and Port Numbers

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Please also refer to the Supporting CD for more examples and details on port forwarding and NAT.

Table 43 Services and Port Numbers

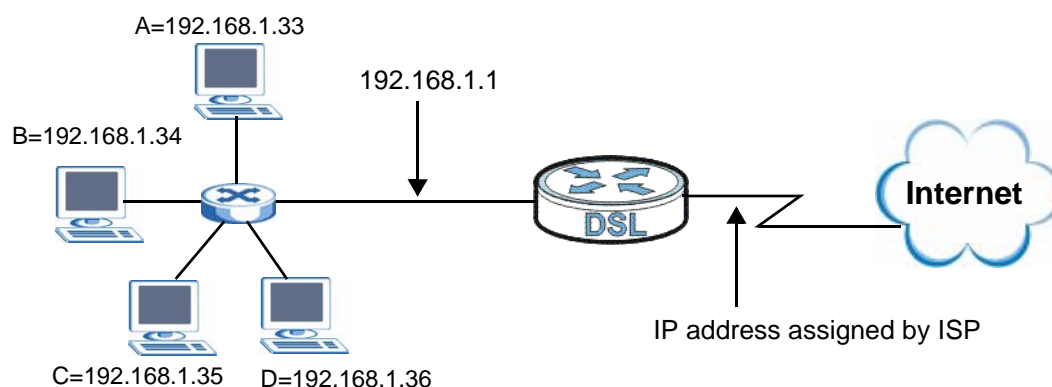
SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161

Table 43 Services and Port Numbers

SERVICES	PORT NUMBER
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

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 72 Multiple Servers Behind NAT Example

MAC Filter

This chapter discusses MAC address filtering.

9.1 Overview

MAC filtering means sifting traffic going through the ZyXEL Device based on the source and/or destination MAC addresses.

9.1.1 What You Can Do in this Chapter

The **MAC Filter** screen lets you view and configure the MAC filtering rules ([Section 9.2 on page 131](#)).

9.2 The MAC Filter Screen

Click **MAC Filtering** or **Security > MAC Filter** to display the following screen. This screen displays the default global MAC filtering policy and a list of the custom

MAC filtering rules. The MAC filtering rules apply only to frames going through a bridge connection.

Figure 73 MAC Filter

MAC Filter

MAC Filtering Setup

MAC Filtering is only effective in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

MAC Filtering Policy For Each Interface:
WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Interface	Policy	Change
ptm0_2	FORWARDED	<input type="checkbox"/>

Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
ptm0_2	AppleTalk		00:c5:01:e8:23:79	BOTH	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 44 MAC Filter

LABEL	DESCRIPTION
MAC Filtering Policy For Each Interface	
Interface	This displays the interface to which this rule is applied.
Policy	This displays the MAC filtering policy for each WAN interface in bridge mode on the ZyXEL Device. By default, the ZyXEL Device allows all frames to pass through the bridge connection.
Change	Select the check box next to the interface for which you want to change the MAC filtering policy.
Change Policy	Select the Change check box and click Change Policy to have the ZyXEL Device change to block or allow all frames on this interface.
Interface	This displays the interface to which this rule is applied.
Protocol	This displays the service to which this rule applies.
Destination MAC	This displays the destination MAC address to which this rule applies. Please note that a blank destination address is equivalent to Any .
Source MAC	This displays the source MAC address to which this rule applies. Please note that a blank source address is equivalent to Any .
Frame Direction	This displays the direction of travel of frame to which this rule applies.
Remove	Select the rule(s) you want to delete in the Remove column and then click the Remove button.

Table 44 MAC Filter (continued)

LABEL	DESCRIPTION
Add	Click Add to create a new rule.
Remove	Click Remove to delete the selected rule(s).

9.2.1 Creating MAC Filtering Rules

In the **MAC Filter** screen, click **Add** to display this screen and refer to the following table for information on the labels.

Figure 74 MAC Filter: Add

The following table describes the labels in this screen.

Table 45 MAC Filtering: Add

LABEL	DESCRIPTION
Protocol Type	Select the service to which this rule applies.
Destination MAC Address	Enter a destination MAC address in valid MAC address format, that is, six hexadecimal character pairs to apply the filter rule to the specified MAC address. Please note that a blank destination address is equivalent to Any .
Source MAC Address	Enter a source MAC address in valid MAC address format, that is, six hexadecimal character pairs to apply the filter rule to the specified MAC address. Please note that a blank source address is equivalent to Any .
Frame Direction	Select the travel direction of frame to which this rule applies.
WAN Interfaces	Select the WAN interface to which this rule applies.
Save/Apply	Click Save/Apply to save your customized settings and exit this screen.

Firewall

10.1 Overview

This chapter shows you how to enable and configure the ZyXEL Device firewall settings.

The ZyXEL Device firewall is a packet filtering firewall and restricts access based on the source/destination computer network address of a packet and the type of application.

10.1.1 What You Can Do in this Chapter

The **Incoming** screen lets you view and configure incoming IP filtering rules ([Section 10.3 on page 136](#)).

10.2 What You Need to Know

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

Basics

Computers share information over the Internet using a common language called TCP/IP. TCP/IP, in turn, is a set of application protocols that perform specific functions. An "extension number", called the "TCP port" or "UDP port" identifies these protocols, such as HTTP (Web), FTP (File Transfer Protocol), POP3 (E-mail), etc. For example, Web traffic by default uses TCP port 80.

When computers communicate on the Internet, they are using the client/server model, where the server "listens" on a specific TCP/UDP port for information requests from remote client computers on the network. For example, a Web server typically listens on port 80. Please note that while a computer may be intended for use over a single port, such as Web on port 80, other ports are also active. If the person configuring or managing the computer is not careful, a hacker could attack it over an unprotected port.

Some of the most common IP ports are:

Table 46 Common IP Ports

21	FTP	53	DNS
23	Telnet	80	HTTP
25	SMTP	110	POP3

Default Filtering Policies

Filtering rules are grouped based on the direction of travel of packets to which they apply.

The default rule for incoming traffic blocks all incoming connections from the WAN to the LAN. If you wish to allow certain WAN users to have access to your LAN, you will need to create custom rules to allow it.

Note: If you configure filtering rules without a good understanding of how they work, you might inadvertently introduce security risks to the firewall and to the protected network. Make sure you test your rules after you configure them.

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

10.3 The Firewall Screen

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

Figure 75 Firewall > Incoming

Incoming

Incoming Firewall ACL rules Setup

When the Firewall ACL rule is enabled on a WAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming Firewall ACL rules.

☒ Active Firewall

Active	Filter Name	Interfaces	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Modify
<input type="checkbox"/>	example	ptm0_1,br0	TCP or UDP			192.168.1.99 / 255.255.255.0		

The following table describes the labels in this screen.

Table 47 Firewall > Incoming

LABEL	DESCRIPTION
Active Firewall	Select this check box to enable the firewall on the ZyXEL Device. When the firewall is enabled, the ZyXEL Device blocks all incoming traffic from the WAN to the LAN. Create customized rules below to allow certain WAN users to access your LAN or to allow traffic from the WAN to a certain computer on the LAN.
Active	Select this check box to enable the rule.
Filter Name	This displays the name of the rule.
Interfaces	This displays the WAN interface(s) to which this rule is applied.
Protocol	This displays the IP protocol that defines the service to which this rule applies.
Source Address / Mask	This displays the source IP addresses and subnet mask to which this rule applies. Please note that a blank source address is equivalent to Any .
Source Port	This is the source port number.
Dest. Address / Mask	This displays the destination IP addresses and subnet mask to which this rule applies. Please note that a blank destination address is equivalent to Any .
Dest. Port	This is the destination port number.
Modify	Click the Edit icon to go to the screen where you can edit the rule. Click the Remove icon to delete an existing rule. Note that subsequent rules move up by one when you take this action.
Add	Click Add to create a new rule.
Apply	Click Apply to save your changes back to the ZyXEL Device.

10.3.1 Creating Incoming Firewall Rules

In the **Incoming** screen, click **Add** to display this screen and refer to the following table for information on the labels.

Figure 76 Firewall > Incoming: Add

Add Firewall ACL rule -- Incoming

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

☐ Active

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

Interface: ☒ Select All ☒ ipoe_0_0_1_1/ptm0_1

The following table describes the labels in this screen.

Table 48 Firewall > Incoming: Add

LABEL	DESCRIPTION
Active	Select this check box to enable the rule.
Filter Name	Enter a descriptive name of up to 16 printable English keyboard characters, including spaces. To add a firewall rule, you need to configure at least one of the following fields (except the Interface field).
Protocol	Select the IP protocol (TCP/UDP , TCP , UDP or ICMP) and enter the protocol (service type) number in the port field. Select NONE to apply the rule to any protocol.
Source IP Address	Enter the source IP address in dotted decimal notation.
Source Subnet Mask	Enter the source subnet mask.
Source Port	Enter a single port number or the range of port numbers of the source.
Destination IP Address	Enter the destination IP address in dotted decimal notation.
Destination Subnet Mask	Enter the destination subnet mask.
Destination Port	Enter the port number of the destination.

Table 48 Firewall > Incoming: Add (continued)

LABEL	DESCRIPTION
Interface	Select Select All to apply the rule to all interfaces on the ZyXEL Device or select the specific WAN interface(s) to which this rule applies.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your customized settings and exit this screen.

Certificate

11.1 Overview

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

11.1.1 What You Can Do in this Chapter

- The **Local Certificates** screen lets you generate certification requests and import the ZyXEL Device's CA-signed certificates ([Section 11.4 on page 149](#)).
- The **Trusted CA** screen lets you save the certificates of trusted CAs to the ZyXEL Device ([Section 11.4 on page 149](#)).

11.2 What You Need to Know

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

Certification Authority

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates. You can use the ZyXEL Device to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

11.3 The Local Certificates Screen

Click **Security > Certificates** to open the **Local Certificates** screen. This is the ZyXEL Device's summary list of certificates and certification requests.

Figure 77 Local Certificates

The screenshot shows the 'Local Certificates' screen with a tabbed interface. The 'Local Certificates' tab is active, and the 'Trusted CA' tab is also visible. Below the tabs, there is a text block: 'Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity. Maximum 4 certificates can be stored.' Below this is a table with columns: Name, In Use, Subject, Type, and Action. The table contains three rows: 'cert' (request), 'test' (request), and 'localcert_test' (signed). Each row has buttons for 'View', 'Load Signed', and 'Remove'. At the bottom of the screen, there are two buttons: 'Create Certificate Request' and 'Import Certificate'.

Name	In Use	Subject	Type	Action
cert		CN=ZyXEL/O=TW/ST=NA/C=US	request	View Load Signed Remove
test		CN=example/O=BigCompany/ST=NoAva/C=US	request	View Load Signed Remove
localcert_test		CN=www.zyxel.com.tw/O=Zyxel/ST=TW/C=TW	signed	View Remove

Create Certificate Request Import Certificate

The following table describes the labels in this screen.

Table 49 Local Certificates

LABEL	DESCRIPTION
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
In Use	This field displays how many applications use the certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Type	<p>This field displays what kind of certificate this is.</p> <p>request represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the Load Certificate screen to import the certificate and replace the request.</p> <p>signed represents a certificate issued by a certification authority.</p>
Modify	<p>Click the View button to open a screen with an in-depth list of information about the certificate (or certification request).</p> <p>Click the Load Signed button to import a valid certification to replace the request.</p> <p>Click the Remove button to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.</p>

Table 49 Local Certificates (continued)

LABEL	DESCRIPTION
Create Certificate Request	Click this button to go to the screen where you can have the ZyXEL Device generate a certification request.
Import Certificate	Click this button to open a screen where you can save the certificate that you have enrolled from a certification authority from your computer to the ZyXEL Device.

11.3.1 Create Certificate Request

Click **Security > Certificates > Local Certificates** and then **Create Certificate Request** to open the **My Certificate Create** screen. Use this screen to have the ZyXEL Device generate a certification request.

Figure 78 Create Certificate Request

The following table describes the labels in this screen.

Table 50 Create Certificate Request

LABEL	DESCRIPTION
Certificate Name	Type up to 31 ASCII characters (not including spaces) to identify this certificate.
Common Name	Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 31 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Organization Name	Type up to 127 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
State/Province Name	Type up to 127 characters to identify the state or province where the certificate owner is located. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
Country/Region Name	Select a country to identify the nation where the certificate owner is located.

Table 50 Create Certificate Request (continued)

LABEL	DESCRIPTION
Back	Click Back to return to the previous screen.
Apply	Click Apply to begin certificate or certification request generation.

After you click **Apply**, the **Certificate Request Details** screen displays. Click **Load Signed Certificate** to import a certificate signed by the CA to replace the request (see [Section 11.3.4 on page 148](#)). Otherwise, click **Back** to return to the **Local Certificates** screen. See [Section 11.3.3 on page 146](#) for field information.

Figure 79 Certificate Request Details

Certificate Request Details

Certificate signing request successfully created. Note a request is not yet functional - have it signed by a Certificate Authority and load the signed certificate to this device.

Name	cert
Type	request
Subject	CN=ZyXEL/O=TW/ST=NA/C=US

Signing Request

```

-----BEGIN CERTIFICATE REQUEST-----
MIIBdjCB4AIBADA3MQ4wDAYDVQQDEWVaeVhFTDELMAkGA1UEChMCVFcxZzAJBgNV
BAgTAk5BMQswCQYDVQQGEwJVUzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwYkCgYEA
wtN4xn4nmvO+ZFvTrK2eWXHt7MIOJkqHWfK3QAcYMEATRsFBovk1xSFtShcqBhbX
IttP9RCEQW3S8frP91OZSaYmnybwwrxja2jUHvVHghdGqubo/f1Nkap877uUWYot
hOKxVi2zCLr4z4g6LLDzg2Tr2acyu9cytp04b1ER0mECawEAAAAMAOGCSqGSIb3
DQEBBAUAA4GBAEcLDVzLS1fhYMD1L57sUsJh1bxXkrSaOVzSIsjxRd6anlgKdqr2
pXbzYt9tcrBv5A7MHLoZKKSqOQzD8ZrYeSAZRHfxJqDvdbkt1WBnV40GQWAndm2t
Iley5AY/EMCZJ99dfVILc/8J5H/PoopxQju96ZvG8Lz7uM1hkVzLrc1t
-----END CERTIFICATE REQUEST-----

```

Back Load Signed Certificate

11.3.2 Import Certificate

Click **Security > Certificates > Local Certificates** and then **Import Certificate** to open the **Import Local Certificate** screen. Follow the instructions in this screen to save an existing certificate to the ZyXEL Device.

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

Figure 80 Import Local Certificate

Import Local Certificate

Enter certificate name, paste certificate content and private key

Certificate Name:

Certificate:

-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----

Private Key:

-----BEGIN RSA PRIVATE KEY-----
<insert private key here>
-----END RSA PRIVATE KEY-----

Back

Apply

The following table describes the labels in this screen.

Table 51 Import Local Certificate

LABEL	DESCRIPTION
Certificate Name	Type up to 31 ASCII characters (not including spaces) to identify this certificate.
Certificate	Copy and paste the certificate into the text box to store it on the ZyXEL Device.

Table 51 Import Local Certificate

LABEL	DESCRIPTION
Private Key	Copy and paste the private key into the text box to store it on the ZyXEL Device.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save the certificate on the ZyXEL Device.

11.3.3 Certificate Details

Click **Security > Certificates > Local Certificates** to open the **My Certificates** screen (see [Figure 77 on page 142](#)). Click the **View** icon to open the **Certificate Details** screen. Use this screen to view in-depth certificate information and change the certificate's name.

Figure 81 Certificate Details

Certificate Details	
Name	cert
Type	request
Subject	CN=ZyXEL/O=TW/ST=NA/C=US
Certificate	(null)
Private Key	<pre> -----BEGIN RSA PRIVATE KEY----- MIICXQIBAAKBgQDC03jGflea875kU9OsrZ5Zce3swg4mSodZ+TdABxgwQBNGwUGi +SXF IW1KFyoGFtc120/1EIRBbdIB+s/3U51JpiafJvDCvGNraNQe9UeqF0aq5uj9 +U2Rqnzvu5R2ii2HQRFWLbMIuvjPiDosePODZ0vZpzK71zK2k7hvURHSYQIDAQAB AoGAMZqCD5ejIdKZURgIJtjljRxrWwjC1DDoWbQaF7mC7LktYkS2xmwQiammsyX CIHcOKW6D90qrzX02EgxlvkT97i7BOjkNUhU51gvdO274m4g2G3w17exJkGgpYfy xqhnXfr4Z9czplc2QgtaKgWUv9WnbewXK3XonRiQAj7QkAECQQDfVJSN4tG1WVjp fF7tkI6uzHNG8dhYuWmkjEc5CJxIVJA4H18BdBnlrS4HxUTm8zp76G7/FvOZsA2O JBTjgaOhAkEA31NxbDUXpuptH11wuS5vqtQFoL5i1Z5n3ZODgMr127LhODJUznt Psd8CsddmQcLWeHDKGn5EsQQYSfPYmG2wQJAKWSw4BeBSgdkbnpJ4fhgKc/1MeoT cmZzSTdi4BRTeyiJTo1xovBU+Hf/xxruKWw9k8fCAu/LGNpDuOvBH2Xg4QJBAJ1w V2m1QM7qGneGV8Cj6w1QB13d8UIcR/ixN2TzONJqINvfmOOVvYXIV62g4z/7gif WNsX1I4UL7zRAWfzAwECQQCNoUEHAbhFZJtZAF6H93JQIsOMs7t5O1wenS617+dG dgjN/UfbjQCohniyOtcchpai3BW4DrMhcq51TzekHa1F -----END RSA PRIVATE KEY----- </pre>
Signing Request	<pre> -----BEGIN CERTIFICATE REQUEST----- MIIBdjCB4AIBADA3MQ4wDAYDVQQDEwVaeVhFTDELMAkGA1UEChMCVFcxZzA5BGNV BAGTAk5BMQswCQYDVQQGEwJVUzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwYkCgYEA wtN4xn4nmwO+ZfVTrK2eWXHt7MIOJkqHWfk3QAcYMEATrSFbovk1xSftShcqBhbX IttP9RCEQW3SAfrP91OZSaYmnybwwrxja2jUHvVHqhdGqubo/f1Nkap877uUWYot hOKxVi2zCLr4z4g6LLDzg2Tr2acyu9cytp04b1ER0mEC&wEAAA&AAOGCSqGSIb3 DQEBBAUAA4GBAEcLDVzLS1fhYMD1L57sUsJh1bxXkrSaOVzSIsjxRd6anlgKdqr2 pXbzYt9tcrBv5A7MHL0ZXXSgOQzD8ZrYeSAZRHfxJqDvdhkt1WBNV40GQWAndm2t I1ey5AY/EMCZJ99dfVILc/8J5H/PooppQju96ZvG8Lz7uM1hkVzLrc1t -----END CERTIFICATE REQUEST----- </pre>

The following table describes the labels in this screen.

Table 52 Certificate Details

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this certificate. You may use any character (not including spaces).
Type	This field displays general information about the certificate. signed means that a Certification Authority signed the certificate. request means this is a certification request.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organization (O), State (ST) and Country (C).
Certificate	<p>This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form.</p> <p>This displays null in a certification request.</p> <p>You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).</p>
Private Key	<p>This read-only text box displays the private key in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form.</p> <p>You can copy and paste the private key into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).</p>
Signing Request	<p>This read-only text box displays the request information in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form.</p> <p>This displays null in a signed certificate.</p>
Back	Click Back to return to the previous screen.
Load Signed Certificate	<p>This button is available only in a certification request details screen</p> <p>Click this to import a certificate signed by the CA to replace the request.</p>

11.3.4 Load Signed Certificate

Click **Security > Certificates > Local Certificates** and then **Load Signed** or the **Load Signed Certificate** button in the **Certificate Details** screen of a certification request to open the **Load Certificate** screen. Follow the instructions in this screen to save a valid certificate to replace the request.

Figure 82 Load Certificate

The following table describes the labels in this screen.

Table 53 Load Certificate

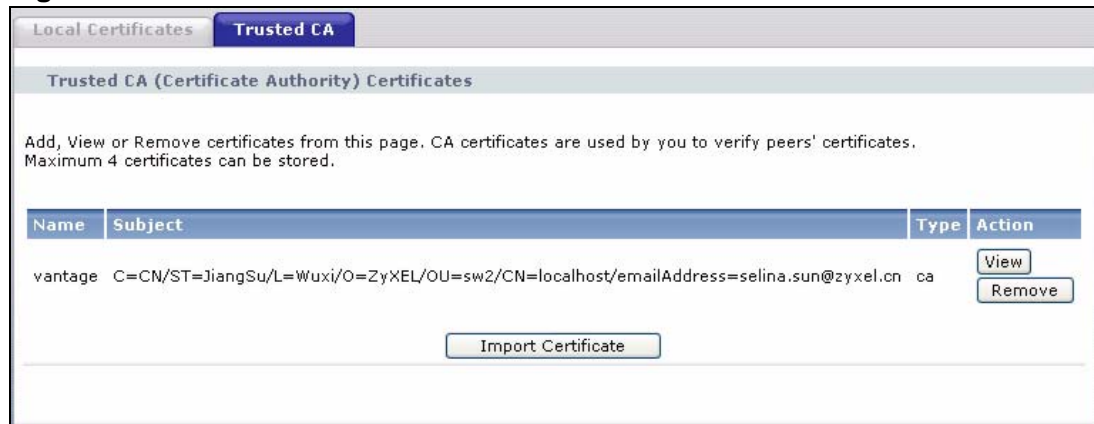
LABEL	DESCRIPTION
Certificate Name	This field is read-only and displays the identifying name of this certificate.
Certificate	Copy and paste the certificate into the text box to store it on the ZyXEL Device.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save the certificate on the ZyXEL Device.

11.4 The Trusted CA Screen

Click **Advanced Setup > Certificates > Trusted CA** to open the following screen. This screen displays a summary list of certificates of the certification authorities that you have set the ZyXEL Device to accept as trusted. The ZyXEL Device accepts any valid certificate signed by a certification authority on this list

as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

Figure 83 Trusted CA



The following table describes the fields in this screen.

Table 54 Trusted CA

LABEL	DESCRIPTION
Name	This field displays the name used to identify this certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), OU (Organizational Unit or department), Organization (O), State (ST) and Country (C). It is recommended that each certificate have unique subject information.
Type	This field displays general information about the certificate. ca means that a Certification Authority signed the certificate.
Action	Click View to open a screen with an in-depth list of information about the certificate. Click Remove to delete the certificate.
Import Certificate	Click this button to open a screen where you can save the certificate of a certification authority that you trust to the ZyXEL Device.

11.4.1 View Trusted CA Certificate

Click the **View** button in the **Trusted CA** screen to open the following screen. Use this screen to view in-depth information about the certification authority's certificate.

Figure 84 Trusted CA: View

The screenshot shows a window titled "Certificate Details". It contains a table with the following fields:

Certificate Details	
Name	vantage
Type	ca
Subject	C=CN/ST=JiangSu/L=Wuxi/O=ZyXEL/OU=sw2/CN=localhost/emailAddress=selina.sun@zyxel.cn
Certificate	<pre>-----BEGIN CERTIFICATE----- MIIDZTCCAs6gAwIBAgIBADANBgkqhkiG9w0BAQFADCBhDELMAkGA1UEBhMCQ04x EDAOBgNVBAgTB0ppYW5nU3UxDTALBgNVBAcTBGd1eGkxZjAMBgNVBAoTBVp5WEVMMQwwCgYDVQQL EwNzdXExEjAQBgNVBAMTCWxvY2FsaG9zdDEiMCAGCSqGSIB3DQEJ ARYTc2VsaW5hLnN1bkB6eXh1bC5jb2JAEFw0WnJAMjQwNzQ3NDNaFw0WnZAMjQw NzQ3NDNaMIGEMQswCQYDVQQGEwJDTjEQMA4GA1UECBMHSm1hbmddTENMA5GA1UE BxMEV3V4aTEOMAwGA1UEChMFbn1YRUwxDDAKBgNVBAsTA3N3MjESMBAGA1UEAxMJ bG9jYW5ob3NOMSIwIAZJKoZiHvcNAQkBFhNzZWxpbmEuc3VuQHp5eGVsLnNuMIGf MAOGCSqGSIB3DQEBAAUAA4GNADCB1QKBgQC/xZ3QyHyZjYyjqSVqO+msVdJ7FZPC KVARZadmqMXiWE/p2BWL4t2gmLa3ZT1Wz5mvIBdCNqKiPLATYYaDfnH/RJlhs1NF f2nAqLNXICsPqAfn6jTtHQvG5HpQvK9du9nL4NC2AlKb5yf6v+T/RN1XkI8wkZt5 JTz5rak36LRCQIDAQABo4HkMIHhMBOGA1UdDgQWBBTB5ubOANka8oftDMiFDfhP r+AWkzCBsQYDVROjBIGpMIGmBTB5ubOANka8oftDMiFDfhPr+AWk6GBiqSBhzCB hDELMAkGA1UEBhMCQ04xEDAOBgNVBAgTB0ppYW5nU3UxDTALBgNVBAcTBGd1eGkx ZjAMBgNVBAoTBVp5WEVMMQwwCgYDVQQL EwNzdXExEjAQBgNVBAMTCWxvY2FsaG9z dDEiMCAGCSqGSIB3DQEJARYTc2VsaW5hLnN1bkB6eXh1bC5jb2JAEFw0WnJAMjQw NzQ3NDNaMIGEMQswCQYDVQQGEwJDTjEQMA4GA1UECBMHSm1hbmddTENMA5GA1UE BxMEV3V4aTEOMAwGA1UEChMFbn1YRUwxDDAKBgNVBAsTA3N3MjESMBAGA1UEAxMJ bG9jYW5ob3NOMSIwIAZJKoZiHvcNAQkBFhNzZWxpbmEuc3VuQHp5eGVsLnNuMIGf MAOGCSqGSIB3DQEBAAUAA4GBAJ380QrfqjGzZaLswWP8s/nhmE4glDdZ T+q8nxXC6cNnpexXakOt9lhrkcr/qNuPkg581JZ6Xm2zp7k5ufP4gWOFPU7N3m7E RKFSJoIvn+rk5s3V/xv5NXs7Wze15Idmth2k88bS/s1VXjcRodC1UWQmMOUUNC1N8 6wiznH6QWS3y</pre>

At the bottom of the window is a "Back" button.

The following table describes the fields in this screen.

Table 55 Trusted CA: View

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate.
Type	This field displays general information about the certificate. ca means that a Certification Authority signed the certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Certificate	<p>This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form.</p> <p>You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).</p>
Back	Click this button to return to the previous screen.

11.4.2 Import Trusted CA Certificate

Click the **Import Certificate** button in the **Trusted CA** screen to open the following screen. The ZyXEL Device trusts any valid certificate signed by any of the imported trusted CA certificates.

Figure 85 Trusted CA: Import Certificate

The following table describes the fields in this screen.

Table 56 Trusted CA: Import Certificate

LABEL	DESCRIPTION
Certificate Name	Enter the name that identifies this certificate.
Certificate	Copy and paste the certificate into the text box to store it on the ZyXEL Device.
Back	Click this button to return to the previous screen.
Apply	Click this button to save your changes back to the ZyXEL Device.

