

# P-870HW-51a v2

*802.11bg Wireless VDSL2 4 port gateway*

## *User's Guide*



### Default Login Details

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

Firmware Version 1.0  
Edition 1, 1/2009

[www.zyxel.com](http://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. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

## Related Documentation

- Quick Start Guide

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

- Web Configurator Online Help

Embedded web help for descriptions of individual screens and supplementary information.

**Note:** It is recommended you use the web configurator to configure the ZyXEL Device.

- Support Disc

Refer to the included CD for support documents.

- ZyXEL Web Site

Please refer to [www.zyxel.com](http://www.zyxel.com) for additional support documentation and product certifications.

## User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,  
ZyXEL Communications Corp.,  
6 Innovation Road II,  
Science-Based Industrial Park,  
Hsinchu, 300, Taiwan.

E-mail: [techwriters@zyxel.com.tw](mailto:techwriters@zyxel.com.tw)

## Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. See [http://www.zyxel.com/web/contact\\_us.php](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-870HW-51a v2 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.







---

<b>Introduction .....</b>	<b>17</b>
Introducing the ZyXEL Device .....	19
Tutorials .....	25
Introducing the Web Configurator .....	35
Status Screens .....	39
<b>Network .....</b>	<b>49</b>
WAN Setup .....	51
LAN Setup .....	69
Wireless LAN .....	79
Network Address Translation (NAT) .....	107
<b>Security .....</b>	<b>115</b>
IP Filter .....	117
<b>Advanced .....</b>	<b>123</b>
Static Route .....	125
Quality of Service (QoS) .....	129
Dynamic DNS Setup .....	141
Remote Management .....	143
Universal Plug-and-Play (UPnP) .....	149
<b>Maintenance, Troubleshooting and Specifications .....</b>	<b>163</b>
System Settings .....	165
Logs .....	169
Tools .....	173
Troubleshooting .....	181
Product Specifications .....	187
<b>Appendices and Index .....</b>	<b>193</b>

---

# Table of Contents

About This User's Guide .....	3
Document Conventions.....	5
Safety Warnings.....	7
Table of Contents.....	11

## Part I: Introduction..... 17

### Chapter 1 Introducing the ZyXEL Device ..... 19

1.1 Overview .....	19
1.2 Ways to Manage the ZyXEL Device .....	19
1.3 Good Habits for Managing the ZyXEL Device .....	20
1.4 Applications for the ZyXEL Device .....	20
1.4.1 Internet Access .....	20
1.5 LEDs (Lights) .....	21
1.6 The RESET Button .....	22
1.6.1 Using the Reset Button .....	22
1.7 The WPS WLAN Button .....	23
1.7.1 Turn the Wireless LAN Off or On .....	23
1.7.2 Activate WPS .....	23

### Chapter 2 Tutorials..... 25

2.1 How to Set up a Wireless Network .....	25
2.1.1 Example Parameters .....	25
2.1.2 Configuring the AP .....	25
2.1.3 Configuring the Wireless Client .....	28

### Chapter 3 Introducing the Web Configurator ..... 35

3.1 Web Configurator Overview .....	35
3.1.1 Accessing the Web Configurator .....	35
3.2 Web Configurator Main Screen .....	36
3.2.1 Navigation Panel .....	37
3.2.2 Main Window .....	38