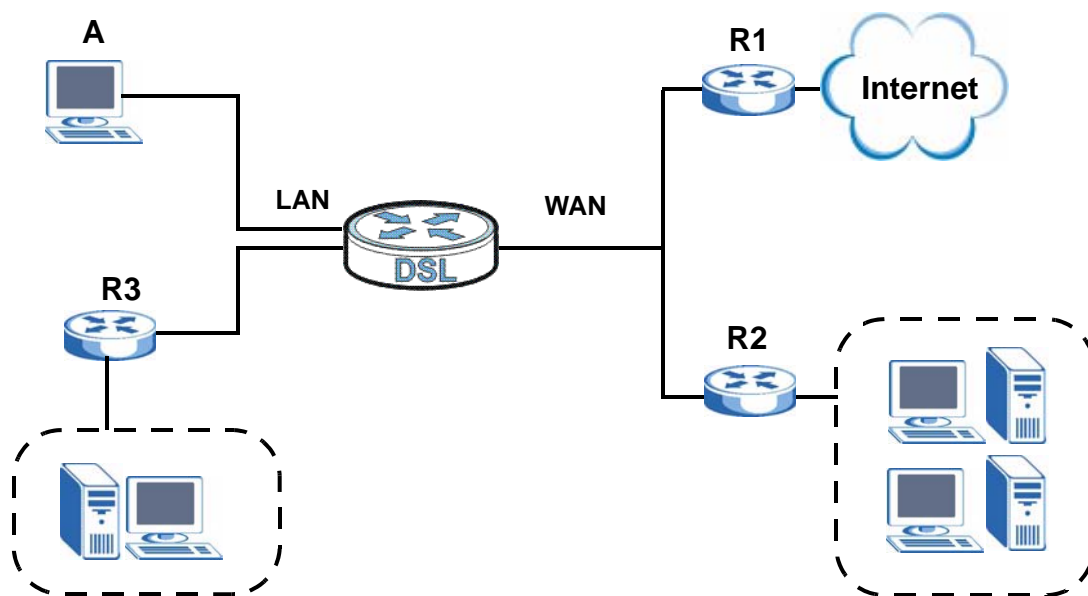
Static Route

12.1 Overview

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

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

Figure 86 Example of Static Routing Topology



12.1.1 What You Can Do in this Chapter

The **Static Route** screens let you view and configure IP static routes on the ZyXEL Device ([Section 12.2 on page 154](#)).

12.2 The Static Route Screen

Click **Advanced > Static Route** to open the **Static Route** screen.

Figure 87 Advanced > Static Route

#	Active	Destination	Netmask	Gateway	Interface	Remove
1	<input checked="" type="checkbox"/>	10.1.2.3	255.255.255.255		ppp0_1	

The following table describes the labels in this screen.

Table 57 Advanced > Static Route

LABEL	DESCRIPTION
#	This is the number of an individual static route.
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.
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Netmask	This parameter specifies the IP network subnet mask of the final destination.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Interface	This is the WAN interface through which the traffic is routed.
Remove	Click the icon to remove a static route from the ZyXEL Device. A window displays asking you to confirm that you want to delete the route.
Add	Click this to create a new rule.
Apply	Click this to apply your changes to the ZyXEL Device.

12.2.1 Static Route Edit

Click the **Add** button in the **Static Route** screen. Use this screen to configure the required information for a static route.

Figure 88 Static Route: Add

The following table describes the labels in this screen.

Table 58 Static Route: Add

LABEL	DESCRIPTION
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Use Interface	Select a WAN interface through which the traffic is sent. You must have the WAN interface(s) already configured in the WAN screens.
Use Gateway IP Address	Select this option and enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your ZyXEL Device's interface(s). The gateway helps forward packets to their destinations.
Back	Click Back to return to the previous screen without saving.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

Policy Forwarding

13.1 Overview

Traditionally, routing is based on the destination address only and the ZyXEL Device takes the shortest path to forward a packet. Policy forwarding allows the ZyXEL Device to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to outgoing packets, prior to the normal routing.

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

13.1.1 What You Can Do in this Chapter

The **Policy Forwarding** screens let you view and configure routing policies on the ZyXEL Device ([Section 13.2 on page 157](#)).

13.2 The Static Route Screen

Click **Advanced > Policy Forwarding** to open the **Policy Forwarding** screen.

Figure 89 Advanced > Policy Forwarding

Policy Forwarding

Policy Forwarding

A maximum 8 entries can be configured.

Policy Name	SourceIP	Protocol	SourcePort	SourceMac	WAN	Remove
test	192.168.1.99	TCP	23	ptm0_1		

The following table describes the labels in this screen.

Table 59 Advanced > Policy Forwarding

LABEL	DESCRIPTION
Policy Name	This is the name of the rule.
SourceIP	This is the source IP address.
Protocol	This is the IP protocol.
SourcePort	This is the source port number.
SourceMAC	This is the source MAC address.
Interface	This is the WAN interface through which the traffic is routed.
Remove	Click the icon to remove a rule from the ZyXEL Device. A window displays asking you to confirm that you want to delete the rule.
Add	Click this to create a new rule.

13.2.1 Policy Forwarding Setup

Click the **Add** button in the **Policy Forwarding** screen. Use this screen to configure the required information for a policy route.

Figure 90 Policy Forwarding: Add

The following table describes the labels in this screen.

Table 60 Policy Forwarding: Add

LABEL	DESCRIPTION
Policy Name	Enter a descriptive name of up to 16 printable English keyboard characters, including spaces.
Source IP Address	Enter the source IP address.
Protocol	Select the IP protocol (TCP or UDP).
Source Port	Enter the source port number.
Use Interface	Select a WAN interface through which the traffic is sent. You must have the WAN interface(s) already configured in the WAN screens.
Back	Click Back to return to the previous screen without saving.

Table 60 Policy Forwarding: Add

LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

14.1 Overview

Routing Information Protocol (RIP, RFC 1058 and RFC 1389) allows a device to exchange routing information with other routers.

14.1.1 What You Can Do in this Chapter

The **RIP** screen lets you set up RIP settings on the ZyXEL Device ([Section 14.2 on page 161](#)).

14.2 The RIP Screen

Click **Advanced > RIP** to open the **RIP** screen.

Figure 91 Advanced > RIP

Interface	Version	Operation	Enabled
ptm0_2	2	Passive	<input type="checkbox"/>
ptm0_5	2	Passive	<input type="checkbox"/>

Apply/Save

The following table describes the labels in this screen.

Table 61 Advanced > RIP

LABEL	DESCRIPTION
Interface	This is the name of the interface in which the RIP setting is used.
Version	The RIP version controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). RIP version 1 is universally supported but RIP version 2 carries more information. RIP version 1 is probably adequate for most networks, unless you have an unusual network topology.
Operation	Select Passive to have the ZyXEL Device update the routing table based on the RIP packets received from neighbors but not advertise its route information to other routers in this interface. Select Active to have the ZyXEL Device advertise its route information and also listen for routing updates from neighboring routers.
Enabled	Select the check box to activate the settings.
Apply/Save	Click Apply/Save to save your changes back to the ZyXEL Device.

Quality of Service (QoS)

15.1 Overview

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

Configure QoS on the ZyXEL Device to group and prioritize application traffic and fine-tune network performance. Setting up QoS involves these steps:

- 1 Configure classifiers to sort traffic into different flows.
- 2 Assign priority and define actions to be performed for a classified traffic flow.

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

This chapter contains information about configuring QoS and editing classifiers.

15.1.1 What You Can Do in this Chapter

- The **General** screen lets you enable or disable QoS and set the default DSCP value for incoming traffic does not match a class ([Section 15.3 on page 164](#)).
- The **Queue Setup** screen lets you configure QoS queue assignment ([Section 15.4 on page 166](#)).
- The **Class Setup** screen lets you add, edit or delete QoS classifiers ([Section 15.5 on page 168](#)).

- The **Monitor** screen lets you view the ZyXEL Device's QoS-related packet statistics ([Section 15.6 on page 174](#)).

15.2 What You Need to Know

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

QoS versus Cos

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

CoS technologies include IEEE 802.1p layer 2 tagging and DiffServ (Differentiated Services or DS). IEEE 802.1p tagging makes use of three bits in the packet header, while DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit ToS (Type of Service) field in the IP header.

Tagging and Marking

In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or service based on the tag or marker.

15.3 The Quality of Service General Screen

Click **Advanced Setup** > **Quality of Service** to open the screen as shown next.

Use this screen to enable or disable QoS and set the default DSCP value for incoming traffic does not match a class. See [Section 15.1 on page 163](#) for more information.

Figure 92 QoS General

The following table describes the labels in this screen.

Table 62 QoS General

LABEL	DESCRIPTION
Active QoS	Select the check box to turn on QoS to improve your network performance.
WAN Managed Upstream Bandwidth	<p>Enter the amount of upstream bandwidth for the WAN interface that you want to allocate using QoS.</p> <p>The recommendation is to set this speed to match the interface's actual transmission speed. For example, set the WAN interface speed to 100000 kbps if your Internet connection has an upstream transmission speed of 100 Mbps.</p> <p>You can set this number higher than the interface's actual transmission speed. The ZyXEL Device uses up to 95% of the DSL port's actual upstream transmission speed even if you set this number higher than the DSL port's actual transmission speed.</p> <p>You can also set this number lower than the interface's actual transmission speed. This will cause the ZyXEL Device to not use some of the interface's available bandwidth.</p> <p>If you leave this field blank, the ZyXEL Device automatically sets this number to be 95% of the DSL port's actual upstream transmission speed.</p>
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

15.4 The Queue Setup Screen

Click **QoS > Queue Setup** to open the screen as shown next.

Use this screen to configure QoS queue assignment.

Figure 93 QoS Queue Setup

No.	Active	Name	Interface	Priority	Weight	Buffer Management	Rate Limit	Modify
1	<input checked="" type="checkbox"/>	Q1	WAN	1	1	DT	1000	

Apply

The following table describes the labels in this screen.

Table 63 QoS Queue Setup

LABEL	DESCRIPTION
Add	Click this button to create a new entry.
No.	This is the index number of this entry.
Active	Select the check box to enable the queue.
Name	This shows the descriptive name of this queue.
Interface	This shows the name of the ZyXEL Device's interface through which traffic in this queue passes.
Priority	This shows the priority of this queue.
Weight	This shows the weight of this queue.
Buffer Management	This shows the queue management algorithm used by the ZyXEL Device.
Rate Limit	This shows the maximum transmission rate allowed for traffic on this queue.
Modify	Click the Edit icon to go to the screen where you can edit the queue. Click the Remove icon to delete an existing queue. Note that subsequent rules move up by one when you take this action.
Apply	Click Apply to save your changes back to the ZyXEL Device.

15.4.1 Adding a QoS Queue

Click the **Add** button or the edit icon in the **Queue Setup** screen to configure a queue.

Figure 94 QoS Queue Setup: Add

The following table describes the labels in this screen.

Table 64 QoS Queue Setup: Add

LABEL	DESCRIPTION
Active	Select to enable or disable this queue.
Name	Enter the descriptive name of this queue.
Interface	Select the interface to which this queue is applied.
Priority	Select the priority level (from 1 to 3) of this queue. The smaller the number, the higher the priority level. Traffic assigned to higher priority queues gets through faster while traffic in lower priority queues is dropped if the network is congested.
Weight	Select the weight (from 1 to 8) of this queue. If two queues have the same priority level, the ZyXEL Device divides the bandwidth across the queues according to their weights. Queues with larger weights get more bandwidth than queues with smaller weights.
Buffer Management	This field displays Drop Tail (DT) and the ZyXEL Device drops the newly arriving packet when the queue is full.
Rate Limit	Specify the maximum transmission rate (in Kbps) allowed for traffic on this queue.
Back	Click Back to return to the previous screen without saving.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

15.5 The Class Setup Screen

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

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

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

Figure 95 QoS Class Setup

The following table describes the labels in this screen.

Table 65 QoS Class Setup

LABEL	DESCRIPTION
Add	Click this button to create a new classifier.
Order	This field displays the index number of the classifier.
Active	Select the check box to enable the classifier.
Class Name	This is the name of the classifier.
Classification Criteria	This shows criteria specified in this classifier, for example the interface from which traffic of this class should come and the source MAC address of traffic that matches this classifier.
Forward To	This is the interface through which traffic that matches this classifier is forwarded out.
DSCP Mark	This is the DSCP number added to traffic of this classifier.
802.1P Mark	This is the IEEE 802.1p priority level assigned to traffic of this classifier.

Table 65 QoS Class Setup (continued)

LABEL	DESCRIPTION
VLAN ID Tag	This is the VLAN ID number assigned to traffic of this classifier.
To Queue	This is the name of the queue in which traffic of this classifier is put.
Modify	<p>Click the Edit icon to go to the screen where you can edit the classifier.</p> <p>Click the Remove icon to delete an existing classifier. Note that subsequent rules move up by one when you take this action.</p>
Apply	Click Apply to save your changes back to the ZyXEL Device.

15.5.1 QoS Class Edit

Click the **Add** button or the **Edit** icon in the **Class Setup** screen to configure a classifier.

Figure 96 QoS Class Setup: Add

Class Configuration

☒ Active

Class Name

Classification Order ▼

Forward To Interface ▼

DSCP Mark ▼ (0~63)

802.1P Mark ▼

VLAN ID Tag ▼ (1~4095)

To Queue ▼

Criteria Configuration

Basic

☒ From Interface ▼

☒ Ether Type ▼

Source

☐ MAC Address MAC Mask ☐ Exclude

☐ IP Address IP Subnet Mask ☐ Exclude

☐ TCP/UDP Port Range ~ ☐ Exclude

Destination

☐ MAC Address MAC Mask ☐ Exclude

☐ IP Address IP Subnet Mask ☐ Exclude

☐ TCP/UDP Port Range ~ ☐ Exclude

Others

☐ 802.1P ▼ ☐ Exclude

☐ VLAN ID (1~4095) ☐ Exclude

☒ IP Protocol ▼ ☐ Exclude

☐ IP Packet Length ~ ☐ Exclude

☐ DSCP (0~63) ☐ Exclude

☐ TCP ACK ☐ Exclude

☐ DHCP ▼ ☐ Exclude

The following table describes the labels in this screen.

Table 66 QoS Class Configuration

LABEL	DESCRIPTION
Class Configuration	
Active	Select to enable or disable this classifier.
Class Name	Enter a descriptive name of up to 20 printable English keyboard characters, including spaces.
Classification Order	Select an existing number for where you want to put this classifier to move the classifier to the number you selected after clicking Apply . Select Last to put this rule in the back of the classifier list.
Forward to Interface	Select a WAN interface through which traffic of this class will be forwarded out. If you select Unchange , the ZyXEL Device forward traffic of this class according to the default routing table.
DSCP Mark	This field is available only when you select the Ether Type check box. If you select Mark , enter a DSCP value with which the ZyXEL Device replaces the DSCP field in the packets. If you select Auto Mapping and there is a VLAN tag carried in the matched packets, the ZyXEL Device will replace the IP ToS field with the 802.1p priority field. If you select Unchange , the ZyXEL Device keep the DSCP field in the packets.
802.1p Mark	Select a priority level with which the ZyXEL Device replaces the IEEE 802.1p priority field in the packets. If you select Unchange , the ZyXEL Device keep the 802.1p priority field in the packets.
VLAN ID Tag	If you select Remark , enter a VLAN ID number (between 1 and 4095) with which the ZyXEL Device replaces the VLAN ID of the frames. If you select Remove , the ZyXEL Device deletes the VLAN ID of the frames before forwarding them out. If you select Add , the ZyXEL Device treat all matched traffic untagged and add a second VLAN ID. If you select Unchange , the ZyXEL Device keep the VLAN ID in the packets.
To Queue	Select a queue that applies to this class. You should have configured a queue in the Queue Setup screen already.
Criteria Configuration	
Use the following fields to configure the criteria for traffic classification.	
Basic	
From Interface	Select from which Ethernet port or wireless interface traffic of this class should come.

Table 66 QoS Class Configuration (continued)

LABEL	DESCRIPTION
Ether Type	<p>Select a predefined application to configure a class for the matched traffic.</p> <p>If you select IP, you also need to configure source or destination MAC address, IP address, DHCP options, DSCP value or the protocol type.</p> <p>If you select 8021Q, you can configure an 802.1p priority level and VLAN ID in the Others section.</p>
Source	
MAC Address	Select the check box and enter the source MAC address of the packet.
MAC Mask	<p>Type the mask for the specified MAC address to determine which bits a packet's MAC address should match.</p> <p>Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.</p>
IP Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
IP Subnet Mask	Enter the source subnet mask.
TCP/UDP Port Range	If you select TCP or UDP in the IP Protocol field, select the check box and enter the port number(s) of the source.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Destination	
MAC Address	Select the check box and enter the destination MAC address of the packet.
MAC Mask	<p>Type the mask for the specified MAC address to determine which bits a packet's MAC address should match.</p> <p>Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.</p>
IP Address	Select the check box and enter the destination IP address in dotted decimal notation. A blank source IP address means any source IP address.
IP Subnet Mask	Enter the destination subnet mask.
TCP/UDP Port Range	If you select TCP or UDP in the IP Protocol field, select the check box and enter the port number(s) of the source.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Others	

Table 66 QoS Class Configuration (continued)

LABEL	DESCRIPTION
802.1P	<p>This field is available only when you select 802.1Q in the Ether Type field.</p> <p>Select this option and select a priority level (between 0 and 7) from the drop down list box.</p> <p>"0" is the lowest priority level and "7" is the highest.</p>
VLAN ID	<p>This field is available only when you select 802.1Q in the Ether Type field.</p> <p>Select this option and specify a VLAN ID number between 1 and 4095.</p>
IP Protocol	<p>This field is available only when you select IP in the Ether Type field.</p> <p>Select this option and select the protocol (service type) from TCP, UDP, ICMP or IGMP. If you select User defined, enter the protocol (service type) number.</p>
IP Packet Length	<p>This field is available only when you select IP in the Ether Type field.</p> <p>Select this option and enter the minimum and maximum packet length (from 28 to 1500) in the fields provided.</p>
DSCP	<p>This field is available only when you select IP in the Ether Type field.</p> <p>Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.</p>
TCP ACK	<p>This field is available only when you select IP in the Ether Type field.</p> <p>If you select this option, the matched TCP packets must contain the ACK (Acknowledge) flag.</p>
DHCP	<p>This field is available only when you select IP in the Ether Type field.</p> <p>Select this option and select a DHCP option.</p> <p>If you select Vendor Class ID (DHCP Option 60), enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware.</p> <p>If you select User Class ID (DHCP Option 77), enter a string that identifies the user's category or application type in the matched DHCP packets.</p>
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Back	Click Back to return to the previous screen without saving.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

15.6 The QoS Monitor Screen

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

Figure 97 QoS > Monitor

General Queue Setup Class Setup **Monitor**

Monitor

Refresh Interval: No Refresh

Interface Monitor

No.	Name	Pass Rate (bps)	Drop Rate (bps)
1	ptm0_1	0	0
2	ptm0_2	0	0
3	ptm0_3	0	0

Queue Monitor

No.	Name	Pass Rate (bps)	Drop Rate (bps)
1	Q1		

The following table describes the labels in this screen.

Table 67 QoS > Monitor

LABEL	DESCRIPTION
Refresh Interval	Enter how often you want the ZyXEL Device to update this screen. Select No Refresh to stop refreshing statistics.
Interface Monitor	
No.	This is the index number of the entry.
Name	This shows the name of the WAN interface on the ZyXEL Device.
Pass	This shows how many packets forwarded to this interface are transmitted successfully.
Drop	This shows how many packets forwarded to this interface are dropped.
Queue Monitor	
No.	This is the index number of the entry.
Name	This shows the name of the queue.
Pass	This shows how many packets assigned to this queue are transmitted successfully.
Drop	This shows how many packets assigned to this queue are dropped.

15.7 Technical Reference

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

IEEE 802.1Q Tag

The IEEE 802.1Q standard defines an explicit VLAN tag in the MAC header to identify the VLAN membership of a frame across bridges. A VLAN tag includes the 12-bit VLAN ID and 3-bit user priority. The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network.

IEEE 802.1p specifies the user priority field and defines up to eight separate traffic types. The following table describes the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).

Table 68 IEEE 802.1p Priority Level and Traffic Type

PRIORITY LEVEL	TRAFFIC TYPE
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for "spare bandwidth".
Level 1	This is typically used for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.

DiffServ

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

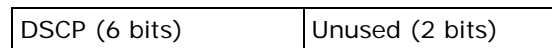
DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of

service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

DSCP and Per-Hop Behavior

DiffServ defines a new Differentiated Services (DS) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.



The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

Dynamic DNS Setup

16.1 Overview

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

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

16.1.1 What You Can Do in this Chapter

Use the **Dynamic DNS** screen ([Section 16.3 on page 178](#)) to enable DDNS and configure the DDNS settings on the ZyXEL Device.

16.2 What You Need To Know

DYNDNS Wildcard

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

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

16.3 The Dynamic DNS Screen

To change your ZyXEL Device's DDNS, click **Advanced > Dynamic DNS**. The screen appears as shown.

Figure 98 Advanced > Dynamic DNS

The following table describes the fields in this screen.

Table 69 Advanced > Dynamic DNS

LABEL	DESCRIPTION
Service Provider	Select the name of your Dynamic DNS service provider.
Host Name	Type the domain name assigned to your ZyXEL Device by your Dynamic DNS provider. You can specify up to two host names in the field separated by a comma (",").
Interface	Select the WAN interface to use for updating the IP address of the domain name.
User Name	Type your user name.
Password	Type the password assigned to you.
Email	If you select TZO in the Service Provider field, enter the user name you used to register for this service.
Key	If you select TZO in the Service Provider field, enter the password you used to register for this service.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

Remote Management

17.1 Overview

This chapter explains how to configure the TR-069 settings and access control settings on the ZyXEL Device.

17.1.1 What You Can Do in this Chapter

- The **TR-069** screen lets you configure the ZyXEL Device's TR-069 auto-configuration settings ([Section 17.3 on page 181](#)).
- The **TR-064** screen lets you enable management via TR-064 on the ZyXEL Device ([Section 17.3 on page 181](#)).
- The **Service Control** screens let you configure through which interface(s) users can use which service(s) to manage the ZyXEL Device ([Section 17.4 on page 182](#)).
- The **IP Address** screens let you configure from which IP address(es) users can use a service to manage the ZyXEL Device ([Section 17.5 on page 183](#)).

17.2 The TR-069 Screen

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

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

Click **Advanced > Remote MGMT** to open the following screen. Use this screen to configure your P-870HA to be managed by an ACS.

Figure 99 TR-069

The screenshot shows the TR-069 configuration interface. It includes tabs for TR069, TR064, ServiceControl, and IPAddress. The TR069 tab is selected. The configuration options are as follows:

- Inform:** Radio buttons for ☒ Disable and ☐ Enable.
- Inform Interval:** A text box containing '300' followed by 'sec (Min.: 30 sec)'.
- ACS URL:** An empty text box.
- ACS User Name:** A text box containing 'admin'.
- ACS Password:** A text box with masked characters '*****'.
- WAN Interface used by TR-069 client:** A dropdown menu showing 'Any_WAN'.
- Display SOAP messages on serial console:** Radio buttons for ☒ Disable and ☐ Enable.
- Connection Request Authentication:** A checked checkbox.
- ConnectionRequest User Name:** A text box containing 'admin'.
- ConnectionRequest Password:** A text box with masked characters '*****'.
- Connection Request URL:** A text box containing 'http://172.16.1.112:30005/'.

At the bottom of the form are two buttons: 'Apply/Save' and 'Cancel'.

The following table describes the fields in this screen.

Table 70 TR-069

LABEL	DESCRIPTION
Inform	Select Enable to activate remote management via TR-069 on the WAN. Otherwise, select Disable .
Inform Interval	Enter the time interval (in seconds) at which the ZyXEL Device sends information to the auto-configuration server.
ACS URL	Enter the URL or IP address of the auto-configuration server.
ACS User Name	Enter the TR-069 user name for authentication with the auto-configuration server.
ACS Password	Enter the TR-069 password for authentication with the auto-configuration server.
WAN Interface used by TR-069 client	Select a WAN interface through which the TR-069 traffic passes.
Display SOAP messages on serial console	Select Enable to show the SOAP messages on the console.
Connection Request Authentication	Select this option to enable authentication when there is a connection request from the ACS.
Connection Request User Name	Enter the connection request user name. When the ACS makes a connection request to the ZyXEL Device, this user name is used to authenticate the ACS.

Table 70 TR-069 (continued)

LABEL	DESCRIPTION
Connection Request Password	Enter the connection request password. When the ACS makes a connection request to the ZyXEL Device, this password is used to authenticate the ACS.
Connection Request URL	This shows the connection request URL. The ACS can use this URL to make a connection request to the ZyXEL Device.
Apply/Save	Click this button to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

17.3 The TR-064 Screen

TR-064 is a LAN-Side DSL CPE Configuration protocol defined by the DSL Forum. TR-064 is built on top of UPnP. It allows the users to use a TR-064 compliant CPE management application on their computers from the LAN to discover the CPE and configure user-specific parameters, such as the username and password.

Click **Advanced** > **Remote MGMT** > **TR064** to open the following screen.

Figure 100 TR-064

The following table describes the fields in this screen.

Table 71 TR-064

LABEL	DESCRIPTION
Enable TR064	Select the check box to activate management via TR-064 on the LAN.
Apply	Click this button to save your changes back to the ZyXEL Device.

17.4 The Service Control Screen

Click **Advanced > Remote MGMT > Service Control** to open the following screen. Use this screen to decide what services you may use to access which ZyXEL Device interface.

Figure 101 Service Control

#	Services	LAN	WAN
1	FTP	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
2	HTTP	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
3	SSH	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
4	TELNET	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
5	TFTP	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable

Apply

The following table describes the fields in this screen.

Table 72 Access Control: Services

LABEL	DESCRIPTION
Service Control	Select Enable to turn on service control. Otherwise, select Disable .
#	This is the index number of the entry.
Services	This is the service you may use to access the ZyXEL Device.
LAN	Select the Enable check box for the corresponding services that you want to allow access to the ZyXEL Device from the LAN.
WAN	Select the Enable check box for the corresponding services that you want to allow access to the ZyXEL Device from the WAN.
Apply	Click this button to save your changes back to the ZyXEL Device.

17.5 The IP Address Screen

Click **Advanced > Remote MGMT > IP Address** to open the following screen. Use this screen to specify the “trusted” computers from which an administrator may use a service to manage the ZyXEL Device.

Figure 102 IP Address

TR069 TR064 ServiceControl **IPAddress**

Access Control -- IP Address

The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List

Access Control Mode: ☒ Disable ☐ Enable

IP Address	Remove
192.168.1.99	<input type="checkbox"/>

.....

Add Remove

The following table describes the fields in this screen.

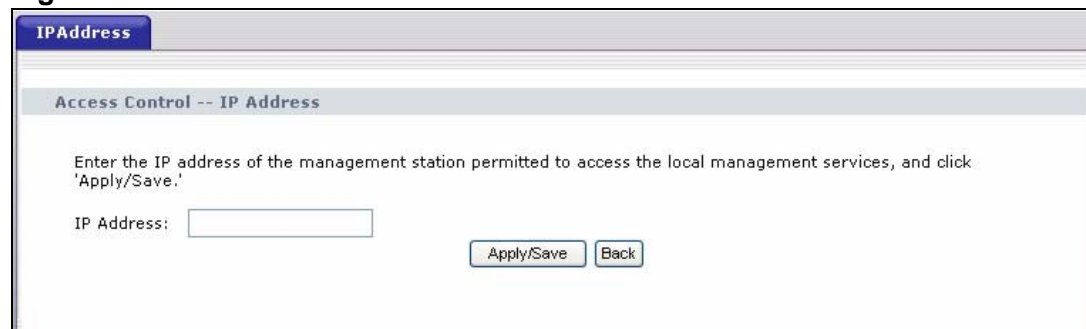
Table 73 IP Address

LABEL	DESCRIPTION
Access Control Mode	Select Enable to activate the secured client list. Select Disable to disable the list without deleting it.
IP Address	This is the IP address of the trusted computer from which you can manage the ZyXEL Device.
Remove	Select this check box and click the Remove button to delete this entry from the ZyXEL Device.
Add	Click this button to create a new entry.
Remove	Click this button to delete the selected entry.

17.5.1 Adding an IP Address

Click the **Add** button in the **IP Address** screen to open the following screen.

Figure 103 IP Address: Add



IPAddress

Access Control -- IP Address

Enter the IP address of the management station permitted to access the local management services, and click 'Apply/Save.'

IP Address:

Apply/Save Back

The following table describes the fields in this screen.

Table 74 IP Address: Add

LABEL	DESCRIPTION
IP Address	Enter the IP address of the trusted computer from which you can manage the ZyXEL Device.
Apply/Save	Click this button to save your changes back to the ZyXEL Device.
Back	Click this button to return to the previous screen without saving.

Universal Plug-and-Play (UPnP)

18.1 Overview

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

18.1.1 What You Can Do in this Chapter

The **UPnP** screen lets you enable UPnP on the ZyXEL Device ([Section 18.3 on page 186](#)).

18.2 What You Need to Know

How do I know if I'm using UPnP?

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

NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the NAT chapter for more information on NAT.

Cautions with UPnP

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

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

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

UPnP and ZyXEL

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

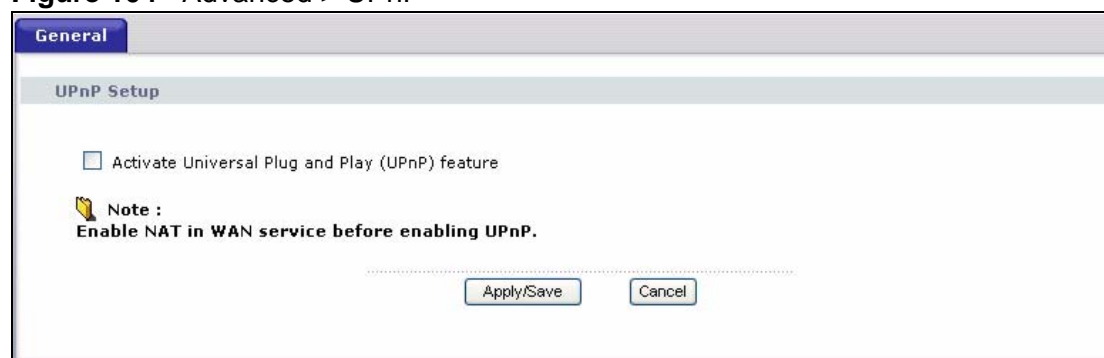
See the following sections for examples of installing and using UPnP.

18.3 The UPnP Screen

Click **Advanced > UPnP** to display the screen shown next.

See [Section 18.1 on page 185](#) for more information.

Figure 104 Advanced > UPnP



The following table describes the fields in this screen.

Table 75 Advanced > UPnP

LABEL	DESCRIPTION
Activate Universal Plug and Play (UPnP) Feature	Select this check box to enable UPnP. Be aware that anyone could use a UPnP application to open the Web Configurator's login screen without entering the ZyXEL Device's IP address (although you must still enter the password to access the Web Configurator).
Apply/Save	Click this to save the setting to the ZyXEL Device.
Cancel	Click this to return to the previously saved settings.

18.4 Installing UPnP in Windows Example

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

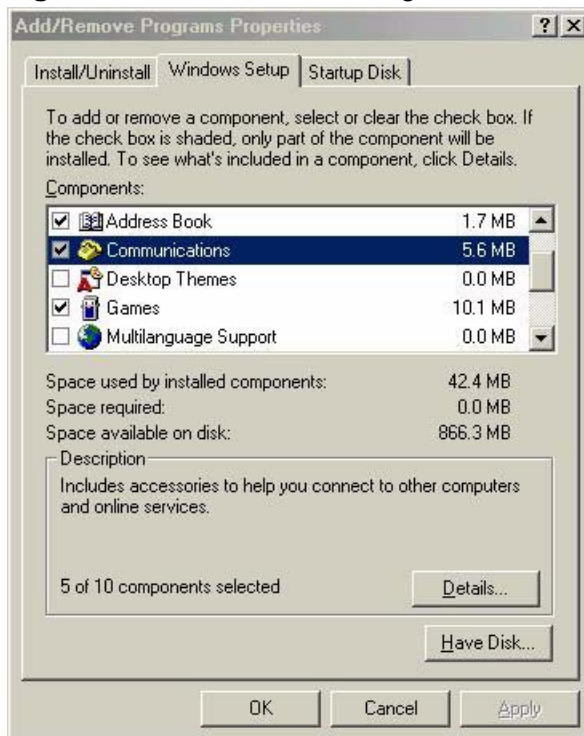
Installing UPnP in Windows Me

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

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

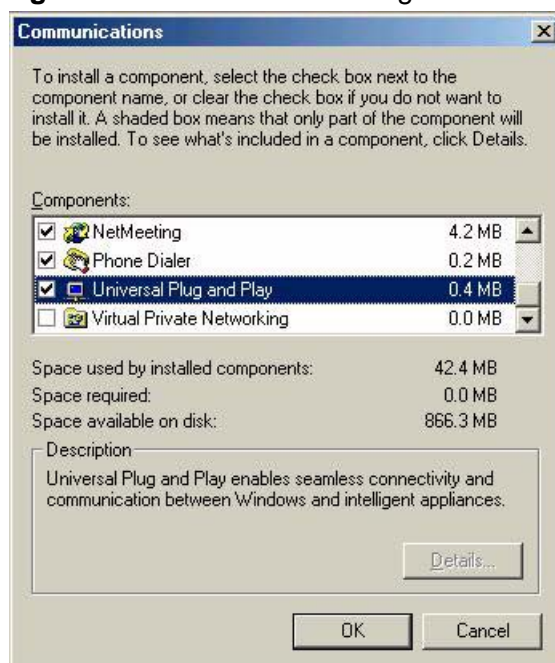
- 2 Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.

Figure 105 Add/Remove Programs: Windows Setup: Communication



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

Figure 106 Add/Remove Programs: Windows Setup: Communication: Components



- 4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.
- 5 Restart the computer when prompted.

Installing UPnP in Windows XP

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

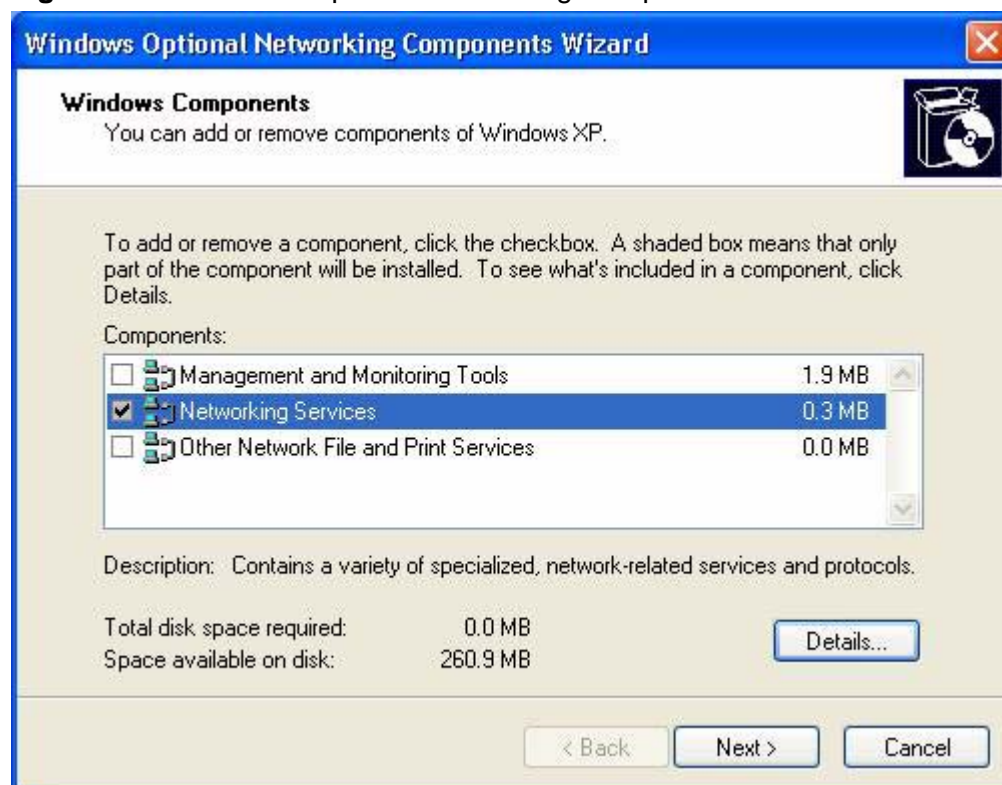
- 1 Click **Start** and **Control Panel**.
- 2 Double-click **Network Connections**.
- 3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components**

Figure 107 Network Connections



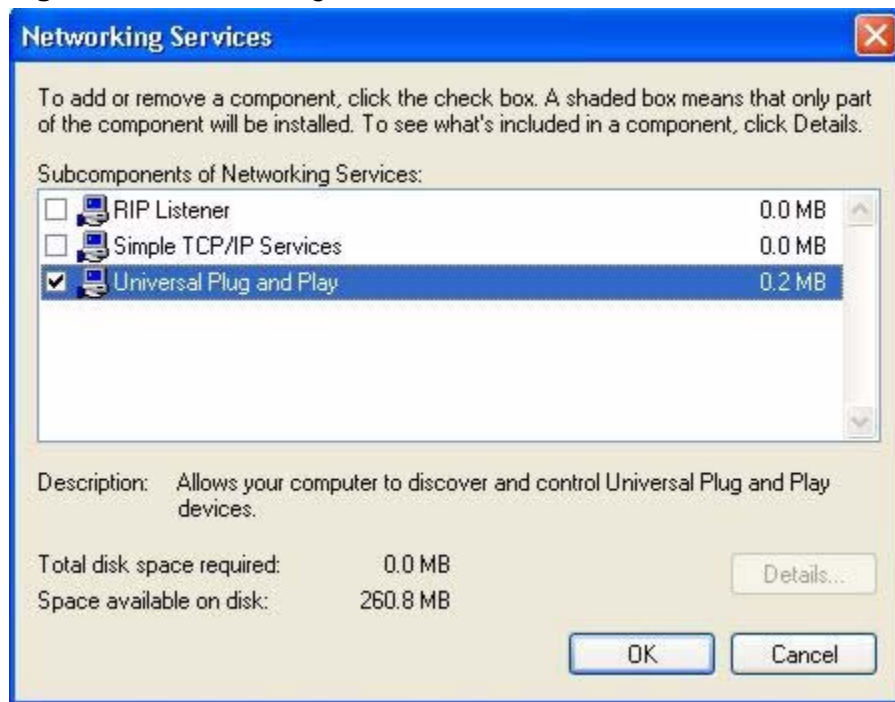
- 4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

Figure 108 Windows Optional Networking Components Wizard



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

Figure 109 Networking Services



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

18.5 Using UPnP in Windows XP Example

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

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

Auto-discover Your UPnP-enabled Network Device

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

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

Figure 110 Network Connections



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

Figure 111 Internet Connection Properties



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

Figure 112 Internet Connection Properties: Advanced Settings

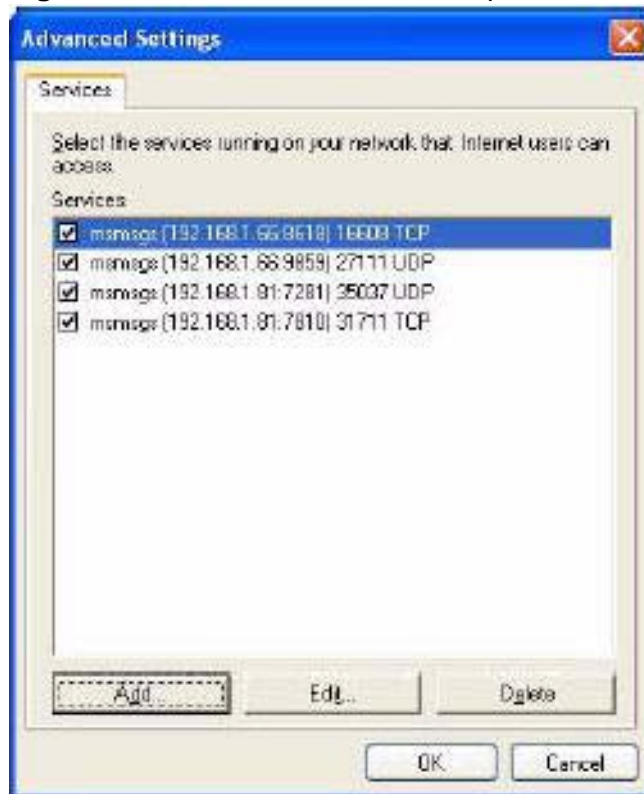
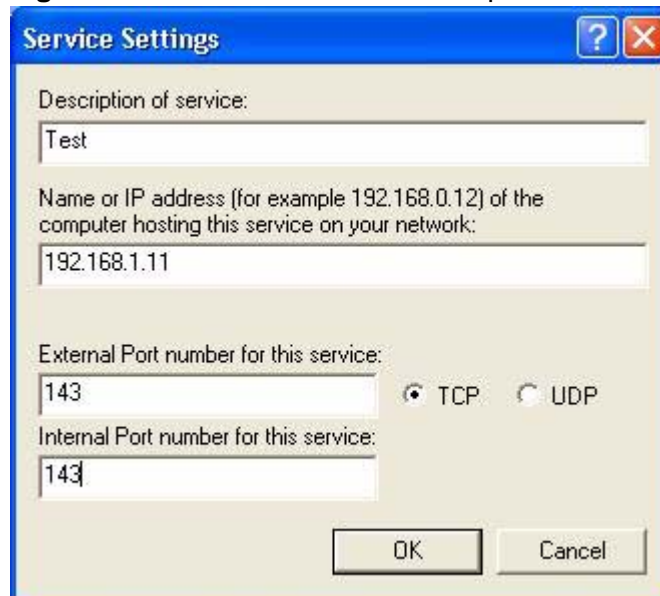


Figure 113 Internet Connection Properties: Advanced Settings: Add



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

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

Figure 114 System Tray Icon



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

Figure 115 Internet Connection Status



Web Configurator Easy Access

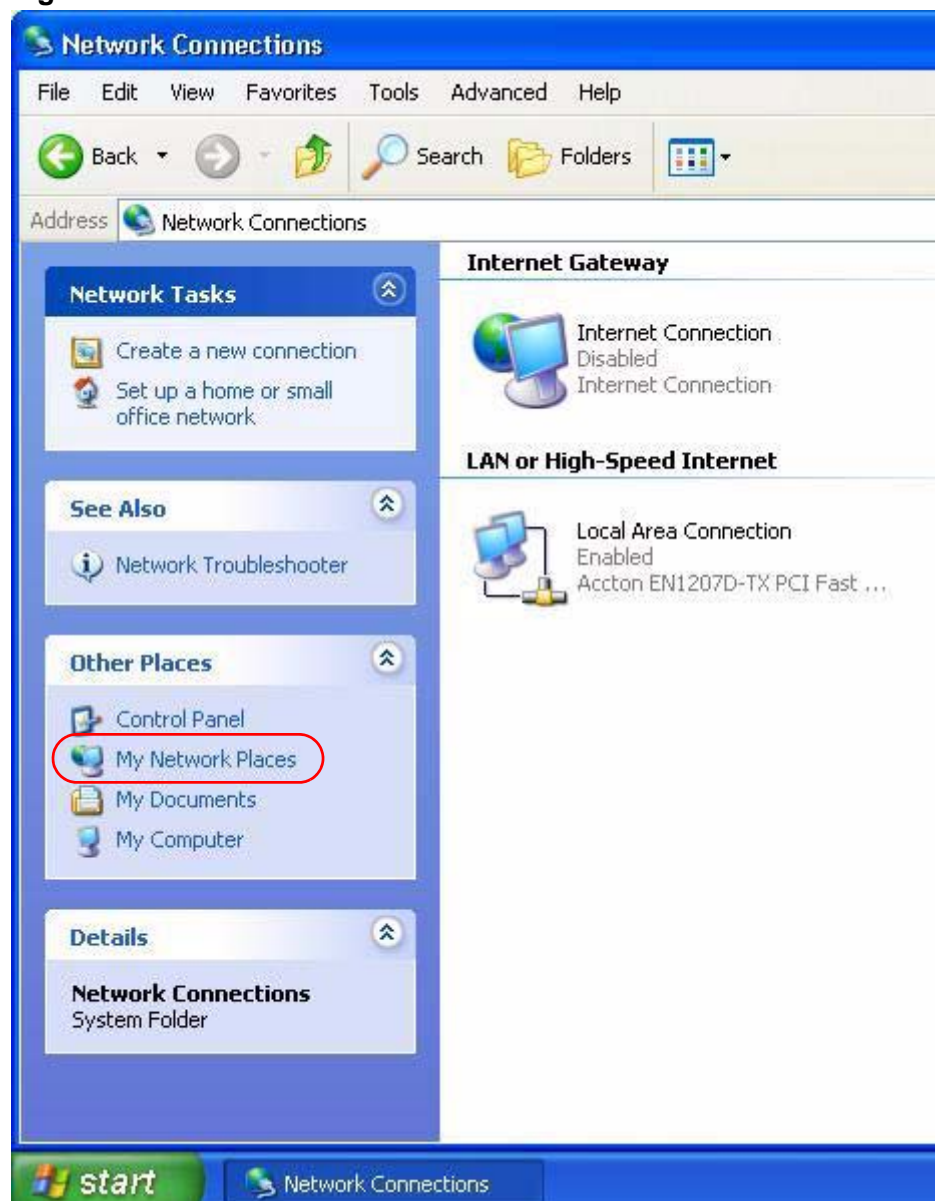
With UPnP, you can access the web-based configurator on the ZyXEL Device without finding out the IP address of the ZyXEL Device first. This comes helpful if you do not know the IP address of the ZyXEL Device.

Follow the steps below to access the Web Configurator.

- 1 Click **Start** and then **Control Panel**.
- 2 Double-click **Network Connections**.

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

Figure 116 Network Connections



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

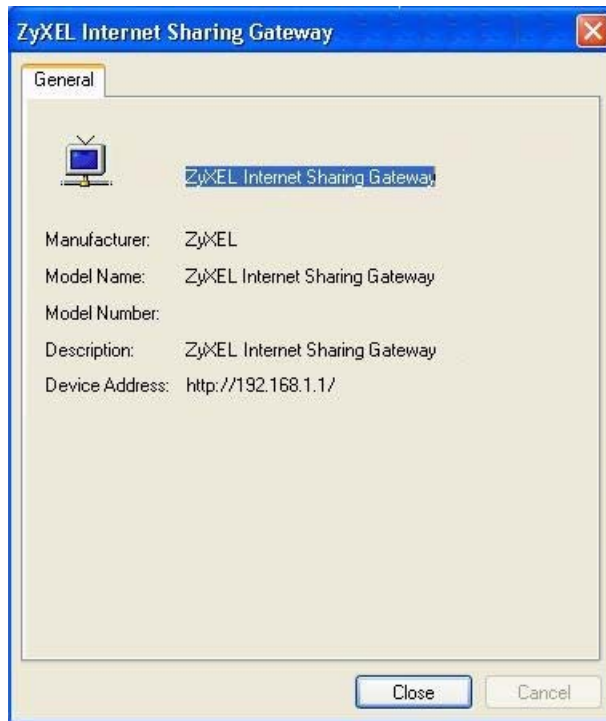
- 5 Right-click on the icon for your ZyXEL Device and select **Invoke**. The Web Configurator login screen displays.

Figure 117 Network Connections: My Network Places



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

Figure 118 Network Connections: My Network Places: Properties: Example



Parental Control

19.1 Overview

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

19.1.1 What You Can Do in this Chapter

- The **Time Restriction** screen lets you give different time restrictions to each user of your network ([Section 19.2 on page 199](#)).
- The **URL Filter** screen lets you restrict home network users from viewing inappropriate websites ([Section 19.3 on page 201](#)).

19.2 The Time Restriction Screen

Use this screen to view the schedules and enable parental control on a specific user during certain periods.

Click **Advanced Setup > Parental Control** to open the following screen.

Figure 119 Parental Control > Time restriction

#	Active	username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Modify
1	<input checked="" type="checkbox"/>	Bob	00:a0:c5:01:23:45	x	x	x	x	x			08:00	17:30	

.....

The following table describes the fields in this screen.

Table 76 Parental Control > Time Restriction

LABEL	DESCRIPTION
#	This shows the index number of the schedule.
Active	Select the check box to enable the schedule.
username	This shows the name of the user.
MAC	This shows the MAC address of the LAN user's computer to which this schedule applies.
Mon ~ Sun	x indicates the day(s) on which parental control is enabled.
Start	This shows the time when the schedule starts.
Stop	This shows the time when the schedule ends.
Modify	Click the Edit icon to go to the screen where you can edit the schedule. Click the Remove icon to delete an existing schedule.
Add	Click Add to create a new schedule.
Apply	Click Apply to save your changes back to the ZyXEL Device.

19.2.1 Adding a Schedule

Click the **Add** button in the **Time Restriction** screen to open the following screen. Use this screen to configure a restricted access schedule for a specific user on your network.

Figure 120 Time Restriction Configuration

Add Access Time Restriction

This page adds time of day restriction to a special LAN device connected to the Router. To restrict the LAN device, enter the MAC address of the LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".

User Name

MAC Address

Days of the week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

The following table describes the fields in this screen.

Table 77 Time Restriction Configuration

LABEL	DESCRIPTION
User Name	Enter the name of the user.
MAC Address	Enter the MAC address of the LAN user's computer to which this schedule applies.
Days of the week	Select check boxes for the days that you want the ZyXEL Device to perform parental control.
Start Blocking Time End Blocking Time	Enter the time period of each day, in 24-hour format, during which parental control will be enforced.
Back	Click this button to return to the previous screen without saving any changes.
Save/Apply	Click this button to save your settings back to the ZyXEL Device.

19.3 The URL Filter Screen

Use this screen to configure URL filtering settings to allow or block the users on your network from accessing certain web sites.

Click **Advanced Setup > Parental Control > URL Filter** to open the following screen.

Figure 121 Parental Control > URL Filter

Time Restriction **URL Filter**

URL Filter

A maximum 100 entries can be configured.

☒ Active URL Filter

URL List Type: ☒ Block ☐ Access Only

#	Active	Address	Port	Modify
1	<input checked="" type="checkbox"/>	www.bad.com	80	

The following table describes the fields in this screen.

Table 78 Parental Control > URL Filter

LABEL	DESCRIPTION
Active URL Filter	Select the check box to enable URL filtering on the ZyXEL Device.
URL List Type	If you select Block , the ZyXEL Device prohibits the users from viewing the Web sites with the URLs listed below. If you select Access Only , the ZyXEL Device blocks access to all URLs except ones listed below.
#	This is the index number of the rule.
Active	Select the check box to enable the filtering rule.
Address	This is the URL of the web site in this rule.
Port	This is the port number the web server uses to forward HTTP traffic.
Modify	Click the Edit icon to go to the screen where you can edit the rule. Click the Remove icon to delete an existing rule.
Add	Click Add to create a new rule.
Apply	Click this button to save your settings back to the ZyXEL Device.

19.3.1 Adding URL Filter

Click the **Add** button in the **URL Filter** screen to open the following screen.

Figure 122 URL Filter Configuration

The screenshot shows a web-based configuration interface titled "Add URL Filter". It contains two text input fields. The first is labeled "URL Address:" and the second is labeled "Port Number:". To the right of the "Port Number" field, there is a small text note: "(Default 80 will be applied if leave blank.)". At the bottom of the form, there are two buttons: "Back" and "Save/Apply".

The following table describes the fields in this screen.

Table 79 URL Filter Configuration

LABEL	DESCRIPTION
URL Address	Enter the URL of web site to which the ZyXEL Device blocks or allows access.
Port Number	Specify the port number the web server uses to forward HTTP traffic.
Back	Click this button to return to the previous screen without saving any changes.
Save/Apply	Click this button to save your settings back to the ZyXEL Device.

Interface Group

20.1 Overview

By default, all LAN and WAN interfaces on the ZyXEL Device are in the same group and can communicate with each other. You can create multiple groups to have the ZyXEL Device assign the IP addresses in different domains to different groups. Each group acts as an independent network on the ZyXEL Device.

20.1.1 What You Can Do in this Chapter

The **Interface Group** screen lets you create multiple networks on the ZyXEL Device ([Section 20.2 on page 203](#)).

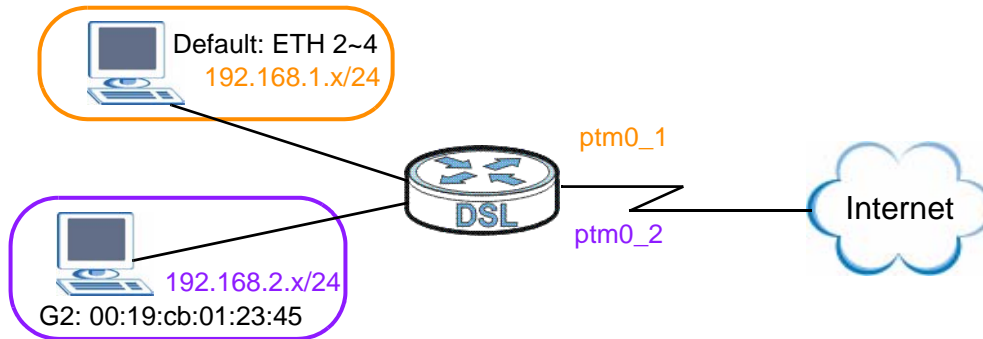
20.2 The Interface Group Screen

You can manually add a LAN interface to a new group. Alternatively, you can have the ZyXEL Device automatically add the incoming traffic and the LAN interface on which traffic is received to the new group when its source MAC address or DHCP option information matches the predefined filtering criteria.

Use the **LAN** screen to configure the private IP addresses the DHCP server on the ZyXEL Device assigns to the clients in the default and/or user-defined groups. If you set the ZyXEL Device to assign IP addresses based on the client's source MAC address or DHCP option information, you must enable DHCP server and configure LAN TCP/IP settings for both the default and user-defined groups. See [Chapter 6 on page 77](#) for more information.

In the following example, the client that sends packets with the source MAC address 00:19:cb:01:23:45 is assigned the IP address 192.168.2.2 and uses the WAN interface ptm0_2.

Figure 123 Interface Grouping Application



Click **Advanced Setup > Interface Group** to open the following screen.