3.2.3 Status Bar .....	38
<b>Chapter 4</b>	
<b>Status Screens .....</b>	<b>39</b>
4.1 Status Screen .....	39
4.1.1 WAN Service Statistics .....	42
4.1.2 Route Info .....	43
4.1.3 WLAN Station List .....	45
4.1.4 LAN Statistics .....	46
4.1.5 Client List .....	47
<b>Part II: Network.....</b>	<b>49</b>
<b>Chapter 5</b>	
<b>WAN Setup.....</b>	<b>51</b>
5.1 Overview .....	51
5.1.1 What You Can Do in this Chapter .....	51
5.2 What You Need to Know .....	52
5.3 Before You Begin .....	52
5.4 The Internet Connection Screen .....	53
5.4.1 Advanced Internet Connection Setup .....	56
5.5 The More Connections Screen .....	57
5.5.1 More Connections Edit .....	59
5.5.2 Configuring More Connections Advanced Setup .....	62
5.6 Technical Reference .....	63
<b>Chapter 6</b>	
<b>LAN Setup.....</b>	<b>69</b>
6.1 Overview .....	69
6.1.1 What You Can Do in this Chapter .....	69
6.2 What You Need To Know .....	70
6.3 Before You Begin .....	71
6.4 The LAN IP Screen .....	71
6.5 The Client List Screen .....	72
6.6 The IP Alias Screen .....	73
6.6.1 Configuring the LAN IP Alias Screen .....	74
6.7 Technical Reference .....	75
<b>Chapter 7</b>	
<b>Wireless LAN.....</b>	<b>79</b>
7.1 Overview .....	79

7.1.1 What You Can Do in this Chapter .....	79
7.2 What You Need to Know .....	80
7.3 Before You Begin .....	82
7.4 The General Screen .....	82
7.4.1 No Security .....	84
7.4.2 WEP Encryption .....	85
7.4.3 WPA(2)-PSK .....	86
7.4.4 WPA(2) Authentication .....	88
7.5 The WPS Screen .....	89
7.6 The WPS Station Screen .....	91
7.7 The MAC Filter Screen .....	91
7.8 The Advanced Setup Screen .....	93
7.9 Technical Reference .....	94
7.9.1 Wireless Network Overview .....	95
7.9.2 Additional Wireless Terms .....	96
7.9.3 Wireless Security Overview .....	96
7.9.4 WiFi Protected Setup .....	98
<b>Chapter 8</b>	
<b>Network Address Translation (NAT).....</b>	<b>107</b>
8.1 Overview .....	107
8.1.1 What You Can Do in this Chapter .....	107
8.2 What You Need to Know .....	107
8.3 The Port Forwarding Screen .....	108
8.3.1 The Port Forwarding Edit Screen .....	110
8.4 The DMZ Host Screen .....	111
8.5 Technical Reference .....	112
<b>Part III: Security.....</b>	<b>115</b>
<b>Chapter 9</b>	
<b>IP Filter.....</b>	<b>117</b>
9.1 Overview .....	117
9.1.1 What You Can Do in this Chapter .....	117
9.2 What You Need to Know .....	117
9.3 The Incoming IP Filtering Screen .....	118
9.3.1 Creating Incoming Filtering Rules .....	120
<b>Part IV: Advanced .....</b>	<b>123</b>

<b>Chapter 10</b>	
<b>Static Route .....</b>	<b>125</b>
10.1 Overview .....	125
10.1.1 What You Can Do in this Chapter .....	125
10.2 The Static Route Screen .....	126
10.2.1 Static Route Edit .....	127
<b>Chapter 11</b>	
<b>Quality of Service (QoS).....</b>	<b>129</b>
11.1 Overview .....	129
11.1.1 What You Can Do in this Chapter .....	129
11.2 What You Need to Know .....	130
11.3 The Quality of Service General Screen .....	130
11.4 The Queue Setup Screen .....	131
11.4.1 Adding a QoS Queue .....	132
11.5 The Class Setup Screen .....	133
11.5.1 QoS Class Edit .....	135
11.6 Technical Reference .....	137
<b>Chapter 12</b>	
<b>Dynamic DNS Setup .....</b>	<b>141</b>
12.1 Overview .....	141
12.1.1 What You Can Do in this Chapter .....	141
12.2 What You Need To Know .....	141
12.3 The Dynamic DNS Screen .....	142
<b>Chapter 13</b>	
<b>Remote Management.....</b>	<b>143</b>
13.1 Overview .....	143
13.1.1 What You Can Do in this Chapter .....	143
13.2 The TR-069 Screen .....	143
13.3 The Service Control Screen .....	145
13.4 The IP Address Screen .....	146
13.4.1 Adding an IP Address .....	147
<b>Chapter 14</b>	
<b>Universal Plug-and-Play (UPnP).....</b>	<b>149</b>
14.1 Overview .....	149
14.1.1 What You Can Do in this Chapter .....	149
14.2 What You Need to Know .....	149
14.3 The UPnP Screen .....	150
14.4 Installing UPnP in Windows Example .....	151
14.5 Using UPnP in Windows XP Example .....	155