Figure 124 Interface Group

Interface Group					
Interface Group					
#	Group Name	WAN Interface	LAN Interfaces	Criteria	Remove
1	Default	ptm0_1,ppp1_4,ptm0_5	eth0,eth1,eth2,wl0,wl0.1 wl0.2,wl0.3		
2	test	ptm0_2			
3	test_1	ppp0_3	eth3	mac:00:a5:c8:01:23:45	
<input type="button" value="Add"/>					

The following table describes the fields in this screen.

Table 80 Interface Grouping

LABEL	DESCRIPTION
#	This shows the index number of the entry.
Group Name	This shows the descriptive name of the group.
WAN Interface	This shows the WAN interfaces in the group.
LAN Interfaces	This shows the LAN interfaces in the group.
Criteria	This shows the filtering criteria for the group.
Remove	Click the Remove icon to delete the group.
Add	Click this button to create a new group.

20.2.1 Interface Group Configuration

Click the **Add** button in the **Interface Group** screen to open the following screen. Use this screen to create a new interface group.

Note: An interface can belong to a group only.

Figure 125 Interface Group Configuration

General

Group Name:

WAN Interface

WAN Interface used in the grouping:

LAN Interface

Grouped LAN Interfaces

Available LAN Interfaces

eth0
eth1
eth2
wl0_Guest1
wl0_Guest2
wl0_Guest3

Criteria

Automatically Add Clients With the following Criteria

#	Filter Criteria	Remove

Add

Back Apply

The following table describes the fields in this screen.

Table 81 Interface Group Configuration

LABEL	DESCRIPTION
Group Name	Enter a name to identify this group.
WAN Interface used in the grouping	Select a WAN interface to be used in this group. Select No Interface/None to not add a WAN interface to this group.
Grouped LAN Interfaces Available LAN Interfaces	Select a LAN or wireless LAN interface in the Available LAN Interfaces and use the left-facing arrow to move it to the Grouped LAN Interfaces to add the interface to this group. To remove a LAN or wireless LAN interface from the Grouped LAN Interfaces , use the right-facing arrow.
#	This shows the index number of the rule.
Filter Criteria	This shows the filtering criteria. The LAN interface on which the matched traffic is received will belong to this group automatically.
Remove	Click the Remove icon to delete this rule from the ZyXEL Device.
Add	Click this button to create a new rule.

Table 81 Interface Group Configuration (continued)

LABEL	DESCRIPTION
Back	Click this button to return to the previous screen without saving any changes.
Apply	Click this button to save your settings back to the ZyXEL Device.

20.2.2 Interface Grouping Criteria

Click the **Add** button in the **Interface Grouping Configuration** screen to open the following screen.

Figure 126 Interface Grouping Criteria

The screenshot shows the 'Interface Grouping Criteria' configuration screen. It features a title bar 'Criterion' and a list of radio buttons for selection: Source MAC Address, DHCP option 60, DHCP option 61 (selected), IAID, and DHCP option 125. Below each radio button are input fields: Source MAC Address, DHCP option 60, IAID, DHCP option 125 Enterprise Number, Manufacturer OUI, Product Class, Model Name, and Serial Number. There is also a 'DUID type' dropdown menu set to 'DUID-LLT'. At the bottom are 'Back' and 'Apply' buttons.

The following table describes the fields in this screen.

Table 82 Interface Grouping Criteria

LABEL	DESCRIPTION
Source MAC Address	Enter the source MAC address of the packet.
DHCP Option 60	Select this option and enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware.
DHCP Option 61	Select this and enter the device identity of the matched traffic.
IAID	Enter the Identity Association Identifier (IAID) of the device, for example, the WAN connection index number.

Table 82 Interface Grouping Criteria (continued)

LABEL	DESCRIPTION
DUID Type	<p>Select DUID-LLT (DUID Based on Link-layer Address Plus Time) to enter the hardware type, a time value and the MAC address of the device.</p> <p>Select DUID-EN (DUID Assigned by Vendor Based upon Enterprise Number) to enter the vendor's registered enterprise number.</p> <p>Select DUID-LL (DUID Based on Link-layer Address) to enter the device's hardware type and hardware address (MAC address) in the following fields.</p> <p>Select Other to enter any string that identifies the device in the DUID field.</p>
Hardware type	Enter the 16-bit hardware type of the device from which the traffic comes. For example, Ethernet is 1 and Experimental Ethernet is 2.
Time	Enter the time (in seconds since midnight (UTC), January 1, 2000) the DUID is generated.
Link-layer address	Enter the MAC address of the device.
Enterprise number	Enter the vendor's 32-bit enterprise number registered with the IANA (Internet Assigned Numbers Authority).
Identifier	Enter a unique identifier assigned by the vendor.
DUID	Enter the DHCP Unique Identifier (DUID) of the device.
DHCP Option 125	Select this and enter vendor specific information of the matched traffic.
Enterprise number	Enter the vendor's 32-bit enterprise number registered with the IANA (Internet Assigned Numbers Authority).
Manufacturer OUI	Specify the vendor's OUI (Organization Unique Identifier). It is usually the first three bytes of the MAC address.
Product Class	Enter the product class of the device.
Model Name	Enter the model name of the device.
Serial Number	Enter the serial number of the device.
Back	Click this button to return to the previous screen without saving any changes.
Apply	Click this button to save your settings back to the ZyXEL Device.

System Settings

21.1 Overview

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

21.1.1 What You Can Do in this Chapter

- The **General** screen lets you configure system settings ([Section 21.2 on page 209](#)).
- The **Time Setting** screen lets you set the system time ([Section 21.3 on page 210](#)).

21.2 The General Screen

Use the **General** screen to configure system settings such as the system password.

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

Figure 127 Maintenance > System > General

The screenshot shows a web-based configuration interface with two tabs: 'General' (selected) and 'Time Setting'. Under the 'General' tab, there is a section titled 'UserName/Password'. It contains four input fields: 'UserName' (with 'admin' entered), 'Old Password', 'New Password', and 'Retype to Confirm'. Below these fields is a red warning icon and text: 'Caution: Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.' At the bottom of the form are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 83 Maintenance > System > Genera

LABEL	DESCRIPTION
UserName	Type the user name you use to access the system.
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the ZyXEL Device.
Retype to Confirm	Type the new password again for confirmation.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

21.3 The Time Setting Screen

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

Figure 128 Maintenance > System > Time Setting

The screenshot shows the 'Time Setting' configuration page. At the top, there are two tabs: 'General' and 'Time Setting', with 'Time Setting' being the active tab. Below the tabs, the 'Current Time' section displays the current time as 00:44:17 and the current date as 01 Jan 2000. The 'Time and Date Setup' section contains two radio button options: 'Manual' (which is selected) and 'Get from Time Server'. Under the 'Manual' option, there are input fields for 'New Time (hh:mm:ss)' and 'New Date (yyyy/mm/dd)'. Under the 'Get from Time Server' option, there are five dropdown menus for 'First NTP time server', 'Second NTP time server', 'Third NTP time server', 'Fourth NTP time server', and 'Fifth NTP time server'. The 'First NTP time server' is set to 'time.nist.gov', the 'Second NTP time server' is set to 'ntp1.tummy.com', and the others are set to 'None'. There are also empty input fields to the right of these dropdowns. The 'Time zone offset' dropdown is set to '(GMT-08:00) Pacific Time, Tijuana'. At the bottom of the form, there are 'Apply' and 'Cancel' buttons.

The following table describes the fields in this screen.

Table 84 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Current Time	
Current Time	This field displays the time of your ZyXEL Device. Each time you reload this page, the ZyXEL Device synchronizes the time with the time server.
Current Date	This field displays the date of your ZyXEL Device. Each time you reload this page, the ZyXEL Device synchronizes the date with the time server.
Time and Date Setup	
Manual	Select this option to enter the time and date manually.
Get from Time Server	Select this option to have the ZyXEL Device get the time and date from the time server you specified below.
First NTP time server Second NTP time server Third NTP time server Fourth NTP time server Fifth NTP time server	Select an NTP time server from the drop-down list box. Otherwise, select Other and enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Select None if you don't want to configure the time server. Check with your ISP/network administrator if you are unsure of this information.
Time zone offset	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

22.1 Overview

This chapter contains information about configuring general log settings and viewing the ZyXEL Device's logs.

The Web Configurator allows you to choose which categories of events and/or alerts to have the ZyXEL Device log and then display the logs or have the ZyXEL Device send them to a syslog server.

22.1.1 What You Can Do in this Chapter

- The **View Log** screen lets you see the logs for the categories that you selected in the **Log Settings** screen ([Section 22.2 on page 213](#)).
- The **Log Settings** screen lets you configure to where the ZyXEL Device is to send logs and which logs and/or immediate alerts the ZyXEL Device is to record ([Section 22.3 on page 214](#)).

22.2 The View Log Screen

Click **Maintenance > Logs** to open the **View Log** screen. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see [Section 22.3 on page 214](#)).

The log wraps around and deletes the old entries after it fills.

Figure 129 Maintenance > Logs > View Log

#	Date/Time	Severity	System	Message
1	Jan 1 00:53:02	High	System Event	BCM96345 started: BusyBox v1.00 (2009.07.06-04:52+0000)
2	Jan 1 00:53:02	Medium	System Event	kernel: IPSEC SPU: SUCCEEDED
3	Jan 1 00:53:02	Medium	Ethernet	kernel: eth1 Link UP 100 mbps full duplex

The following table describes the fields in this screen.

Table 85 Maintenance > Logs > View Log

LABEL	DESCRIPTION
Display	Select a severity level of logs to view. The ZyXEL Device displays the logs with the severity level equal to or higher than what you selected.
#	This field is a sequential value and is not associated with a specific entry.
Date/Time	This field displays the time the log was recorded.
Severity	This field displays the severity level of the log.
System	This field displays the system module from which the logs come.
Message	This field states the reason for the log.

22.3 The Log Settings Screen

Use the **Log Settings** screen to configure to where the ZyXEL Device is to send logs and which logs and/or immediate alerts the ZyXEL Device is to record and display.

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

Figure 130 Maintenance > Logs > Log Settings

Syslog Logging

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

☒ Active

Log Level: Low

Mode: Both

Syslog Server IP Address: 0.0.0.0

Syslog Server UDP Port: 514

Apply

The following table describes the fields in this screen.

Table 86 Maintenance > Logs > Log Settings

LABEL	DESCRIPTION
Active	Select to enable or disable system logging.
Log Level	Select the severity level of the logs that you want the ZyXEL Device to display, record and send to the log server. The ZyXEL Device displays and records the logs with the severity level equal to or higher than what you selected.
Mode	Select Local to record the logs and store them in the local memory of the ZyXEL Device only. Select Remote to send logs to the specified log server. Select Both to record the logs and store them in the local memory and also send logs to the log server.
Syslog Server IP Address	Enter the server name or the IP address of the log server.
Syslog Server UDP Port	Enter the UDP port of the log server.
Apply	Click Apply to save your customized settings.

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE your ZyXEL Device.

23.1 Overview

This chapter explains how to upload new firmware, manage configuration files and restart your ZyXEL Device.

Use the instructions in this chapter to change the device's configuration file or upgrade its firmware. After you configure your device, you can backup the configuration file to a computer. That way if you later misconfigure the device, you can upload the backed up configuration file to return to your previous settings. You can alternately upload the factory default configuration file if you want to return the device to the original default settings. The firmware determines the device's available features and functionality. You can download new firmware releases from your nearest ZyXEL FTP site (or www.zyxel.com) to use to upgrade your device's performance.

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

23.1.1 What You Can Do in this Chapter

- The **Firmware** screen lets you upload firmware to your device ([Section 23.2 on page 218](#)).
- The **Configuration** screen lets you backup and restore device configurations ([Section 23.3 on page 220](#)). You can also reset your device settings back to the factory default.
- The **Restart** screen lets you restart your ZyXEL Device ([Section 23.4 on page 222](#)).

23.2 The Firmware Screen

Click **Maintenance > Tools** to open the **Firmware** screen. Follow the instructions in this screen to upload firmware to your ZyXEL Device. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

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

Figure 131 Maintenance > Tools > Firmware

Firmware Upgrade

To upgrade the internal router firmware, browse to the location of the binary (.BIN) upgrade file and click **Upload**. Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure.

NOTE: The update process takes about 2 minutes to complete, and the DSL Router will reboot.

Current Firmware Version: **1.00(AWZ.4)b2**

File Path:

The following table describes the labels in this screen.

Table 87 Maintenance > Tools > Firmware

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

After you see the **Firmware Upload in Progress** screen, wait two minutes before logging into the ZyXEL Device again.

Figure 132 Firmware Upload In Progress



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

Figure 133 Network Temporarily Disconnected



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

If the upload was not successful, the following screen will appear. Click **Tools** to go back to the **Firmware** screen.

Figure 134 Error Message



23.3 The Configuration Screen

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

Figure 135 Maintenance > Tools > Configuration

The screenshot shows a web interface with three tabs at the top: 'Firmware', 'Configuration' (which is selected), and 'Restart'. Below the tabs, there are three main sections:

- Backup Configuration**: A section with the instruction 'Click **Backup** to save the current configuration of your system to your computer.' and a single 'Backup' button.
- Restore Configuration**: A section with the instruction 'To restore a previously saved configuration file to your system, browse to the location of the configuration file and click **Upload**.' It includes a 'File Path' input field, a 'Browse...' button, and an 'Upload' button.
- Back to Factory Defaults**: A section with the instruction 'Click **Reset** to clear all user-entered configuration information and return to factory defaults. After resetting, the' followed by a list of default settings:
 - Password will be 1234
 - LAN IP address will be 192.168.1.1
 - DHCP will be reset to serverand a 'Reset' button.

Backup Configuration

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

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

Restore Configuration

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

Table 88 Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse ... to find it.
Browse...	Click Browse... to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click Upload to begin the upload process.

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

After you see a “restore configuration successful” screen, you must then wait one minute before logging into the ZyXEL Device again.

Figure 136 Configuration Upload Successful



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

Figure 137 Network Temporarily Disconnected



If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1). See [Appendix A on page 241](#) for details on how to set up your computer's IP address.

If the upload was not successful, the following screen will appear. Click **Tools > Configuration** to go back to the **Configuration** screen.

Figure 138 Configuration Upload Error



Reset to Factory Defaults

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

Figure 139 Reset Warning Message



You can also press the **RESET** button on the rear panel to reset the factory defaults of your ZyXEL Device. Refer to [Section 1.6 on page 25](#) for more information on the **RESET** button.

23.4 The Restart Screen

System restart allows you to reboot the ZyXEL Device without turning the power off.

Click **Maintenance > Tools > Restart**. Click **Restart** to have the ZyXEL Device reboot. This does not affect the ZyXEL Device's configuration.

Figure 140 Maintenance > Tools > Restart



Diagnostic

24.1 Overview

The **Diagnostic** screens display information to help you identify problems with the ZyXEL Device.

The route between a CO VDSL switch and one of its CPE may go through switches owned by independent organizations. A connectivity fault point generally takes time to discover and impacts subscriber's network access. In order to eliminate the management and maintenance efforts, IEEE 802.1ag is a Connectivity Fault Management (CFM) specification which allows network administrators to identify and manage connection faults. Through discovery and verification of the path, CFM can detect, analyze and isolate connectivity faults in bridged LANs.

24.1.1 What You Can Do in this Chapter

- The **General** screen lets you ping an IP address or trace the route packets take to a host ([Section 24.4 on page 227](#)).
- The **802.1ag** screen lets you perform CFM actions ([Section 24.4 on page 227](#)).

24.2 What You Need to Know

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

How CFM Works

A Maintenance Association (MA) defines a VLAN and associated Maintenance End Point (MEP) ports on the device under a Maintenance Domain (MD) level. An MEP port has the ability to send Connectivity Check Messages (CCMs) and get other MEP ports information from neighbor devices' CCMs within an MA.

CFM provides two tests to discover connectivity faults.

- Loopback test - checks if the MEP port receives its Loop Back Response (LBR) from its target after it sends the Loop Back Message (LBM). If no response is received, there might be a connectivity fault between them.
- Link trace test - provides additional connectivity fault analysis to get more information on where the fault is. If an MEP port does not respond to the source MEP, this may indicate a fault. Administrators can take further action to check and resume services from the fault according to the line connectivity status report.

24.3 The General Diagnostic Screen

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

Figure 141 Maintenance > Diagnostic > General

The screenshot shows a web-based diagnostic tool window. At the top, there's a tab labeled 'General' with a sub-tab '802.1ag'. Below the tabs, the main content area is titled 'General'. It features a large, empty text box with the placeholder text '- Info -'. At the bottom of the window, there's a section for 'TCP/IP Address' with a text input field containing the placeholder 'URL or IP Address'. To the right of the input field are two buttons: 'Ping' and 'Traceroute'.

The following table describes the fields in this screen.

Table 89 Maintenance > Diagnostic > General

LABEL	DESCRIPTION
TCP/IP Address	Type the IP address of a computer that you want to ping in order to test a connection or trace the route packets take to.
Ping	Click this button to ping the IP address that you entered.
Traceoute	Click this button to perform the traceroute function. This determines the path a packet takes to the specified host.

24.4 The 802.1ag Screen

Click **Diagnostic** to open the following screen. Use this screen to perform CFM actions.

Figure 142 802.1ag

The following table describes the fields in this screen.

Table 90 Maintenance > Diagnostic > 802.1ag

LABEL	DESCRIPTION
802.1ag Connectivity Fault Management	
Maintenance Domain (MD) Name	Type a name of up to 39 printable English keyboard characters for this MD. The combined length of the MD Name and MA name must be less or equal to 44bytes.
Maintenance Domain (MD) Level	Select a level (0-7) under which you want to create an MA.
Maintenance Association (MA) Name	Type a name of up to 39 printable English keyboard characters for this MA. The combined length of the MD Name and MA name must be less or equal to 44bytes.

Table 90 Maintenance > Diagnostic > 802.1ag (continued)

LABEL	DESCRIPTION
Maintenance Association (MA) Format	<p>Select the format which the ZyXEL Device uses to send this MA information in the domain (MD). Options are VID, String and Integer.</p> <p>If you select VID or Integer, the ZyXEL Device adds the VLAN ID you specified for an MA in the CCM.</p> <p>If you select String, the ZyXEL Device adds the MA name you specified above in the CCM.</p> <p>Note: The MEPs in the same MA should use the same MA format.</p>
Destination MAC Address	Enter the target device's MAC address to which the ZyXEL Device performs a CFM loopback test.
Count	Set how many times the ZyXEL Device send loopback messages (LBMs).
802.1Q VLAN ID	Type a VLAN ID (0-4095) for this MA.
Maintenance End Point ID	Enter an ID number (1-8191) for this MEP port. Each MEP port needs a unique ID number within an MD. The MEP ID is to identify an MEP port used when you perform a CFM action
Status	
Continuity Check Message (CCM)	This shows how many Connectivity Check Messages (CCMs) are sent and if there is any invalid CCM or cross-connect CCM.
Loopback Message (LBM)	This shows how many Loop Back Messages (LBMs) are sent and if there is any in order or out of order Loop Back Response (LBR) received from a remote MEP.
Linktrace Message (LTM)	This shows the destination MAC address in the Link Trace Response (LTR).
Save	Click this to save your changes back to the ZyXEL Device.
Enable CCM	Click this button to have the selected MEP send Connectivity Check Messages (CCMs) to other MEPs.
Disable CCM	Click this button to disallow the selected MEP to send Connectivity Check Messages (CCMs) to other MEPs.
Update CC status	Click this button to reload the test result.
Send Loopback	Click this button to have the selected MEP send the LBM (Loop Back Message) to a specified remote end point.
Send Linktrace	Click this button to have the selected MEP send the LTMs (Link Trace Messages) to a specified remote end point.

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- [Power, Hardware Connections, and LEDs](#)
- [ZyXEL Device Access and Login](#)
- [Internet Access](#)

25.1 Power, Hardware Connections, and LEDs

The ZyXEL Device does not turn on. None of the LEDs turn on.

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

One of the LEDs does not behave as expected.

- 1 Make sure you understand the normal behavior of the LED. See [Section 1.5 on page 24](#).

- 2 Check the hardware connections. See the Quick Start Guide.
- 3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.
- 4 Turn the ZyXEL Device off and on.
- 5 If the problem continues, contact the vendor.

25.2 ZyXEL Device Access and Login

I forgot the IP address for the ZyXEL Device.

- 1 The default IP address is **192.168.1.1**.
- 2 If you changed the IP address and have forgotten it, you might get the IP address of the ZyXEL Device by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the ZyXEL Device (it depends on the network), so enter this IP address in your Internet browser.
- 3 If this does not work, you have to reset the device to its factory defaults. See [Section 1.6 on page 25](#).

I forgot the password.

- 1 The default password is **1234**.
- 2 If this does not work, you have to reset the device to its factory defaults. See [Section 1.6 on page 25](#).

I cannot see or access the **Login** screen in the Web Configurator.

- 1 Make sure you are using the correct IP address.
 - The default IP address is [192.168.1.1](#).

- If you changed the IP address ([Section on page 82](#)), use the new IP address.
 - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for [I forgot the IP address for the ZyXEL Device](#).
- 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
 - 3 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled. See [Appendix B on page 271](#).
 - 4 Reset the device to its factory defaults, and try to access the ZyXEL Device with the default IP address. See [Section 1.6 on page 25](#).
 - 5 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- If your computer is connected wirelessly, use a computer that is connected to a **ETHERNET** port.

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

- 1 Make sure you have entered the user name and password correctly. The default user name is **admin** and password is **1234**. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 2 Turn the ZyXEL Device off and on.
- 3 If this does not work, you have to reset the device to its factory defaults. See [Section 25.1 on page 229](#).

25.3 Internet Access

I cannot access the Internet.

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 1.5 on page 24](#).

- 2 Make sure you entered your ISP account information correctly in the WAN screens. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 3 If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.
- 4 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
- 5 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the ZyXEL Device), but my Internet connection is not available anymore.

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 1.5 on page 24](#).
- 2 Turn the ZyXEL Device off and on.
- 3 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

- 1 There might be a lot of traffic on the network. Look at the LEDs, and check [Section 1.5 on page 24](#). If the ZyXEL Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
- 2 Check the signal strength. If the signal strength is low, try moving your computer closer to the ZyXEL Device if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).
- 3 Turn the ZyXEL Device off and on.
- 4 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

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

Product Specifications

The following tables summarize the ZyXEL Device's hardware and firmware features.

26.1 Hardware Specifications

Table 91 Hardware Specifications

Dimensions	189 (W) x 132 (D) x 40 (H) mm
Weight	357 g
Power Specification	12 V DC 1A
Built-in Switch	Four auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports
RESET Button	Restores factory defaults
Antenna (wireless devices only)	One attached external dipole antenna, 3dBi
WPS Button (wireless devices only)	1 second: turn on or off WLAN 5 seconds: enable WPS (Wi-Fi Protected Setup)
Operation Temperature	0° C ~ 40° C
Storage Temperature	-20° ~ 60° C
Operation Humidity	20% ~ 85% RH
Storage Humidity	20% ~ 90% RH

26.2 Firmware Specifications

Table 92 Firmware Specifications

Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)

Table 92 Firmware Specifications (continued)

Default User Name	admin
Default Password	1234
DHCP Server IP Pool	192.168.1.33 to 192.168.1.254
Static Routes	16
Device Management	Use the Web Configurator to easily configure the rich range of features on the ZyXEL Device.
Wireless Functionality (wireless devices only)	Allow the IEEE 802.11b and/or IEEE 802.11g wireless clients to connect to the ZyXEL Device wirelessly. Enable wireless security (WEP, WPA(2), WPA(2)-PSK) and/or MAC filtering to protect your wireless network.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the Web Configurator to put it on the ZyXEL Device. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the ZyXEL Device's configuration. You can put it back on the ZyXEL Device later if you decide to revert back to an earlier configuration.
Port Forwarding	If you have a server (mail or web server for example) on your network, you can use this feature to let people access it from the Internet.
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the ZyXEL Device assign IP addresses, an IP default gateway and DNS servers to computers on your network. Your device can also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients.
Dynamic DNS Support	With Dynamic DNS (Domain Name System) support, you can use a fixed URL, www.zyxel.com for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.
IP Multicast	IP multicast is used to send traffic to a specific group of computers. The ZyXEL Device supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).
Time and Date	Get the current time and date from an external server when you turn on your ZyXEL Device. You can also set the time manually. These dates and times are then used in logs.
Logs	Use logs for troubleshooting. You can send logs from the ZyXEL Device to an external syslog server.
Universal Plug and Play (UPnP)	A UPnP-enabled device can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.
QoS (Quality of Service)	You can efficiently manage traffic on your network by reserving bandwidth and giving priority to certain types of traffic and/or to particular computers.
Remote Management	This allows you to decide whether a service (HTTP or FTP traffic for example) from a computer on a network (LAN or WAN for example) can access the ZyXEL Device.

Table 92 Firmware Specifications (continued)

PPPoE Support (RFC2516)	PPPoE (Point-to-Point Protocol over Ethernet) emulates a dial-up connection. It allows your ISP to use their existing network configuration with newer broadband technologies such as ADSL. The PPPoE driver on your device is transparent to the computers on the LAN, which see only Ethernet and are not aware of PPPoE thus saving you from having to manage PPPoE clients on individual computers.
Other PPPoE Features	PPPoE idle time out PPPoE dial on demand
IP Alias	IP alias allows you to partition a physical network into logical networks over the same Ethernet interface. Your device supports three logical LAN interfaces via its single physical Ethernet interface with the your device itself as the gateway for each LAN network.
Packet Filters	Your device's packet filtering function allows added network security and management.
VDSL Standards	<p>VDSL line coding: ITU-T G.993.2 DMT modulation</p> <p>DSL handshake procedure protocol: ITU-T G.994.1</p> <p>DSL physical layer management protocol: ITU-T G.997.1</p> <p>VDSL band plan: 997 and 998</p> <p>Support U0 band</p> <p>VDSL profiles: 8a, 8b, 8c, 8d, 12a, 12b, 17a</p> <p>VDSL speed: up to 100/50 Mbps@ 700 feet</p> <p>Support Annex A, Annex B and 5-band VDSL2</p> <p>Rate adaptation</p> <p>OLR: Bit Swapping/ SRA (Seamless Rate Adaption)</p> <p>Upstream power back-off (UPBO)</p> <p>VDSL OAM communication channels: Indicator bits (IB) channel, VDSL embedded operations channel (EOC) and VDSL overhead control channel (VOC)</p> <p>PTM Transmission Convergence (PTM-TC)</p> <p>Dual-latency xDSL framing (fast and interleaved)</p> <p>Trellis coding</p> <p>INP capability: At least two symbols protection (INP_MIN = 2), up to 16 symbols (INP_MIN = 16)</p>

Table 92 Firmware Specifications (continued)

Other Protocol Support	PPP (Point-to-Point Protocol) link layer protocol Transparent bridging for unsupported network layer protocols RIP I/RIP II ICMP IP Multicasting IGMP v1 and v2 IGMP Proxy
Management	Embedded Web Configurator Remote Firmware Upgrade Syslog TR-069 TR-064

26.3 Wireless Features (for P-870HW Series only)

Table 93 Wireless Features

External Antenna	The ZyXEL Device is equipped with an attached antenna to provide a clear radio signal between the wireless stations and the access points.
Wireless LAN MAC Address Filtering	Your device can check the MAC addresses of wireless stations against a list of allowed or denied MAC addresses.
WEP Encryption	WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network to help keep network communications private.
Wi-Fi Protected Access	Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security standard. Key differences between WPA and WEP are user authentication and improved data encryption.

Table 93 Wireless Features

WPA2	WPA 2 is a wireless security standard that defines stronger encryption, authentication and key management than WPA.
Other Wireless Features	<p>IEEE 802.11g Compliance</p> <p>Frequency Range: 2.4 GHz ISM Band</p> <p>Advanced Orthogonal Frequency Division Multiplexing (OFDM)</p> <p>Data Rates: 54Mbps, 11Mbps, 5.5Mbps, 2Mbps, and 1 Mbps Auto Fallback</p> <p>WPA2</p> <p>WMM</p> <p>IEEE 802.11i</p> <p>IEEE 802.11e</p> <p>Wired Equivalent Privacy (WEP) Data Encryption 64/128 bit</p> <p>WLAN bridge to LAN</p> <p>Up to 32 MAC Address filters</p> <p>IEEE 802.1x</p> <p>Store up to 32 built-in user profiles using EAP-MD5 (Local User Database)</p> <p>External RADIUS server using EAP-MD5, TLS, TTLS</p>

The following list, which is not exhaustive, illustrates the standards supported in the ZyXEL Device.

Table 94 Standards Supported

STANDARD	DESCRIPTION
RFC 1058	RIP-1 (Routing Information Protocol)
RFC 1112	IGMP v1
RFC 1631	IP Network Address Translator (NAT)
RFC 1661	The Point-to-Point Protocol (PPP)
RFC 1723	RIP-2 (Routing Information Protocol)
RFC 2236	Internet Group Management Protocol, Version 2.
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2766	Network Address Translation - Protocol
IEEE 802.11	Also known by the brand Wi-Fi, denotes a set of Wireless LAN/ WLAN standards developed by working group 11 of the IEEE LAN/MAN Standards Committee (IEEE 802).
IEEE 802.11b	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11g	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11g+	Turbo and Super G modes

Table 94 Standards Supported (continued)

STANDARD	DESCRIPTION
IEEE 802.11d	Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges
IEEE 802.11x	Port Based Network Access Control.
IEEE 802.11e QoS	IEEE 802.11 e Wireless LAN for Quality of Service
ITU-T G.993.2 (VDSL2)	ITU standard that defines VDSL2.
TR-069	DSL Forum Standard for CPE Wan Management.
TR-064	DSL Forum LAN-Side DSL CPE Configuration

Setting Up Your Computer's IP Address

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

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

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

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

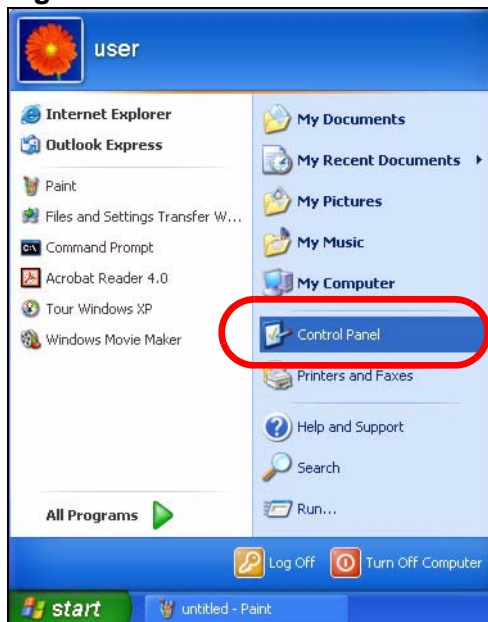
- [Windows XP/NT/2000](#) on [page 242](#)
- [Windows Vista](#) on [page 246](#)
- [Mac OS X: 10.3 and 10.4](#) on [page 251](#)
- [Mac OS X: 10.5](#) on [page 255](#)
- [Linux: Ubuntu 8 \(GNOME\)](#) on [page 258](#)
- [Linux: openSUSE 10.3 \(KDE\)](#) on [page 264](#)

Windows XP/NT/2000

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

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

Figure 143 Windows XP: Start Menu



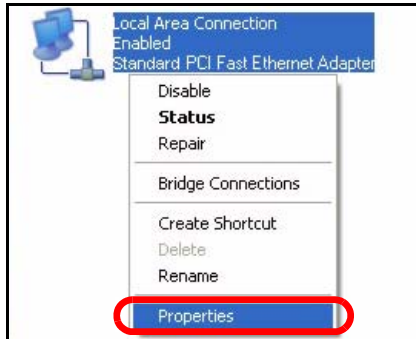
- 2 In the **Control Panel**, click the **Network Connections** icon.

Figure 144 Windows XP: Control Panel



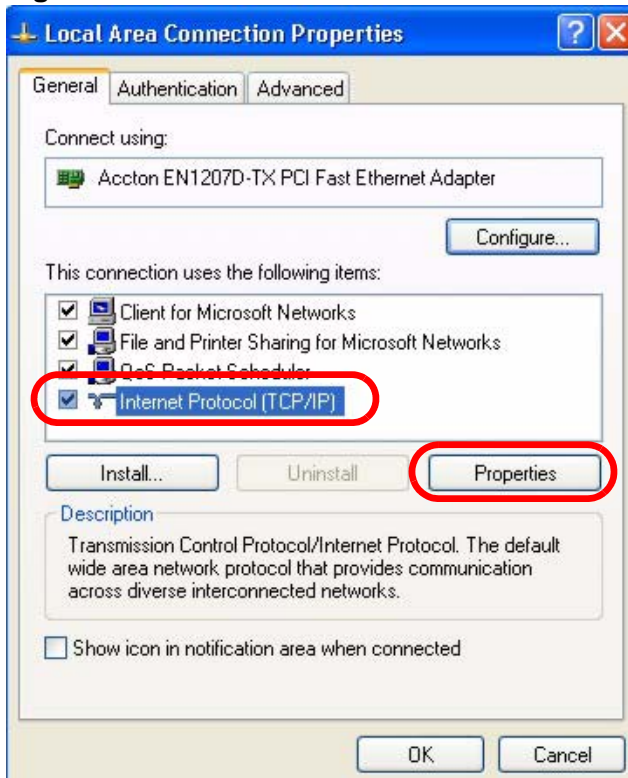
- 3 Right-click **Local Area Connection** and then select **Properties**.

Figure 145 Windows XP: Control Panel > Network Connections > Properties



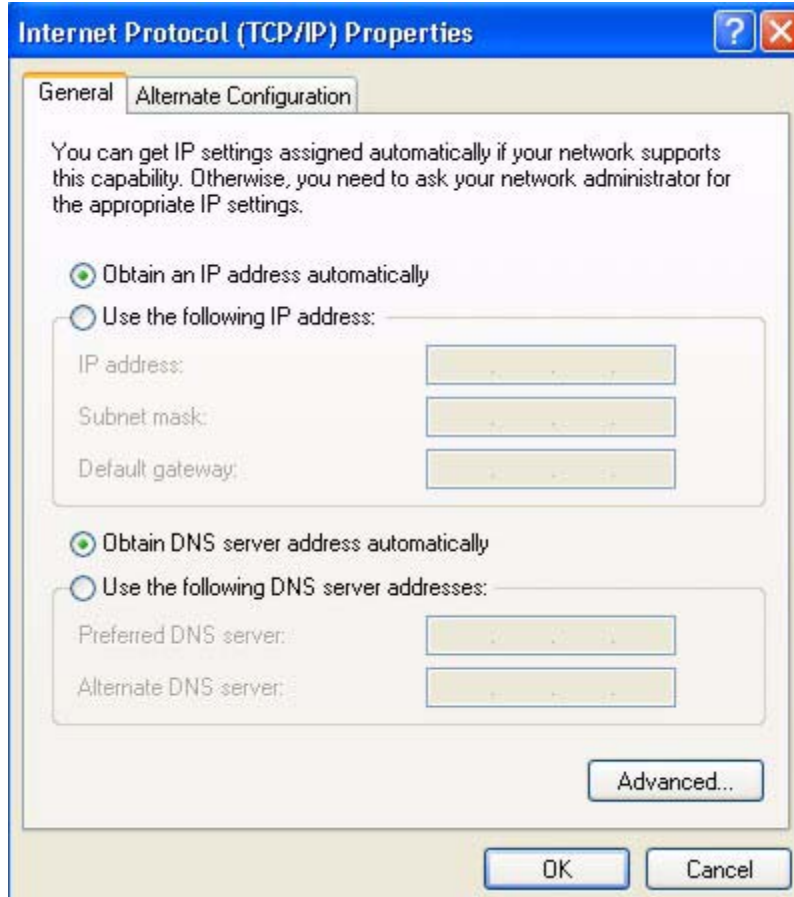
- 4 On the **General** tab, select **Internet Protocol (TCP/IP)** and then click **Properties**.

Figure 146 Windows XP: Local Area Connection Properties



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

Figure 147 Windows XP: Internet Protocol (TCP/IP) Properties



- 6 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server**, if that information was provided.

- 7 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 8 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

- 1 Click **Start > All Programs > Accessories > Command Prompt**.

- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

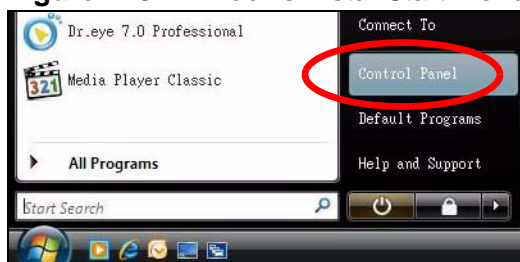
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Windows Vista

This section shows screens from Windows Vista Professional.

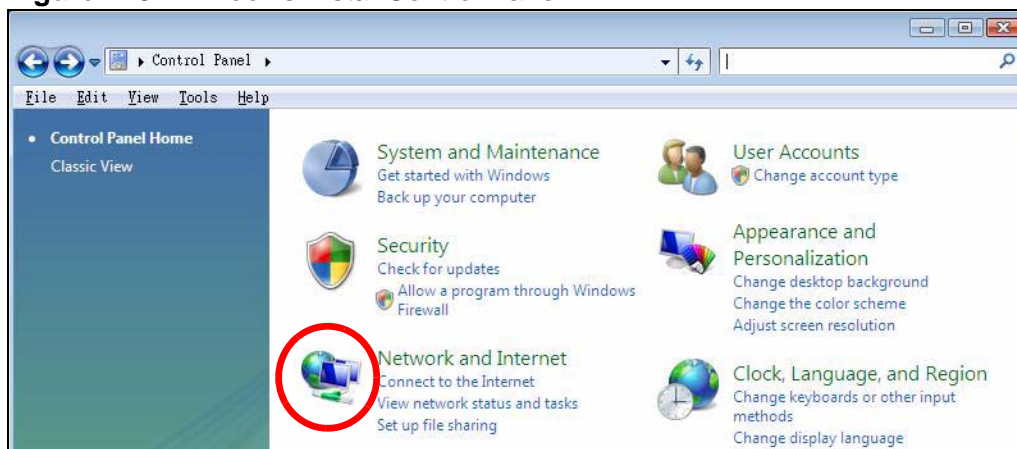
- 1 Click **Start > Control Panel**.

Figure 148 Windows Vista: Start Menu



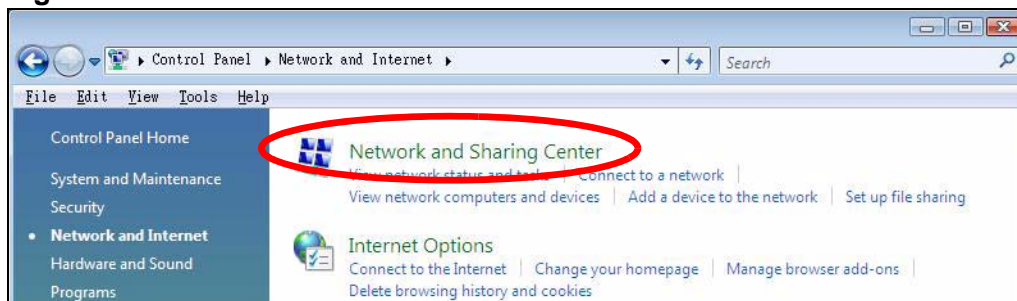
- 2 In the **Control Panel**, click the **Network and Internet** icon.

Figure 149 Windows Vista: Control Panel



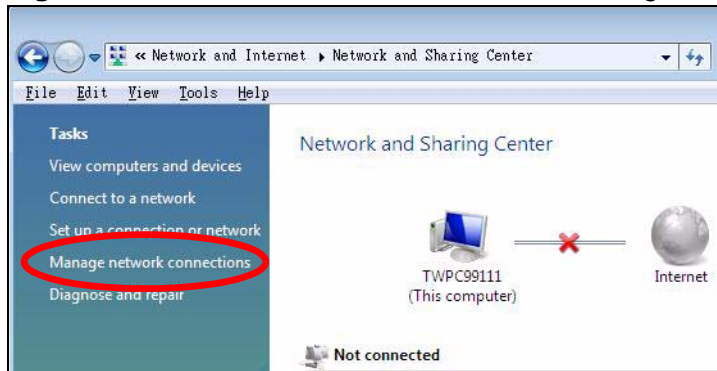
- 3 Click the **Network and Sharing Center** icon.

Figure 150 Windows Vista: Network And Internet



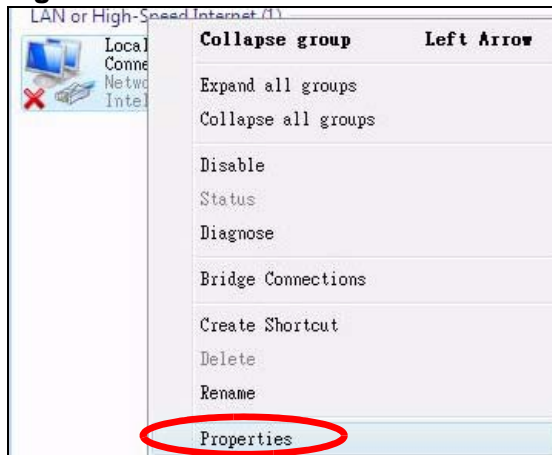
- 4 Click **Manage network connections**.

Figure 151 Windows Vista: Network and Sharing Center



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

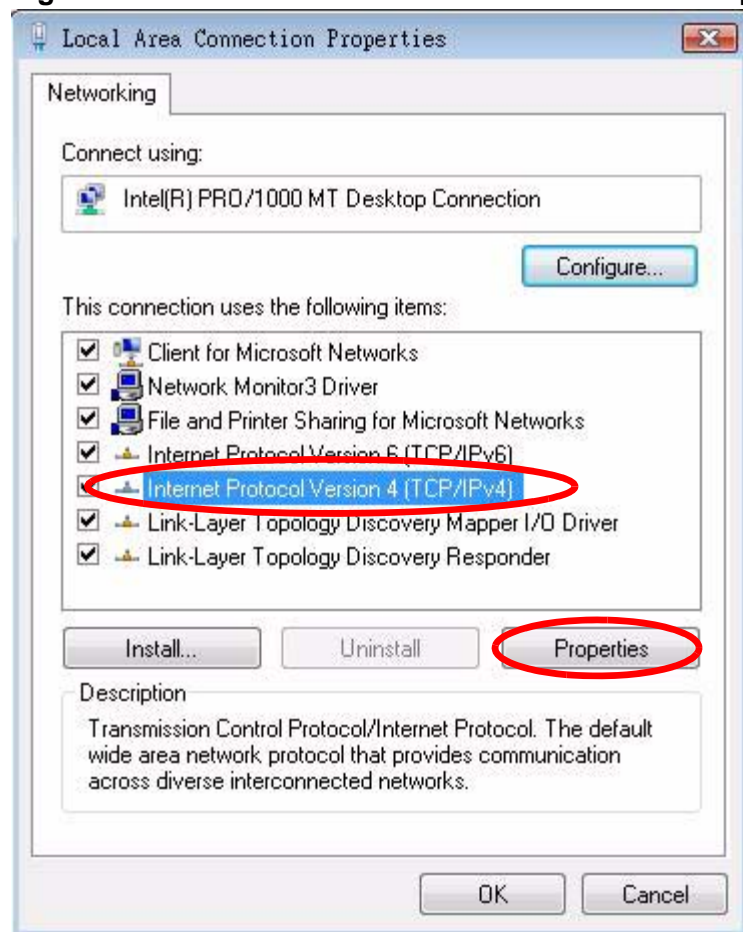
Figure 152 Windows Vista: Network and Sharing Center



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

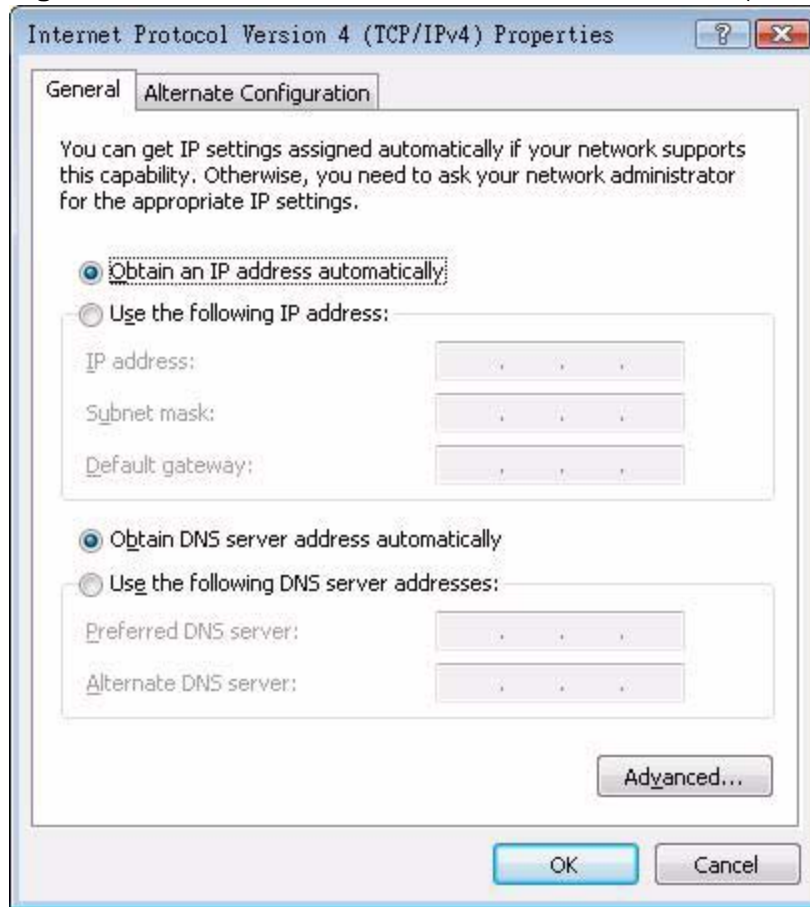
- 6 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

Figure 153 Windows Vista: Local Area Connection Properties



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

Figure 154 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties



- 8 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server**, if that information was provided. Click **Advanced**.

- 9 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 10 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

- 1 Click **Start > All Programs > Accessories > Command Prompt**.

- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

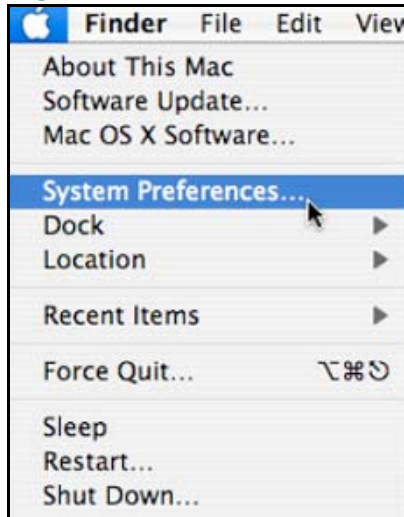
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Mac OS X: 10.3 and 10.4

The screens in this section are from Mac OS X 10.4 but can also apply to 10.3.

- 1 Click **Apple > System Preferences**.

Figure 155 Mac OS X 10.4: Apple Menu



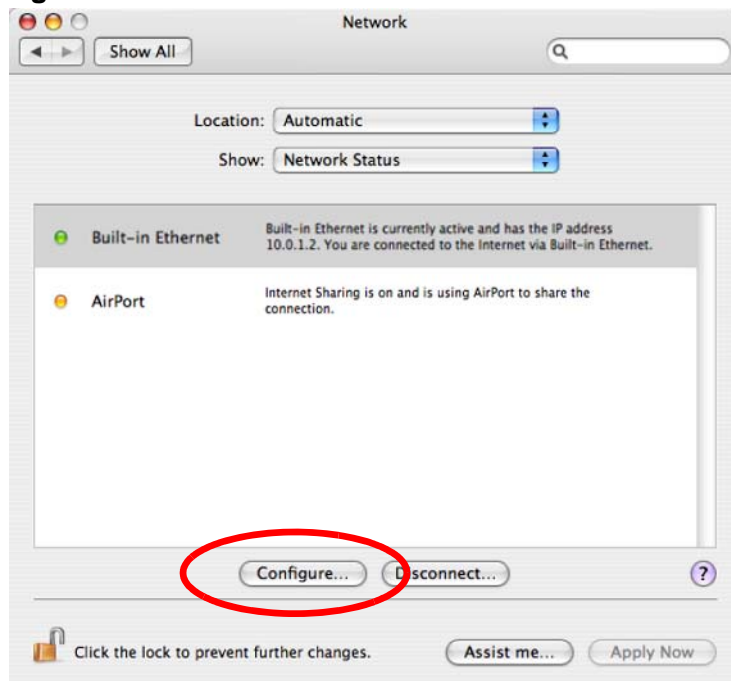
- 2 In the **System Preferences** window, click the **Network** icon.

Figure 156 Mac OS X 10.4: System Preferences



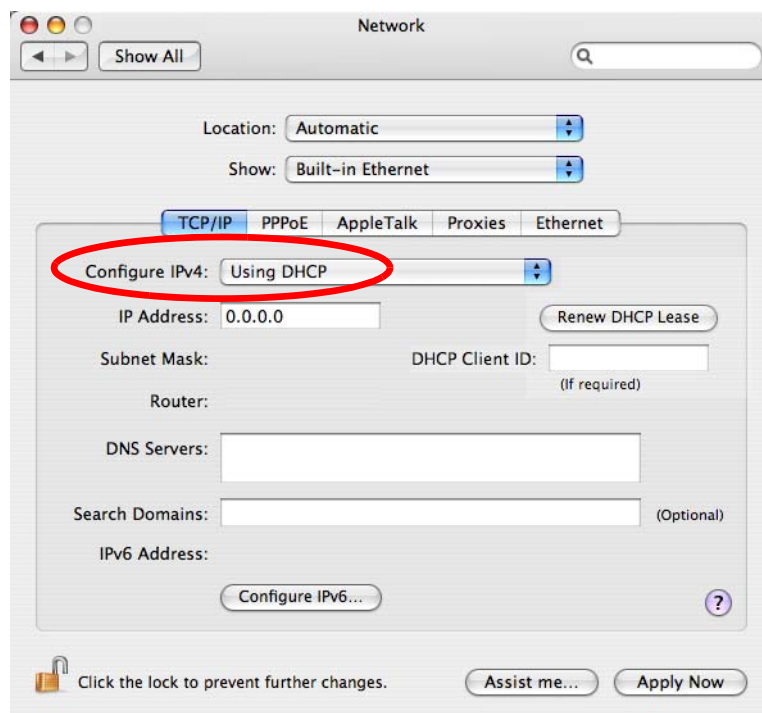
- 3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure**.

Figure 157 Mac OS X 10.4: Network Preferences



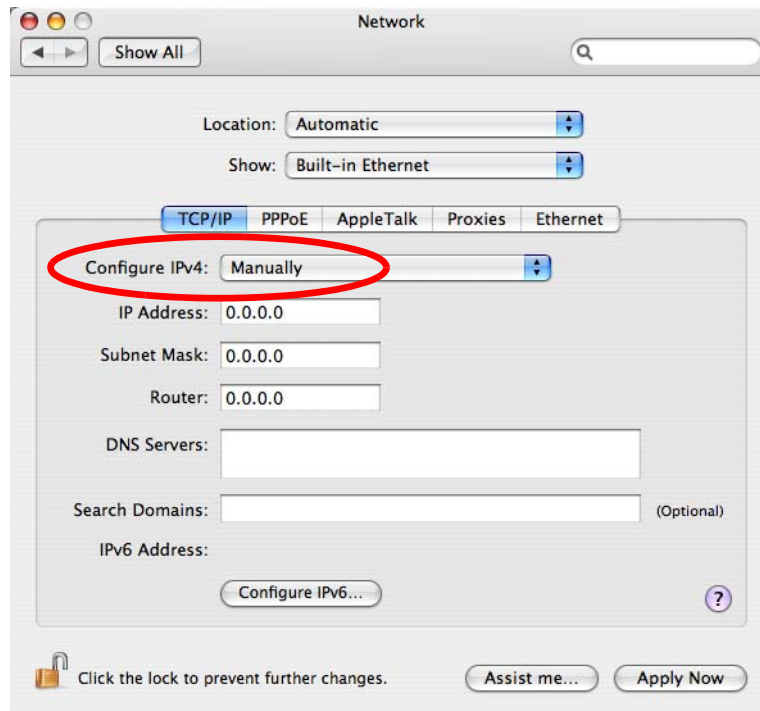
- 4 For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.

Figure 158 Mac OS X 10.4: Network Preferences > TCP/IP Tab.



- 5 For statically assigned settings, do the following:
- From the **Configure IPv4** list, select **Manually**.
 - In the **IP Address** field, type your IP address.
 - In the **Subnet Mask** field, type your subnet mask.
 - In the **Router** field, type the IP address of your device.

Figure 159 Mac OS X 10.4: Network Preferences > Ethernet

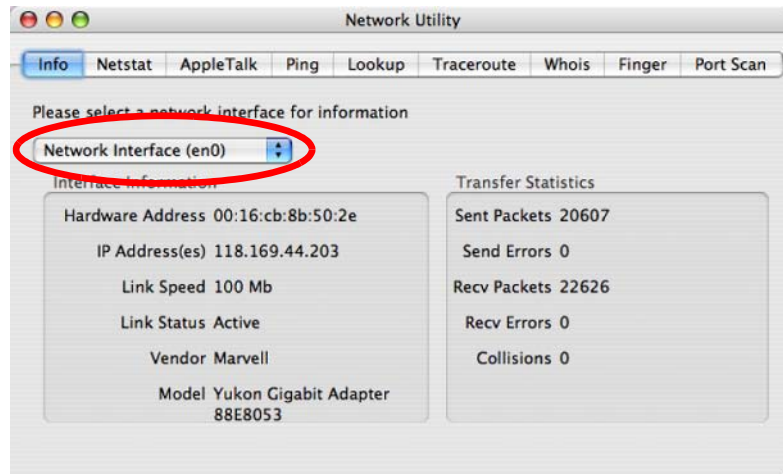


- 6 Click **Apply Now** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network Interface** from the **Info** tab.

Figure 160 Mac OS X 10.4: Network Utility

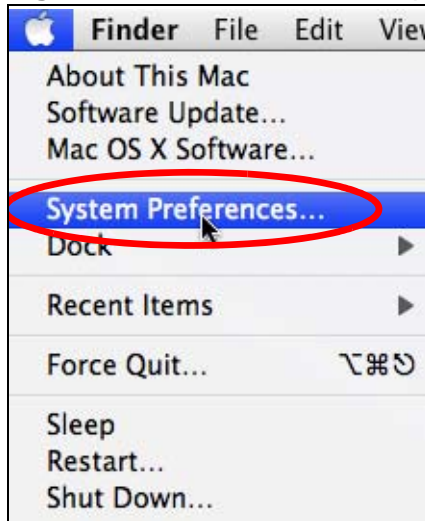


Mac OS X: 10.5

The screens in this section are from Mac OS X 10.5.

- 1 Click **Apple** > **System Preferences**.

Figure 161 Mac OS X 10.5: Apple Menu



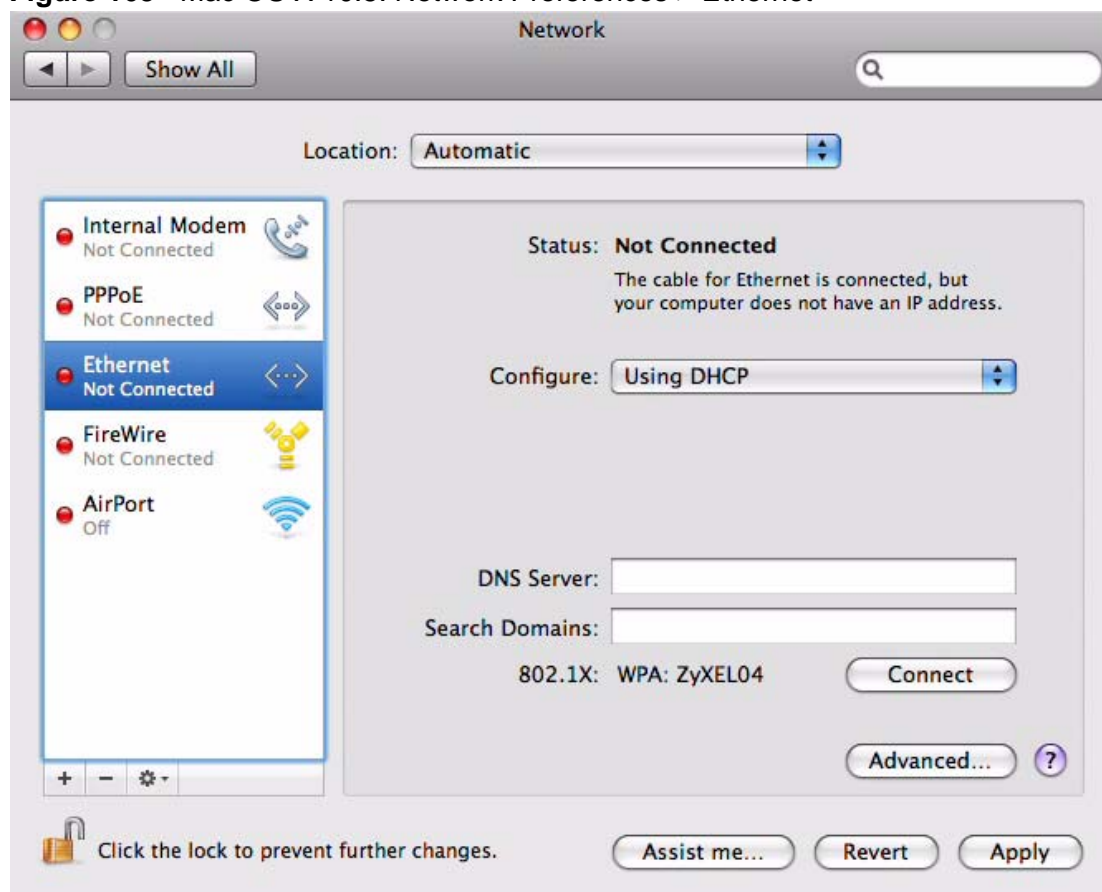
- 2 In **System Preferences**, click the **Network** icon.

Figure 162 Mac OS X 10.5: Systems Preferences



- 3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.

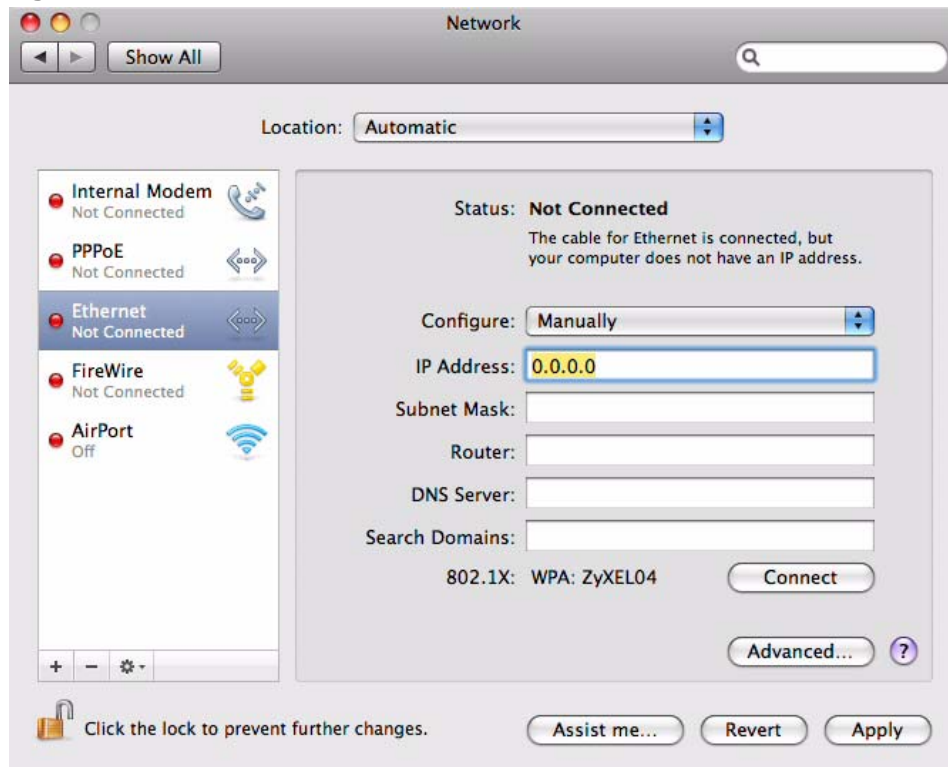
Figure 163 Mac OS X 10.5: Network Preferences > Ethernet



- 4 From the **Configure** list, select **Using DHCP** for dynamically assigned settings.
- 5 For statically assigned settings, do the following:
 - From the **Configure** list, select **Manually**.
 - In the **IP Address** field, enter your IP address.
 - In the **Subnet Mask** field, enter your subnet mask.

- In the **Router** field, enter the IP address of your ZyXEL Device.

Figure 164 Mac OS X 10.5: Network Preferences > Ethernet

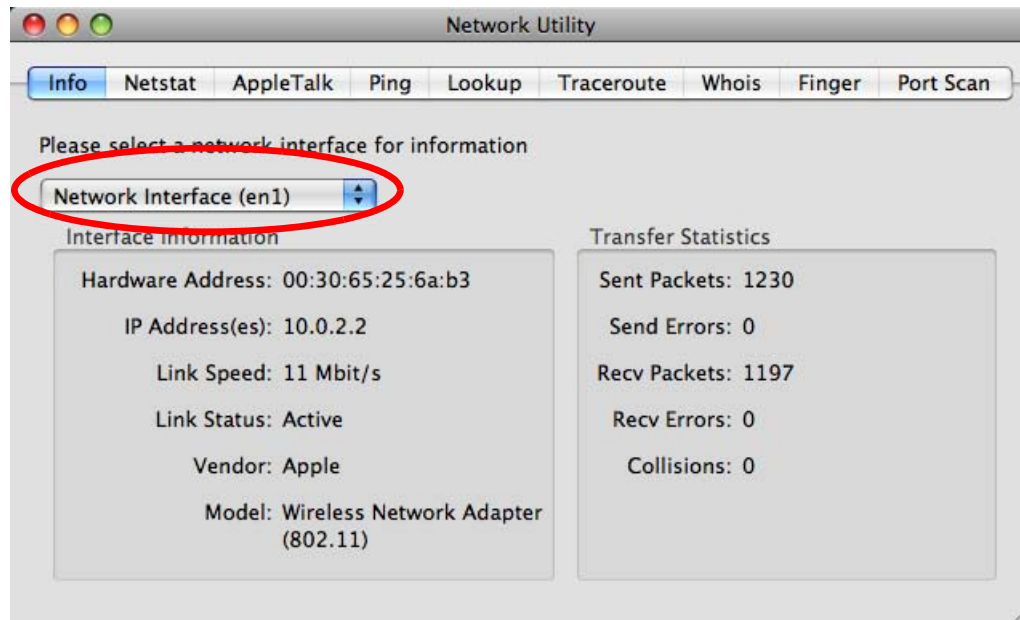


- 6 Click **Apply** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network interface** from the **Info** tab.

Figure 165 Mac OS X 10.5: Network Utility



Linux: Ubuntu 8 (GNOME)

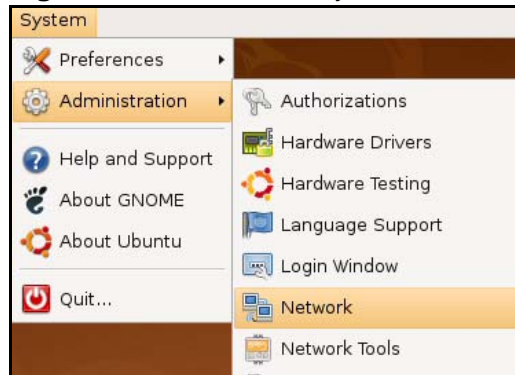
This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default Ubuntu 8 installation.

Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in GNOME:

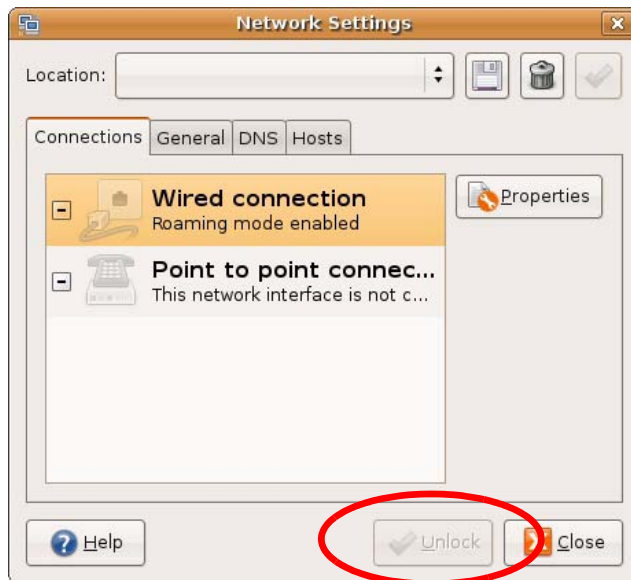
- 1 Click **System > Administration > Network**.

Figure 166 Ubuntu 8: System > Administration Menu



- 2 When the **Network Settings** window opens, click **Unlock** to open the **Authenticate** window. (By default, the **Unlock** button is greyed out until clicked.) You cannot make changes to your configuration unless you first enter your admin password.

Figure 167 Ubuntu 8: Network Settings > Connections



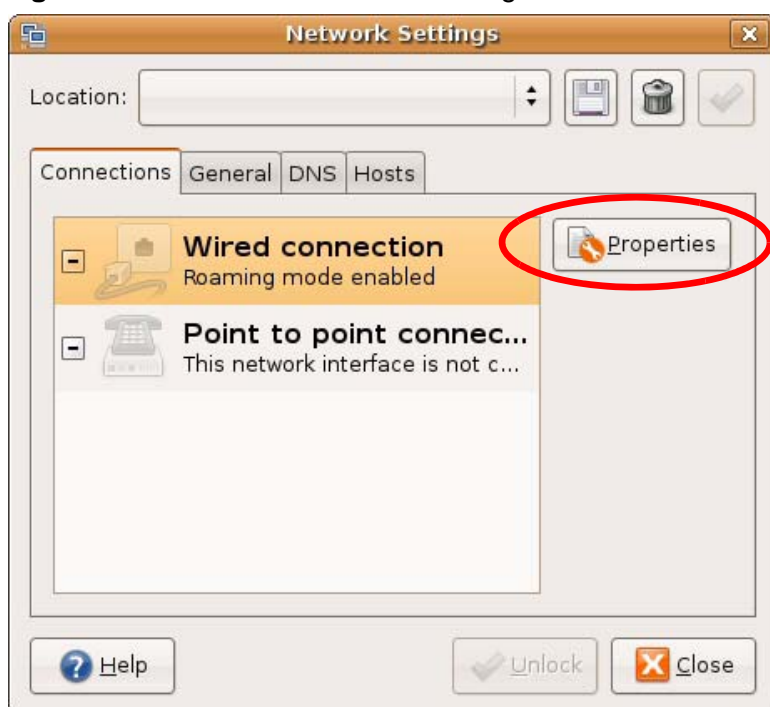
- 3 In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.

Figure 168 Ubuntu 8: Administrator Account Authentication



- 4 In the **Network Settings** window, select the connection that you want to configure, then click **Properties**.

Figure 169 Ubuntu 8: Network Settings > Connections



- 5 The **Properties** dialog box opens.

Figure 170 Ubuntu 8: Network Settings > Properties



- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
 - In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.
- 6 Click **OK** to save the changes and close the **Properties** dialog box and return to the **Network Settings** screen.

- 7 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Settings** window and then enter the DNS server information in the fields provided.

Figure 171 Ubuntu 8: Network Settings > DNS



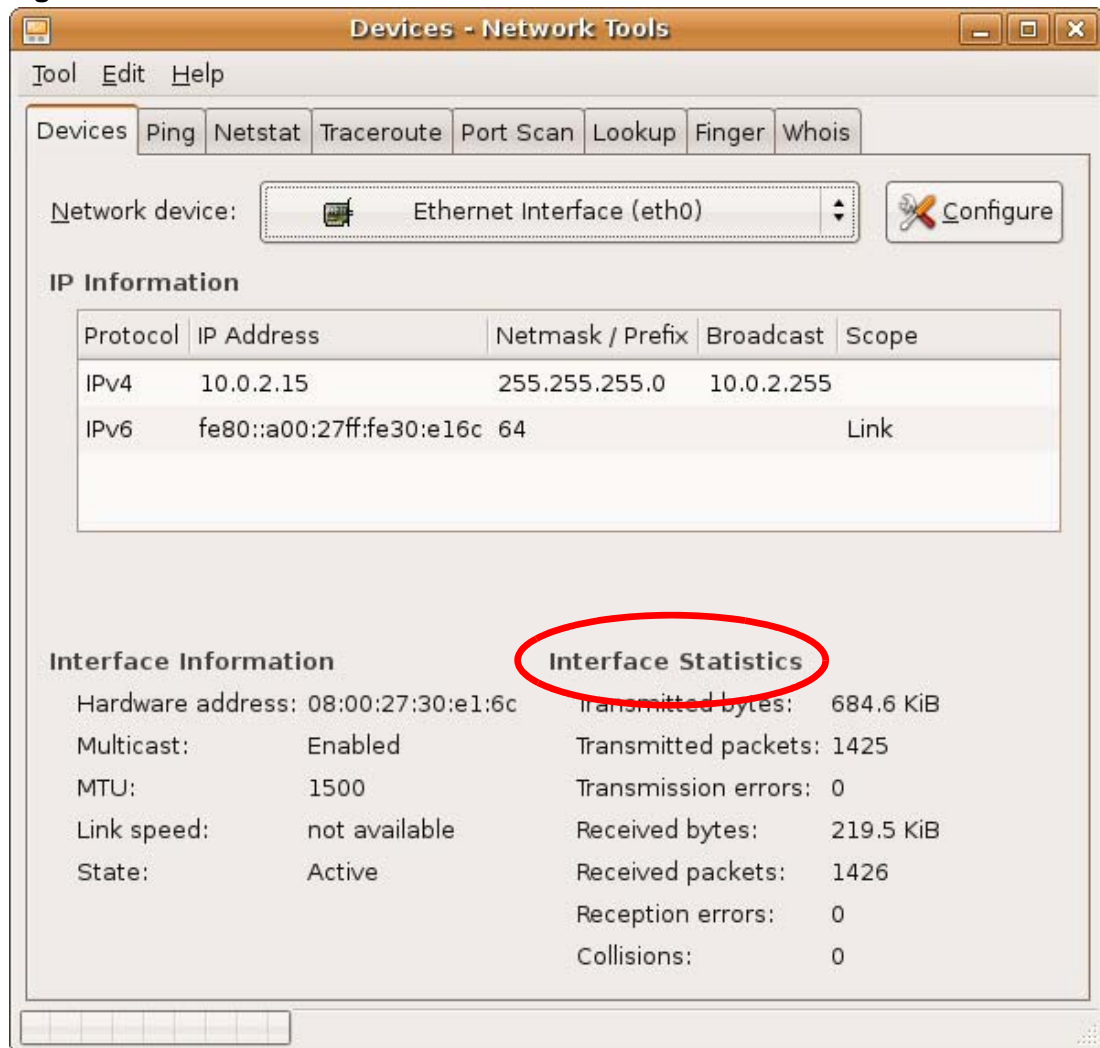
- 8 Click the **Close** button to apply the changes.

Verifying Settings

Check your TCP/IP properties by clicking **System > Administration > Network Tools**, and then selecting the appropriate **Network device** from the **Devices**

tab. The **Interface Statistics** column shows data if your connection is working properly.

Figure 172 Ubuntu 8: Network Tools



Linux: openSUSE 10.3 (KDE)

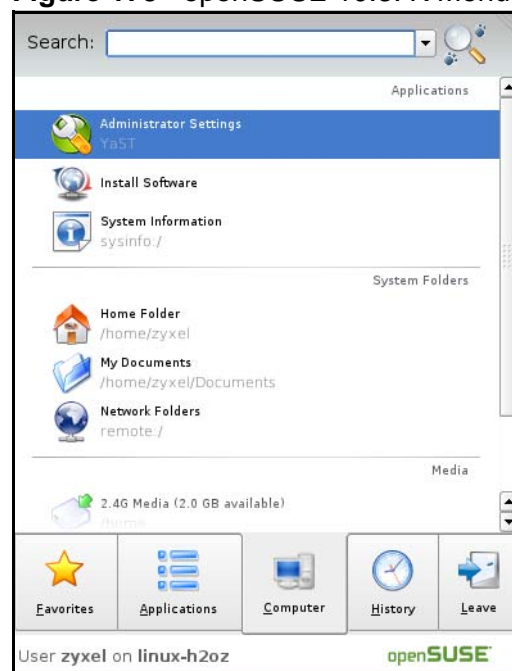
This section shows you how to configure your computer's TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default openSUSE 10.3 installation.

Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in the KDE:

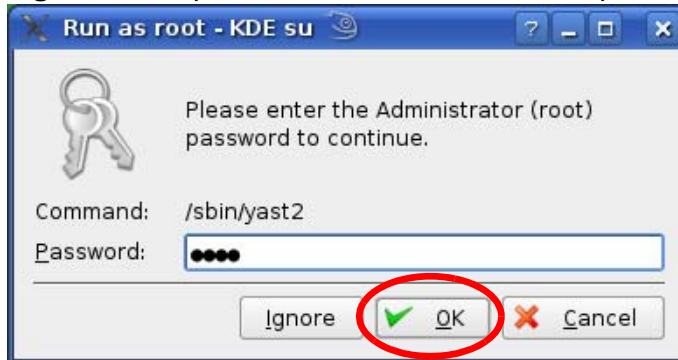
- 1 Click **K Menu > Computer > Administrator Settings (YaST)**.

Figure 173 openSUSE 10.3: K Menu > Computer Menu



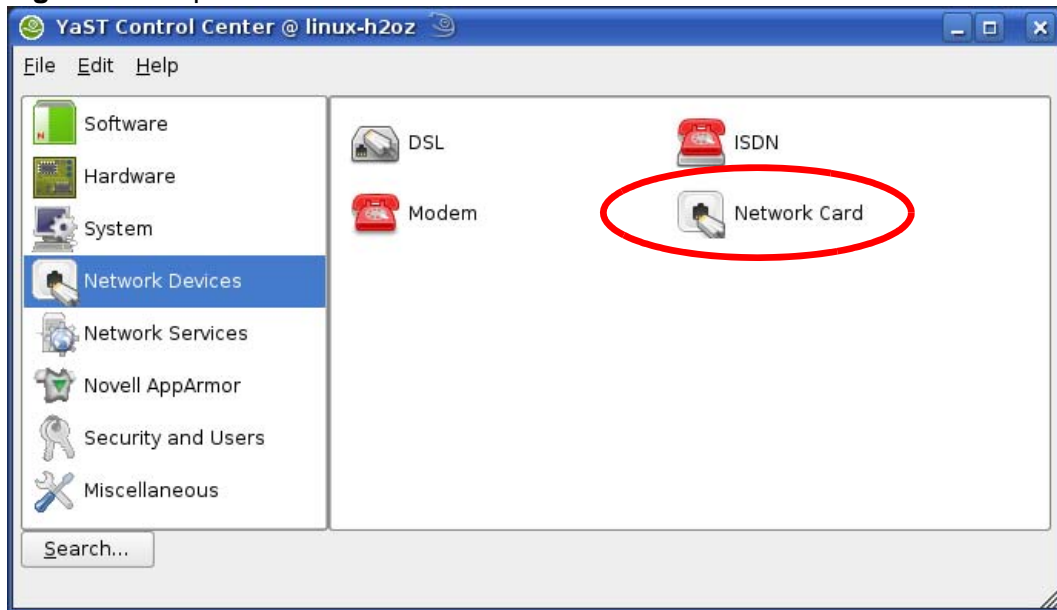
- 2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.

Figure 174 openSUSE 10.3: K Menu > Computer Menu



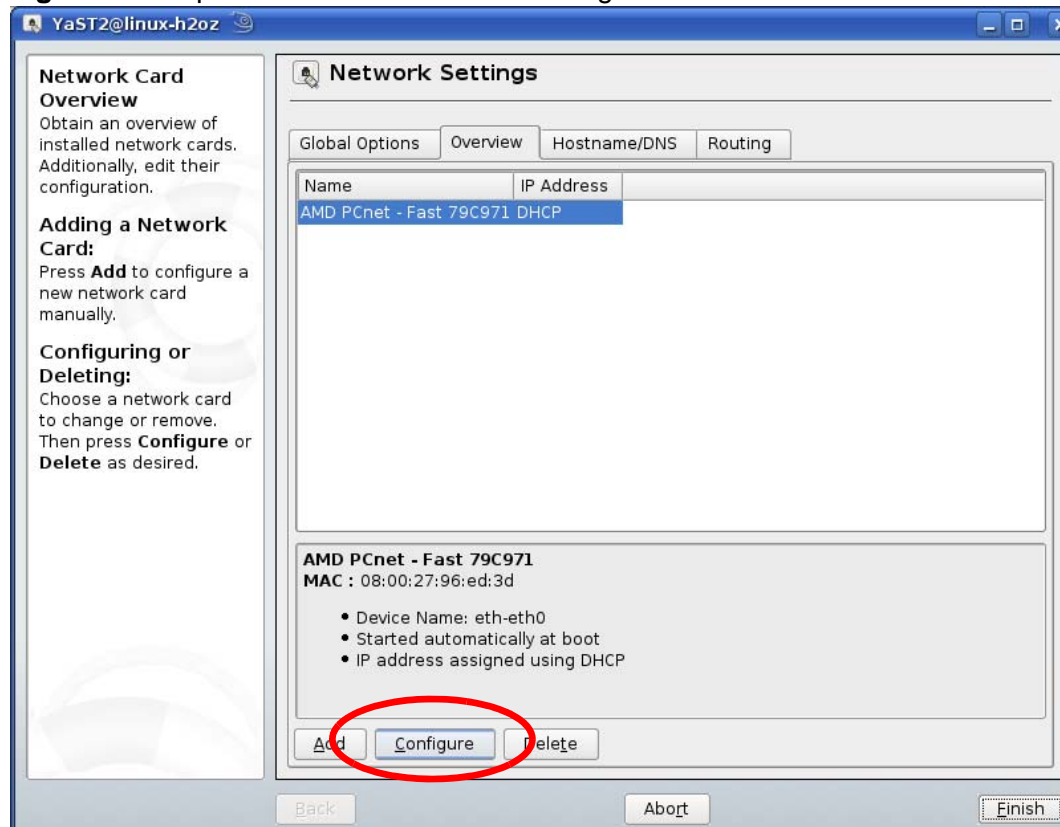
- 3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.

Figure 175 openSUSE 10.3: YaST Control Center



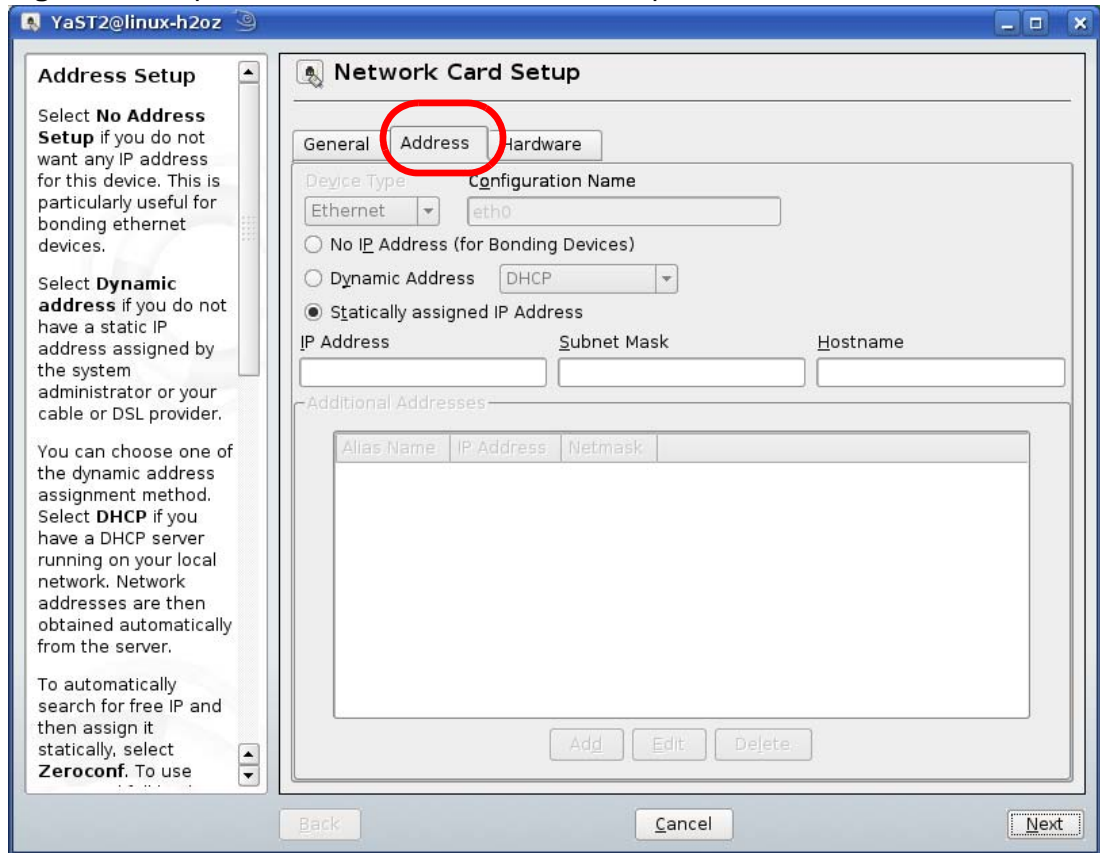
- 4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.

Figure 176 openSUSE 10.3: Network Settings



- 5 When the **Network Card Setup** window opens, click the **Address** tab

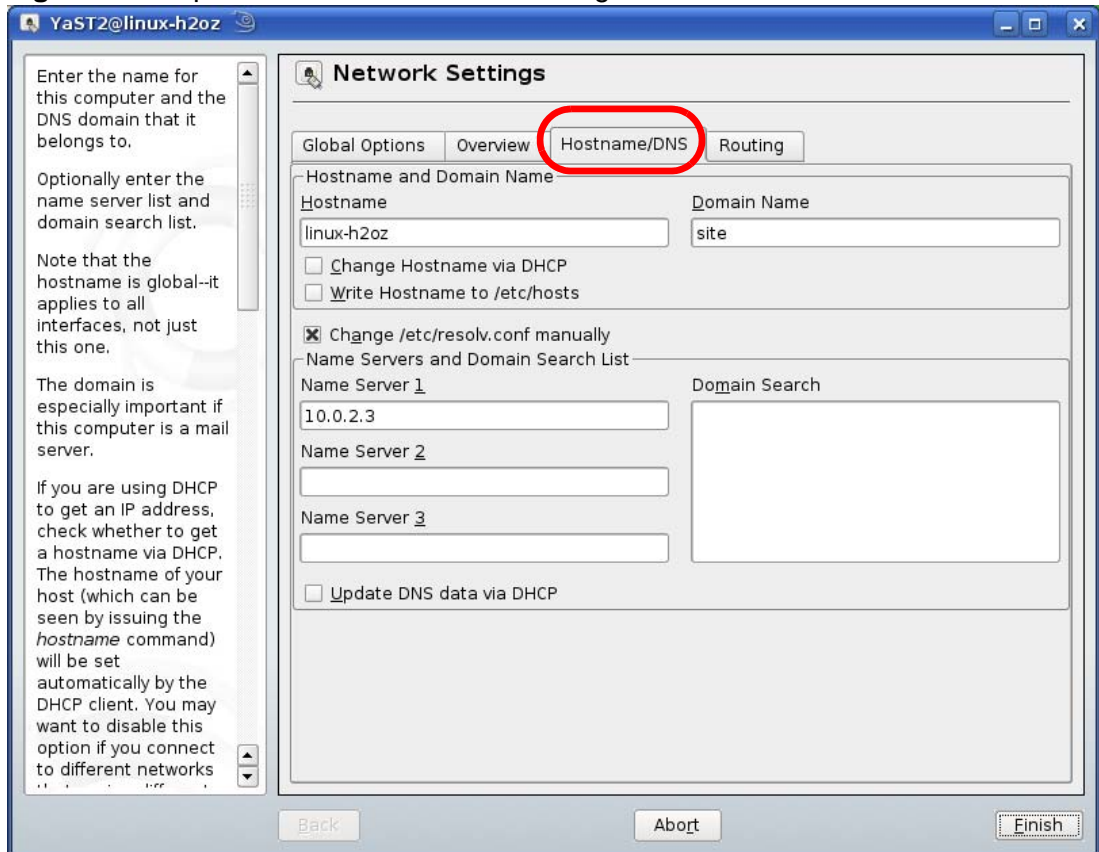
Figure 177 openSUSE 10.3: Network Card Setup



- 6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.
- Select **Statically assigned IP Address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Hostname** fields.
- 7 Click **Next** to save the changes and close the **Network Card Setup** window.

- 8 If you know your DNS server IP address(es), click the **Hostname/DNS** tab in **Network Settings** and then enter the DNS server information in the fields provided.

Figure 178 openSUSE 10.3: Network Settings

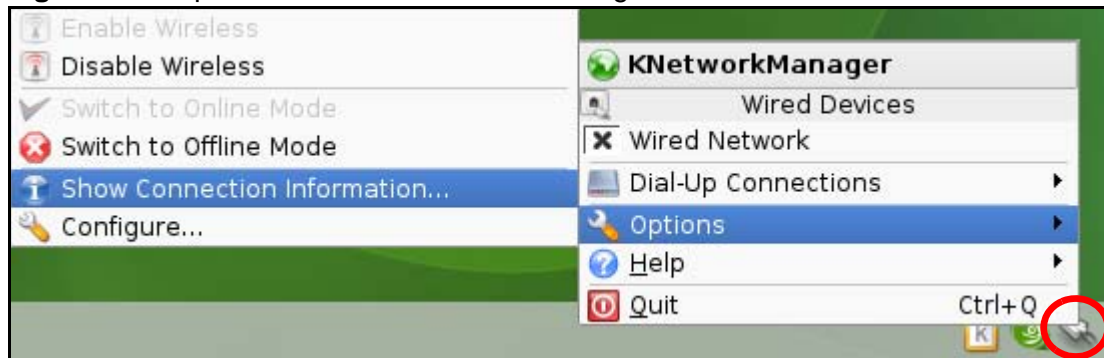


- 9 Click **Finish** to save your settings and close the window.

Verifying Settings

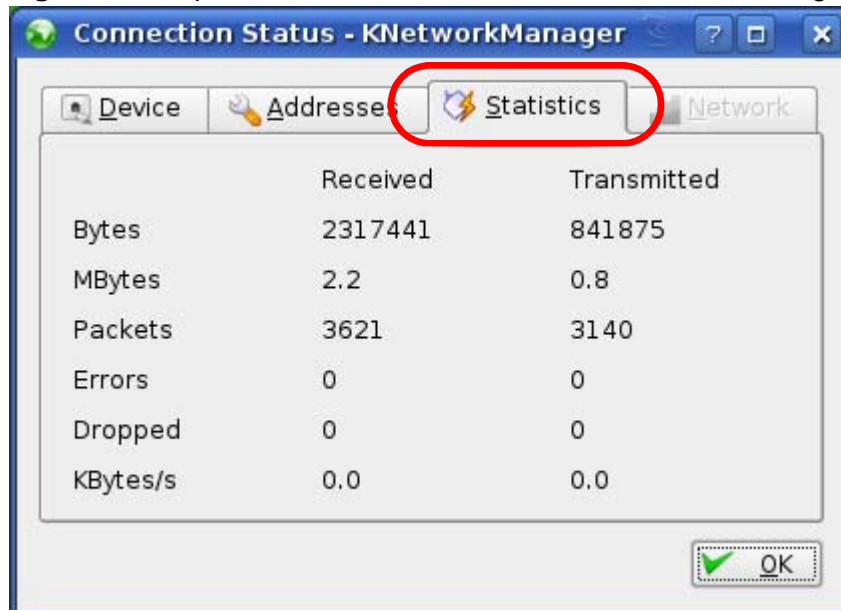
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 179 openSUSE 10.3: KNetwork Manager



When the **Connection Status - KNetwork Manager** window opens, click the **Statistics** tab to see if your connection is working properly.

Figure 180 openSUSE: Connection Status - KNetwork Manager



Pop-up Windows, JavaScript and Java Permissions

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

- Web browser pop-up windows from your device.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

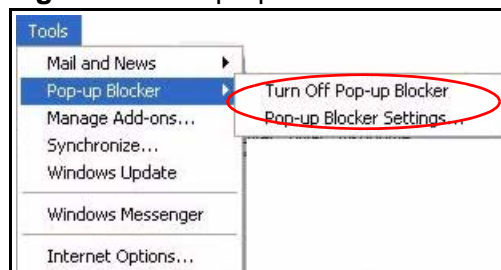
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable Pop-up Blockers

- 1 In Internet Explorer, select **Tools, Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 181 Pop-up Blocker



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

- 1 In Internet Explorer, select **Tools, Internet Options, Privacy**.
- 2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 182 Internet Options: Privacy



- 3 Click **Apply** to save this setting.

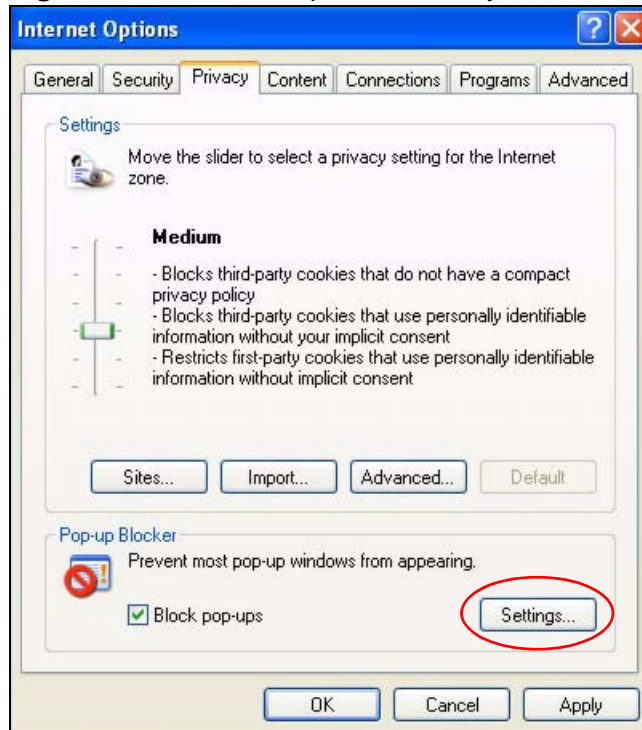
Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

- 1 In Internet Explorer, select **Tools, Internet Options** and then the **Privacy** tab.

- 2 Select **Settings...** to open the **Pop-up Blocker Settings** screen.

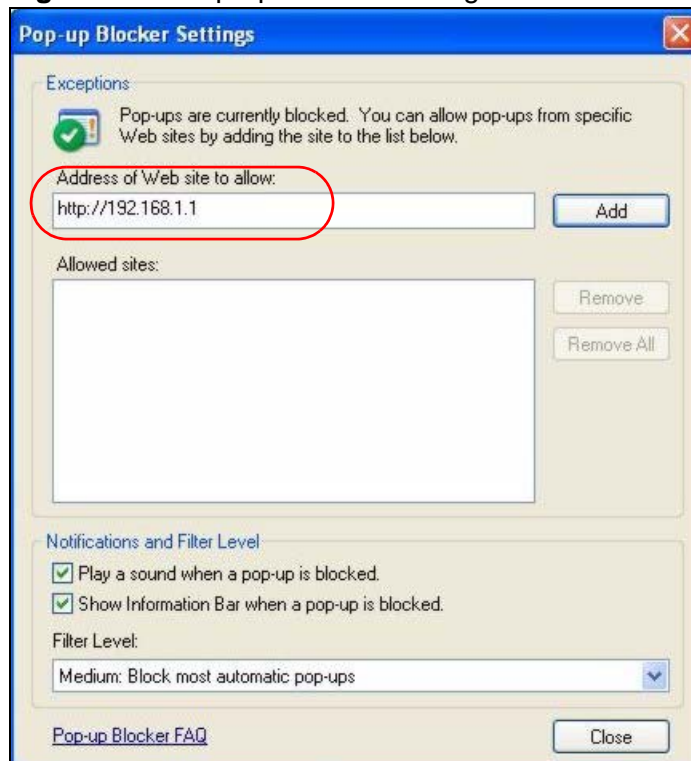
Figure 183 Internet Options: Privacy



- 3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.167.1.

- 4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 184 Pop-up Blocker Settings



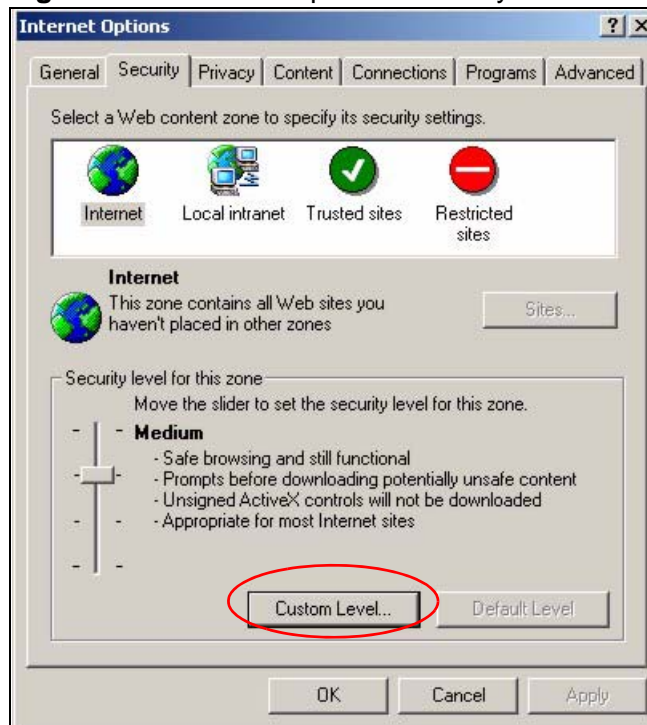
- 5 Click **Close** to return to the **Privacy** screen.
- 6 Click **Apply** to save this setting.

JavaScript

If pages of the Web Configurator do not display properly in Internet Explorer, check that JavaScript are allowed.

- 1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

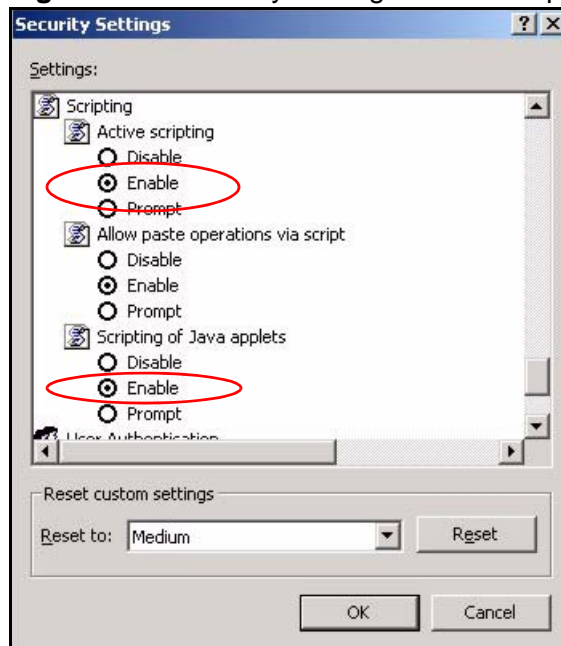
Figure 185 Internet Options: Security



- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Scripting**.
- 4 Under **Active scripting** make sure that **Enable** is selected (the default).
- 5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

- 6 Click **OK** to close the window.

Figure 186 Security Settings - Java Scripting

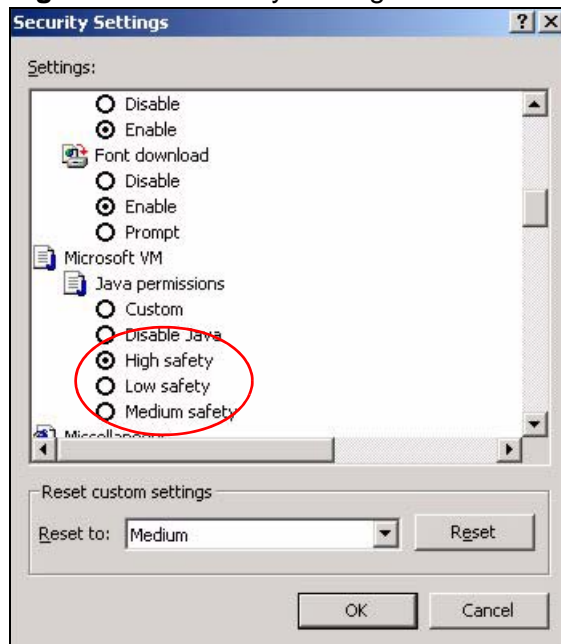


Java Permissions

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Microsoft VM**.
- 4 Under **Java permissions** make sure that a safety level is selected.

- 5 Click **OK** to close the window.

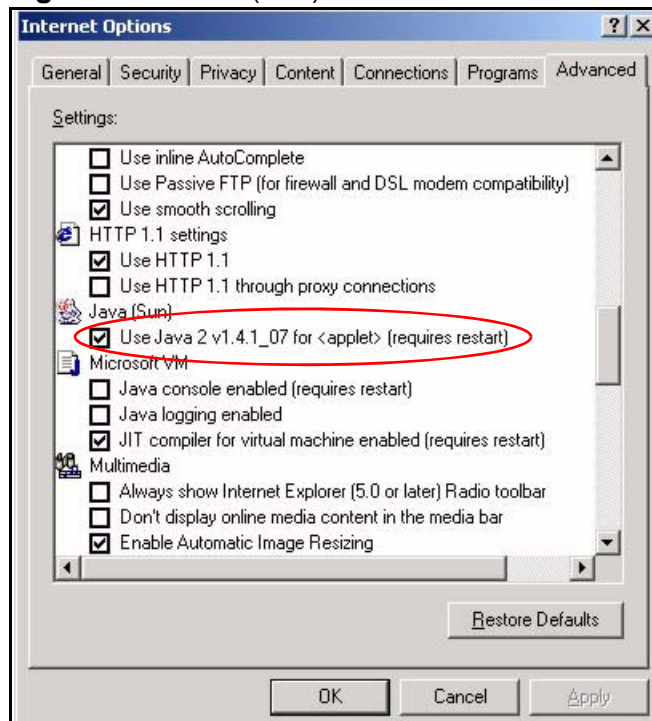
Figure 187 Security Settings - Java



JAVA (Sun)

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Advanced** tab.
- 2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

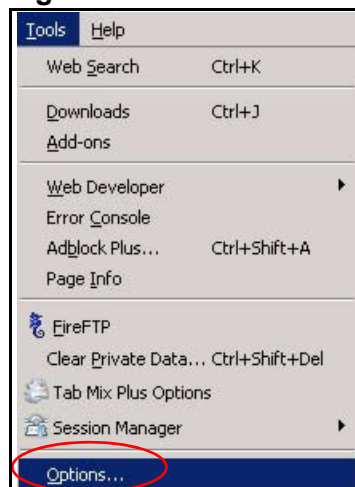
- 3 Click **OK** to close the window.

Figure 188 Java (Sun)

Mozilla Firefox

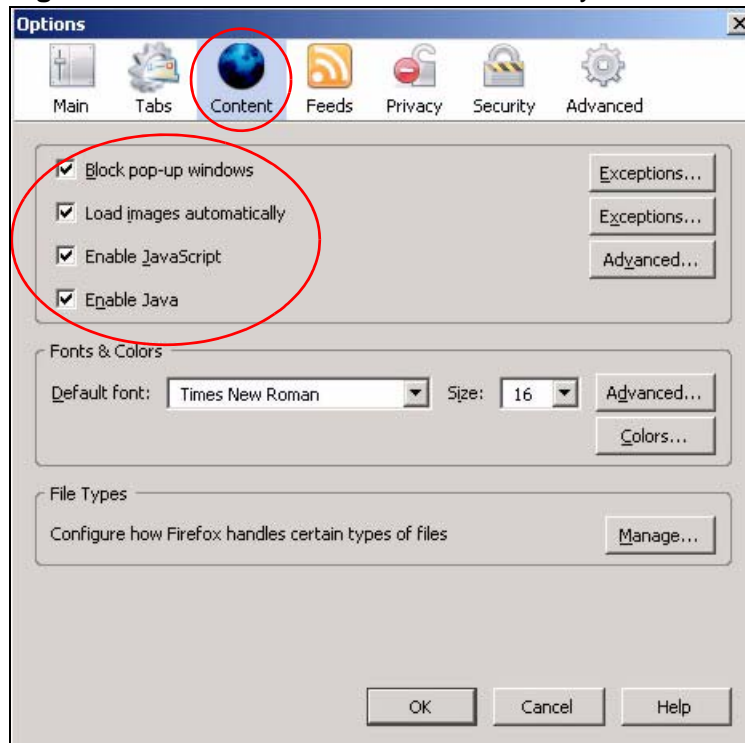
Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary.

You can enable Java, Javascript and pop-ups in one screen. Click **Tools**, then click **Options** in the screen that appears.

Figure 189 Mozilla Firefox: Tools > Options

Click **Content** to show the screen below. Select the check boxes as shown in the following screen.

Figure 190 Mozilla Firefox Content Security



IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

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

Introduction to IP Addresses

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

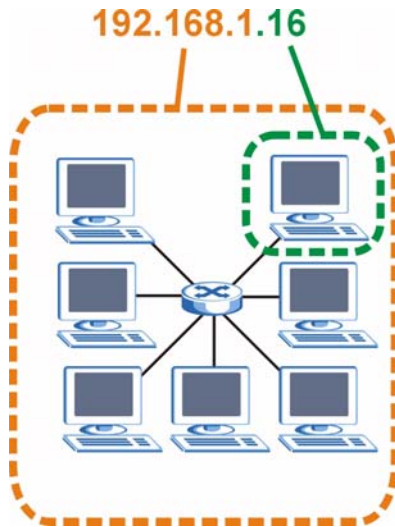
Structure

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

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

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

Figure 191 Network Number and Host ID



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

Subnet Masks

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

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

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

Table 95 IP Address Network Number and Host ID Example

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

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

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

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

Table 96 Subnet Masks

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

Network Size

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

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

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

Table 97 Maximum Host Numbers

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

Notation

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

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

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

Table 98 Alternative Subnet Mask Notation

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

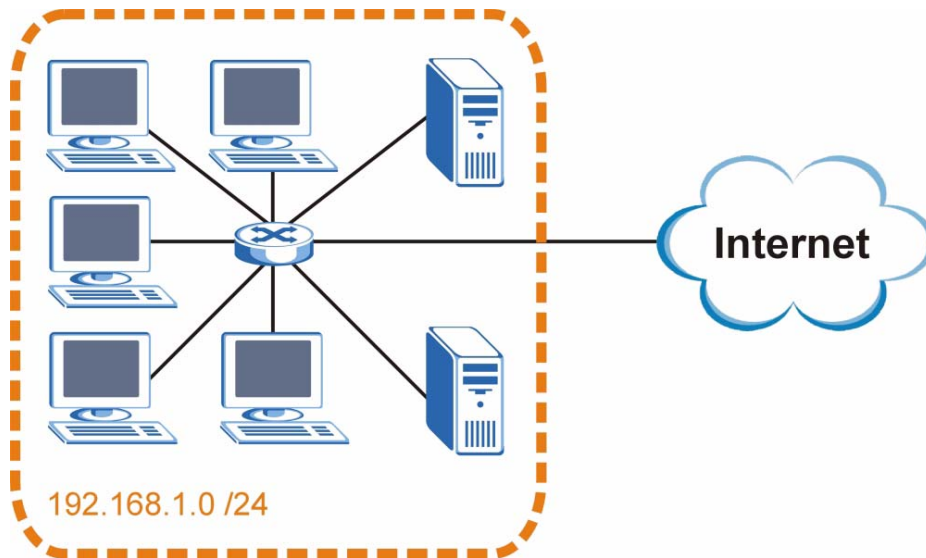
Subnetting

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

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

The following figure shows the company network before subnetting.

Figure 192 Subnetting Example: Before Subnetting

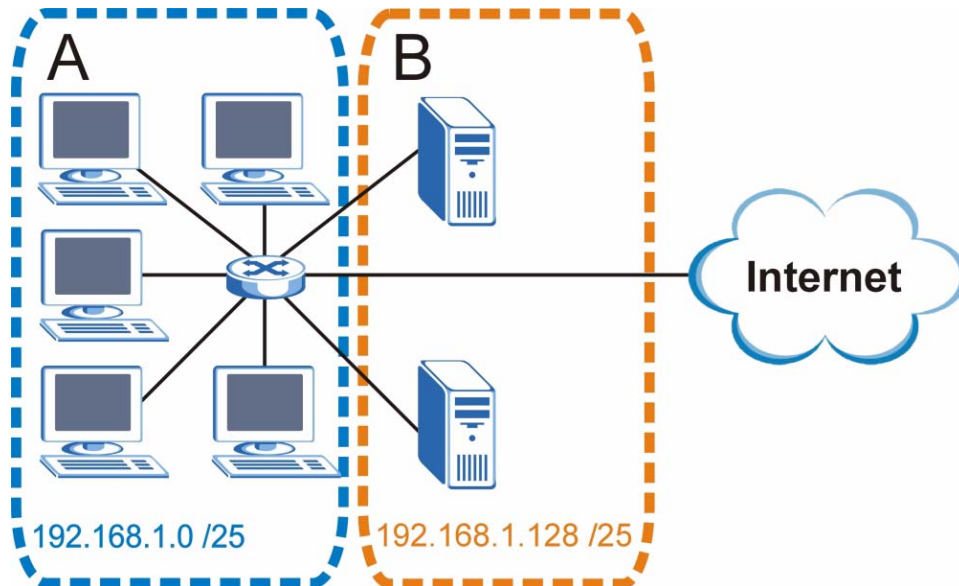


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

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

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

Figure 193 Subnetting Example: After Subnetting



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

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

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

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.11000000) or 255.255.255.192.

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

Table 99 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 100 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	01000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 101 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 102 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	11000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000

Table 102 Subnet 4 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

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

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

Table 103 Eight Subnets

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

Subnet Planning

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

Table 104 24-bit Network Number Subnet Planning

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

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

Table 105 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

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

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

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

The subnet mask specifies the network number portion of an IP address. Your 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 (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

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

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

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

IP Address Conflicts

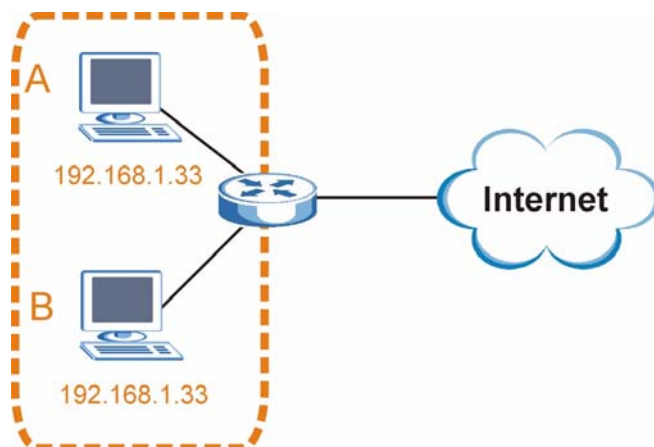
Each device on a network must have a unique IP address. Devices with duplicate IP addresses on the same network will not be able to access the Internet or other resources. The devices may also be unreachable through the network.

Conflicting Computer IP Addresses Example

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

address to computer **A** or setting computer **A** to obtain an IP address automatically.

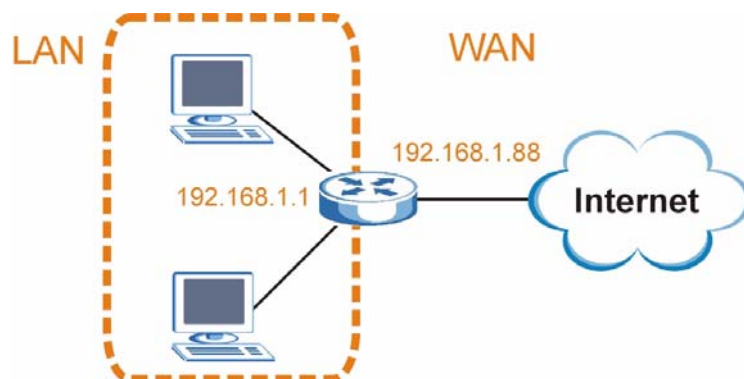
Figure 194 Conflicting Computer IP Addresses Example



Conflicting Router IP Addresses Example

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

Figure 195 Conflicting Computer IP Addresses Example

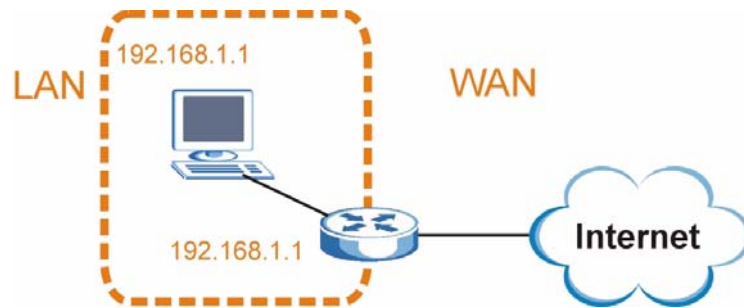


Conflicting Computer and Router IP Addresses Example

More than one device can not use the same IP address. In the following example, the computer and the router's LAN port both use 192.168.1.1 as the IP address.

The computer cannot access the Internet. This problem can be solved by assigning a different IP address to the computer or the router's LAN port.

Figure 196 Conflicting Computer and Router IP Addresses Example



Wireless LANs

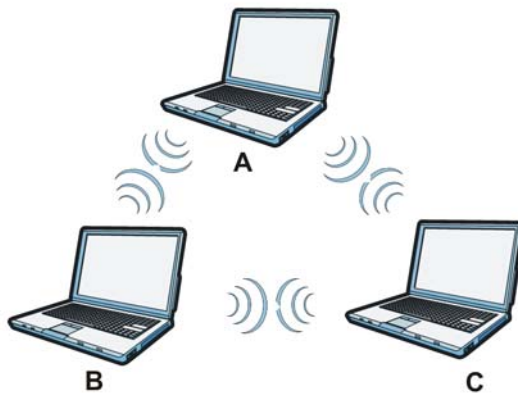
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

Figure 197 Peer-to-Peer Communication in an Ad-hoc Network



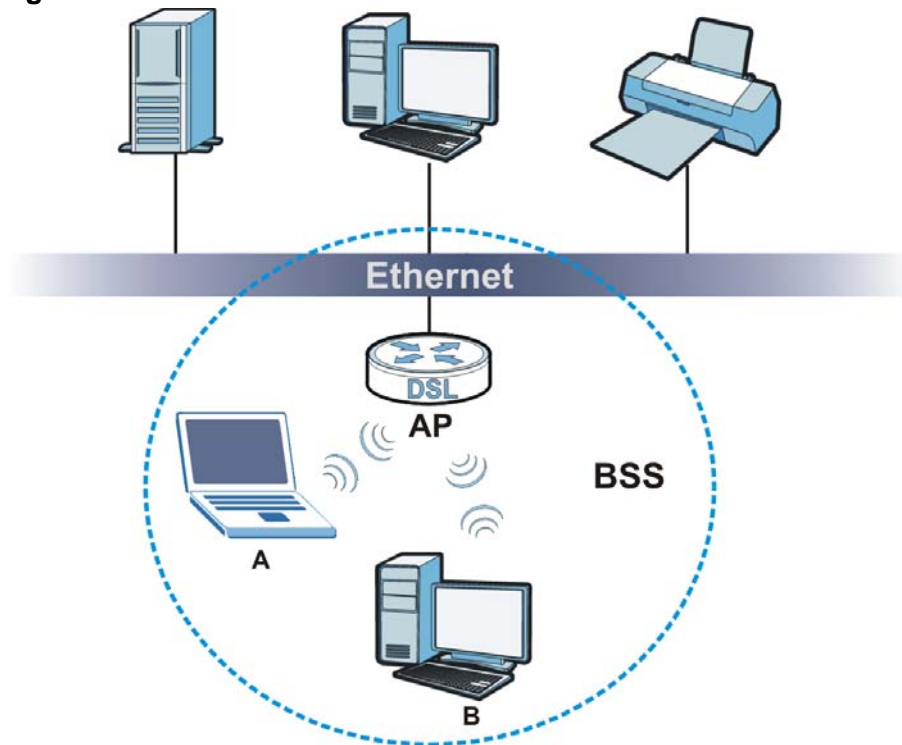
BSS

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

Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate

with each other. When Intra-BSS is disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.

Figure 198 Basic Service Set



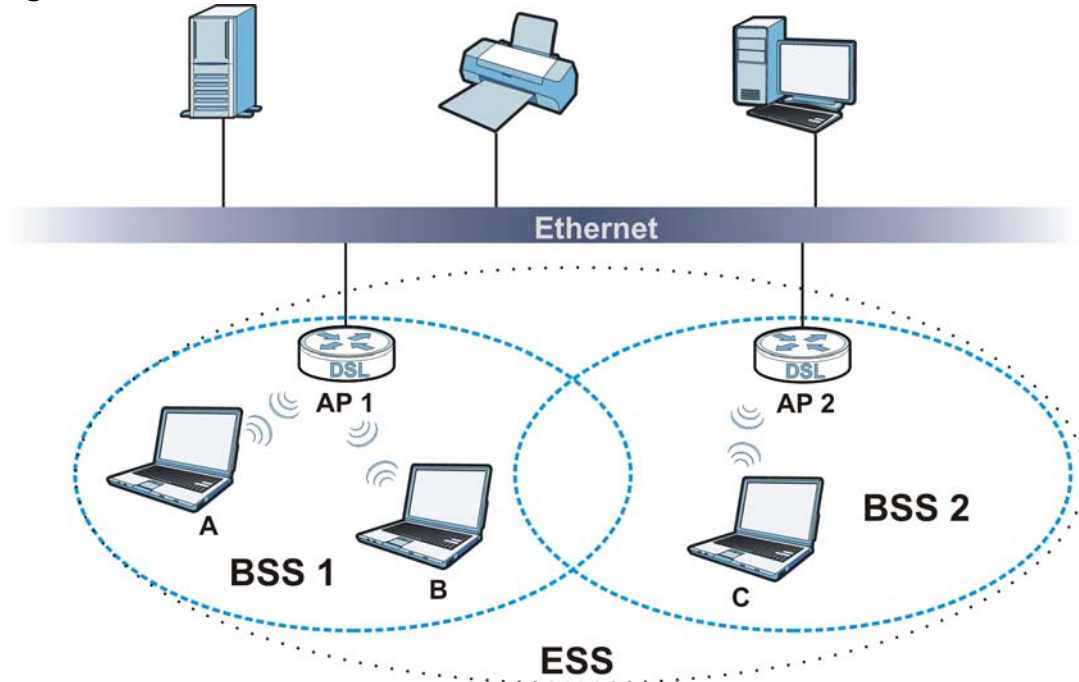
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

Figure 199 Infrastructure WLAN



Channel

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

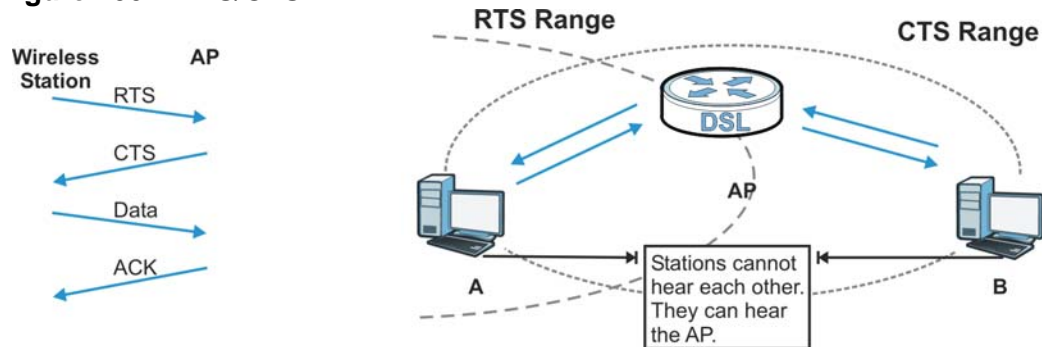
Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel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

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or

wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 200 RTS/CTS



When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Preamble Type

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

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

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

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

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

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

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has

several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 106 IEEE 802.11g

DATA RATE (Mbps)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the ZyXEL Device are data encryption, wireless client authentication, restricting access by device MAC address and hiding the ZyXEL Device identity.

The following figure shows the relative effectiveness of these wireless security methods available on your ZyXEL Device.

Table 107 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
	Wi-Fi Protected Access (WPA)
	WPA2
Most Secure	

Note: You must enable the same wireless security settings on the ZyXEL Device and on all wireless clients that you want to associate with it.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication
Determines the identity of the users.
- Authorization
Determines the network services available to authenticated users once they are connected to the network.
- Accounting
Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request
Sent by an access point requesting authentication.
- Access-Reject
Sent by a RADIUS server rejecting access.
- Access-Accept
Sent by a RADIUS server allowing access.

- Access-Challenge

Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request

Sent by the access point requesting accounting.

- Accounting-Response

Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x. .

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 108 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA2 also uses TKIP when required for compatibility reasons, but offers stronger encryption than TKIP with Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP).

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

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. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption

keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

- 1 The AP passes the wireless client's authentication request to the RADIUS server.
- 2 The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
- 3 A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.

- 4 The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 201 WPA(2) with RADIUS Application Example



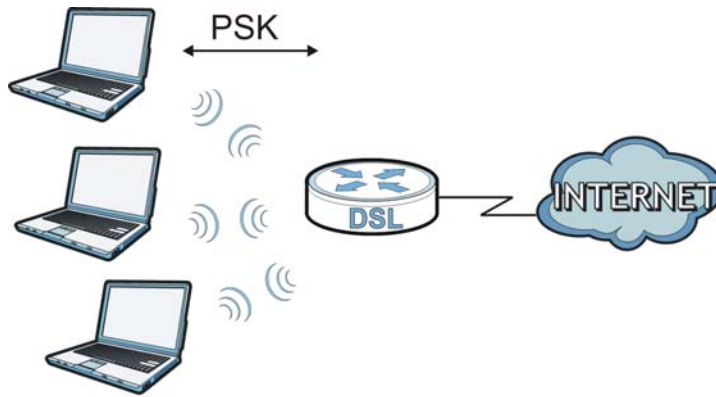
WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

- 1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).
- 2 The AP checks each wireless client's password and allows it to join the network only if the password matches.
- 3 The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

- 4 The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 202 WPA(2)-PSK Authentication



Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 109 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b and IEEE 802.11g) or 5GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to-point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name:** This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol:** This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s):** This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
 - If the **Protocol** is **TCP, UDP, or TCP/UDP**, this is the IP port number.
 - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description:** This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 110 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.

Table 110 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet Internet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).

Table 110 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC: 1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.

Table 110 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

Open Software Announcements

End-User License Agreement for "P-870H/HW Series"

WARNING: ZyXEL Communications Corp. IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED OR ZyXEL, AND YOUR MONEY WILL BE REFUNDED. HOWEVER, CERTAIN ZYXEL'S PRODUCTS MAY CONTAIN—IN PART—SOME THIRD PARTY'S FREE AND OPEN SOFTWARE PROGRAMS WHICH ALLOW YOU TO FREELY COPY, RUN, DISTRIBUTE, MODIFY AND IMPROVE THE SOFTWARE UNDER THE APPLICABLE TERMS OF SUCH THRID PARTY'S LICENSES ("OPEN-SOURCED COMPONENTS"). THE OPEN-SOURCED COMPONENTS ARE LISTED IN THE NOTICE OR APPENDIX BELOW. ZYXEL MAY HAVE DISTRIBUTED TO YOU HARDWARE AND/OR SOFTWARE, OR MADE AVAILABLE FOR ELECTRONIC DOWNLOADS THESE FREE SOFTWARE PROGRAMS OF THRID PARTIES AND YOU ARE LICENSED TO FREELY COPY, MODIFY AND REDISTRIBUTE THAT SOFTWARE UNDER THE APPLICABLE LICENSE TERMS OF SUCH THIRD PARTY. NONE OF THE STATEMENTS OR DOCUMENTATION FROM ZYXEL INCLUDING ANY RESTRICTIONS OR CONDITIONS STATED IN THIS END USER LICENSE AGREEMENT SHALL RESTRICT ANY RIGHTS AND LICENSES YOU MAY HAVE WITH RESPECT TO THE OPEN-SOURCED COMPONENTS UNDER THE APPLICABLE LICENSE TERMS OF SUCH THIRD PARTY.

1. Grant of License for Personal Use

ZyXEL Communications Corp. ("ZyXEL") grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the Software ("Documentation"), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one

backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

2.Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

3.Copyright

The Software and Documentation contain material that is protected by international copyright law, trade secret law, international treaty provisions, and the applicable national laws of each respective country. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation.

4.Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. ZyXEL is not obligated to provide any maintenance, technical or other support for the resultant modified Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. Except as and only to the extent expressly permitted in this License, you may not market, co-brand, and private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing. Portions of the Software utilize or include third party software and other copyright material. Acknowledgements, licensing terms and disclaimers for such material are contained in the License Notice as below for the third party software, and your use of such material is exclusively governed by their respective terms. ZyXEL has provided, as part of the Software package, access to certain third party software as a convenience. To the extent that the Software contains third party software, ZyXEL has no express or implied obligation to provide any technical or other support for such software other than compliance with the applicable license terms of such third party, and makes no warranty (express, implied or statutory) whatsoever with respect thereto. Please

contact the appropriate software vendor or manufacturer directly for technical support and customer service related to its software and products.

5. Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms and conditions of this License Agreement to those persons employed by you who come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

6. No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERRUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

7. Limitation of Liability

IN NO EVENT WILL ZyXEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE OR PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyXEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyXEL's TOTAL AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED THE PRODUCT'S PRICE. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF

LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

8.Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyxEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

9.Audit Rights

ZyxEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

10.Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyxEL all copies of the Software and Documentation in your possession or under your control. ZyxEL may terminate this License Agreement for any reason, including, but not limited to, if ZyxEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyxEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

11.General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in ROC, Taiwan if the parties agree to a binding arbitration. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyxEL. Any waiver or modification of this License Agreement shall only be

effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.

NOTE: Some components of this product incorporate free software programs covered under the open source code licenses which allows you to freely copy, modify and redistribute the software. For at least three (3) years from the date of distribution of the applicable product or software, we will give to anyone who contacts us at the ZyXEL Technical Support (support@zyxel.com.tw), for a charge of no more than our cost of physically performing source code distribution, a complete machine-readable copy of the complete corresponding source code for the version of the Programs that we distributed to you if we are in possession of such.

Notice

Information herein is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, except the express written permission of ZyXEL Communications Corporation.

This Product includes MIPS Linux kernel , Bridge-Utils, BusyBox 1.0.0 toolset , Dproxy, ebtables, bftpd, iproute2, iptables, udhcp and zebra software under GPL 2.0 license.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the

scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who

places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

This Product includes ppp software under below license

This directory contains source code and precompiled binaries for ppp-2.4, a package which implements the Point-to-Point Protocol (PPP) to provide Internet connections over serial lines. ppp-2.4 currently supports Linux and Solaris.

All of the code here can be freely used and redistributed. The individual source files each have their own copyright and permission

notice; some have a BSD-style notice and some are under the GPL.

This Product includes Ssh server: dropbear software under MIT-style license

The MIT License

Copyright (c) <year> <copyright holders>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR

IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,

FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE

AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER

LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,

OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN

THE SOFTWARE.

This Product includes openssl: openssl library software under BSD-style license

Copyright (c) <YEAR>, <OWNER>

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the <ORGANIZATION> nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Legal Information

Copyright

Copyright © 2010 by ZyXEL Communications Corporation.

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

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

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

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

Ce produit est conçu pour les bandes de fréquences 2,4 GHz conformément à la législation Européenne. En France métropolitaine, suivant les décisions n°03-908 et 03-909 de l'ARCEP, la puissance d'émission ne devra pas dépasser 10 mW (10 dB) dans le cadre d'une installation WiFi en extérieur pour les fréquences comprises entre 2454 MHz et 2483,5 MHz.

Viewing Certifications

- 1 Go to <http://www.zyxel.com>.
- 2 Select your product on the ZyXEL home page to go to that product's page.
- 3 Select the certification you wish to view from this page.

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- 1 Reorient or relocate the receiving antenna.
- 2 Increase the separation between the equipment and the receiver.
- 3 Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- 4 Consult the dealer or an experienced radio/TV technician for help.



FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

注意！

依據 低功率電波輻射性電機管理辦法

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

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。
減少電磁波影響，請妥適使用。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Viewing Certifications

- 1 Go to <http://www.zyxel.com>.
- 2 Select your product on the ZyXEL home page to go to that product's page.
- 3 Select the certification you wish to view from this page.

ZyXEL Limited Warranty

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

Note

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

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

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

Index

A

ACS [179](#)
Advanced Encryption Standard
 See AES.
AES [303](#)
ALG [128](#)
alternative subnet mask notation [284](#)
antenna [235](#)
 directional [308](#)
 gain [307](#)
 omni-directional [308](#)
AP (access point) [295](#)
Application Layer Gateway [128](#)
applications
 Internet access [22](#)
Auto Configuration Server, see ACS [179](#)

B

backup [220](#)
Basic Service Set, See BSS [293](#)
blinking LEDs [25](#)
broadcast [74](#)
BSS [293](#)

C

CA [141](#), [301](#)
Canonical Format Indicator See CFI
CCMs [225](#)
certificate
 details [146](#)
 factory default [142](#)
Certificate Authority
 See CA.
certificates [141](#)

authentication [141](#)
CA
 creating [143](#)
 importing [144](#), [148](#)
 public key [141](#)
 replacing [142](#)
 storage space [142](#)
Certification Authority [141](#)
Certification Authority. see CA
certifications [325](#)
 notices [327](#)
 viewing [327](#)
CFI [74](#)
CFM [225](#)
 CCMs [225](#)
 link trace test [226](#)
 loopback test [226](#)
 MA [225](#)
 MD [225](#)
 MEP [225](#)
 MIP [225](#)
channel [295](#)
 interference [295](#)
channel ID [89](#)
configuration [78](#), [81](#)
Connectivity Check Messages, see CCMs
copyright [325](#)
CoS [175](#)
CoS technologies [164](#)
CPU usage [45](#)
creating certificates [143](#)
CTS (Clear to Send) [296](#)

D

date and time [45](#)
default [222](#)
default LAN IP address [37](#)
DHCP [51](#), [78](#), [81](#), [82](#), [177](#)

- DHCP client [51](#)
- DHCP client list [51](#)
- DHCP relay [236](#)
- DHCP server [236](#)
- diagnostic [226](#)
- Differentiated Services, see DiffServ [175](#)
- DiffServ [175](#)
 - marking rule [176](#)
- digital IDs [141](#)
- disclaimer [325](#)
- DNS [79](#)
- DNS server address assignment [74](#)
- Domain Name [129](#)
- domain name system
 - see DNS
- Domain Name System. See DNS.
- DS field [176](#)
- DS, dee differentiated services
- DSCP [175](#)
- DSL interface [56](#)
- dynamic DNS [177](#)
- Dynamic Host Configuration Protocol. See DHCP.
- dynamic WEP key exchange [302](#)
- DYNDNS wildcard [177](#)

E

- EAP Authentication [300](#)
- EAP-MD5 [239](#)
- ECHO [129](#)
- encapsulated routing link protocol (ENET ENCAP) [71](#)
- Encapsulation [71](#)
 - PPP over Ethernet [71](#)
- encapsulation
 - ENET ENCAP [71](#)
- encryption [303](#)
 - WEP [92](#)
- ESS [294](#)
- ESSID [45](#)
- Extended Service Set IDentification [89](#)
- Extended Service Set, See ESS [294](#)

- external antenna [238](#)
- external RADIUS [239](#)

F

- FCC interference statement [325](#)
- Finger [129](#)
- Firewall
 - Creating/Editing Rules [133](#)
- firmware
 - upload [218](#)
 - upload error [219](#)
- firmware version [44](#)
- fragmentation threshold [297](#)
- frequency range [239](#)
- FTP [118](#), [129](#)

H

- hidden node [295](#)
- host [210](#)
- host name [44](#)
- HTTP [129](#), [135](#), [136](#)
- HTTP (Hypertext Transfer Protocol) [218](#)
- humidity [235](#)

I

- IANA [83](#), [290](#)
- IBSS [293](#)
- IEEE 802.11g [297](#)
- IEEE 802.11g wireless LAN [238](#)
- IEEE 802.11i [238](#)
- IEEE 802.1Q [73](#)
- IGMP [74](#), [78](#), [83](#)
 - version [74](#)
- IGMP proxy [238](#)
- IGMP v1 [238](#)
- IGMP v2 [238](#)
- importing certificates [144](#), [148](#)

Independent Basic Service Set
 See IBSS [293](#)
initialization vector (IV) [303](#)
install UPnP [187](#)
 Windows Me [187](#)
 Windows XP [189](#)
internal routing table [48](#)
Internet access [22](#)
Internet Assigned Numbers Authority
 See IANA [290](#)
IP Address [128](#)
IP address [82](#)
IP Address Assignment [71](#)
IP alias [237](#)
IP filter
 basics [135](#)
 creating or editing rules [138](#)
 introduction [135](#)
 policies [136](#)
IP multicasting [238](#)
IP pool [80](#)
IP pool setup [82](#)

L

LAN statistics [50](#)
LAN TCP/IP [82](#)
LAN-Side DSL CPE Configuration [181](#)
LBR [226](#)
link trace [226](#)
Link Trace Message, see LTM
Link Trace Response, see LTR
logs [213](#)
 overview [213](#)
 settings [214](#)
Loop Back Response, see LBR
loopback [226](#)
LTM [226](#)
LTR [226](#)

M

MA [225](#)
MAC [44](#)
MAC address [44](#)
MAC address filter action [96](#)
MAC filter [95, 97](#)
Maintenance Association, see MA
Maintenance Domain, see MD
Maintenance End Point, see MEP
managing the device
 good habits [22](#)
MD [225](#)
memory usage [45](#)
MEP [225](#)
Message Integrity Check (MIC) [303](#)
MTU (Multi-Tenant Unit) [73](#)
multicast [74, 78, 83](#)

N

NAT [82, 117, 289](#)
 address mapping rule [123](#)
 default server [128](#)
 DMZ host [128](#)
 external port [119](#)
 internal port [119](#)
 port forwarding [118](#)
 port number [118, 129](#)
 services [129](#)
 Symmetric [72](#)
NAT example [130](#)
NAT traversal [185](#)
Network Address Translation, see NAT
NNTP [129](#)

O

operation humidity [235](#)
operation temperature [235](#)

P

- Packet Transfer Mode [56](#)
- Pairwise Master Key (PMK) [303](#), [305](#)
- Per-Hop Behavior, see PHB [176](#)
- PHB [176](#)
- Point-to-Point Tunneling Protocol [130](#)
- POP3 [129](#), [135](#), [136](#)
- ports [25](#)
- power adaptor [239](#)
- power specifications [235](#)
- PPP (Point-to-Point Protocol) Link Layer Protocol [238](#)
- PPPoE [71](#)
 - Benefits [71](#)
- PPPoE (Point-to-Point Protocol over Ethernet) [237](#)
- PPTP [130](#)
- preamble mode [297](#)
- product registration [328](#)
- PSK [303](#)
- PTM [56](#)

Q

- QoS [163](#), [175](#)
 - marking [164](#)
 - setup [163](#)
 - tagging [164](#)
 - versus CoS [164](#)
- Quality of Service, see QoS
- Quick Start Guide [37](#)

R

- RADIUS [239](#), [299](#)
 - message types [299](#)
 - messages [299](#)
 - shared secret key [300](#)
- registration
 - product [328](#)
- related documentation [3](#)
- remote management

- TR-069 [179](#)
- Remote Procedure Calls, see RPCs [179](#)
- resetting your device [26](#)
- restore [221](#)
- RFC 1058. See RIP.
- RFC 1389. See RIP.
- RFC 1631 [117](#)
- RFC 2131. See DHCP.
- RFC 2132. See DHCP
- RFC 2516 [237](#)
- RIP [78](#), [161](#)
 - Routing Information Protocol
 - see RIP
- route status [48](#)
- router features [22](#)
- routing information [48](#)
- Routing Information Protocol. See RIP
- RPPCs [179](#)
- RTS (Request To Send) [296](#)
 - threshold [295](#), [296](#)

S

- safety warnings [7](#)
- service access control [182](#)
- Service Set [89](#)
- Services [129](#)
- SIP ALG [128](#)
- SIP Application Layer Gateway [128](#)
- SMTP [129](#)
- SNMP [129](#)
- SNMP trap [130](#)
- static route [153](#), [157](#), [161](#)
- static VLAN
- status indicators [25](#)
- storage humidity [235](#)
- storage temperature [235](#)
- subnet [281](#)
- subnet mask [82](#), [282](#)
- subnetting [284](#)
- Symmetric NAT [72](#)
- Symmetric NAT, Outgoing [73](#)

syntax conventions [5](#)
system name [44](#)

T

Tag Control Information See TCI
Tag Protocol Identifier See TPID
TCI
TCP/IP [135](#)
temperature [235](#)
Temporal Key Integrity Protocol (TKIP) [303](#)
TLS [239](#)
TPID [73](#)
TR-064 [181](#)
TR-069 [179](#)
 ACS setup [179](#)
 authentication [180](#)
trademarks [325](#)
transparent bridging [238](#)
TTLS [239](#)

U

unicast [74](#)
Universal Plug and Play [185](#)
 application [186](#)
UPnP [185](#)
 forum [186](#)
 security issues [186](#)

V

VID
Virtual Local Area Network See VLAN
VLAN [73](#)
 Introduction [73](#)
 number of possible VIDs
 priority frame
 static
VLAN ID [73](#)
VLAN Identifier See VID

VLAN tag [73](#)

W

WAN (Wide Area Network) [55](#)
WAN interface [47](#)
WAN statistics [47](#)
warranty [327](#)
 note [327](#)
Web Configurator [37](#)
WEP (Wired Equivalent Privacy) [238](#)
WEP encryption [94](#)
Wi-Fi Protected Access [302](#)
Wi-Fi Protected Access (WPA) [238](#)
wireless client WPA supplicants [304](#)
wireless LAN MAC address filtering [238](#)
wireless security [298](#)
wireless station list [49](#)
Wireless tutorial [27](#)
WLAN
 interference [295](#)
 security parameters [306](#)
WLAN button [26](#)
WPA [302](#)
 key caching [304](#)
 pre-authentication [304](#)
 user authentication [304](#)
 vs WPA-PSK [303](#)
 wireless client supplicant [304](#)
 with RADIUS application example [304](#)
WPA2 [302](#)
 user authentication [304](#)
 vs WPA2-PSK [303](#)
 wireless client supplicant [304](#)
 with RADIUS application example [304](#)
WPA2-Pre-Shared Key [302](#)
WPA2-PSK [302](#), [303](#)
 application example [305](#)
WPA-PSK [303](#)
 application example [305](#)
WPS
 status [45](#)