## **Part V: Maintenance, Troubleshooting and Specifications ..... 163**

### **Chapter 15**

#### **System Settings ..... 165**

15.1 Overview .....	165
15.1.1 What You Can Do in this Chapter .....	165
15.1.2 What You Need to Know .....	165
15.2 The General Screen .....	166
15.3 The Time Setting Screen .....	167

### **Chapter 16**

#### **Logs ..... 169**

16.1 Overview .....	169
16.1.1 What You Can Do in this Chapter .....	169
16.2 The View Log Screen .....	169
16.3 The Log Settings Screen .....	170

### **Chapter 17**

#### **Tools..... 173**

17.1 Overview .....	173
17.1.1 What You Can Do in this Chapter .....	173
17.2 The Firmware Upgrade Screen .....	174
17.3 The Configuration Screen .....	176
17.4 The Restart Screen .....	178

### **Chapter 18**

#### **Troubleshooting..... 181**

18.1 Power, Hardware Connections, and LEDs .....	181
18.2 ZyXEL Device Access and Login .....	182
18.3 Internet Access .....	183

### **Chapter 19**

#### **Product Specifications ..... 187**

19.1 Hardware Specifications .....	187
19.2 Firmware Specifications .....	187
19.3 Wireless Features .....	190

## **Part VI: Appendices and Index ..... 193**

Appendix A Setting Up Your Computer's IP Address .....	195
--	-----

Appendix B Pop-up Windows, JavaScripts and Java Permissions .....	225
---	-----

Appendix C IP Addresses and Subnetting .....	235
Appendix D Wireless LANs .....	247
Appendix E Common Services.....	263
Appendix F Legal Information .....	267
<b>Index.....</b>	<b>271</b>



---

# PART I

# Introduction

---

Introducing the ZyXEL Device (19)

Tutorials (25)

Introducing the Web Configurator (35)

Status Screens (39)



# 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 P-870HW-51a v2 is a VDSL2 gateway that allows super-fast, secure Internet access over analog (POTS) telephone lines.

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.**

See [Chapter 19 on page 187](#) 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.
- 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.

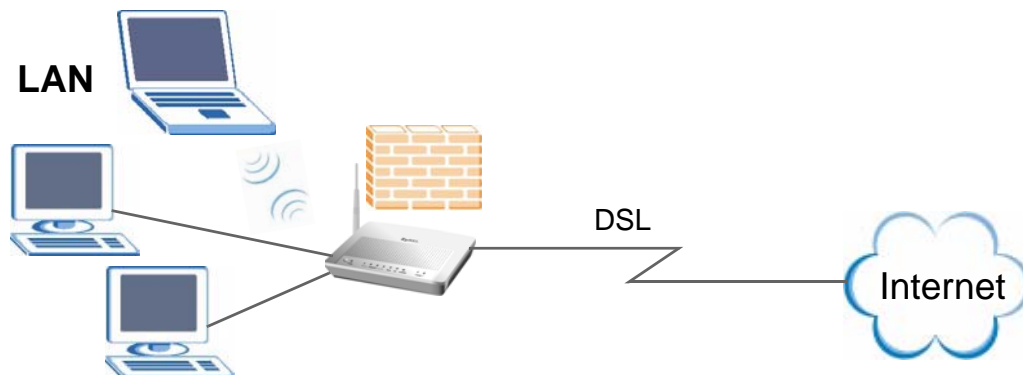
## 1.4 Applications for the ZyXEL Device

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

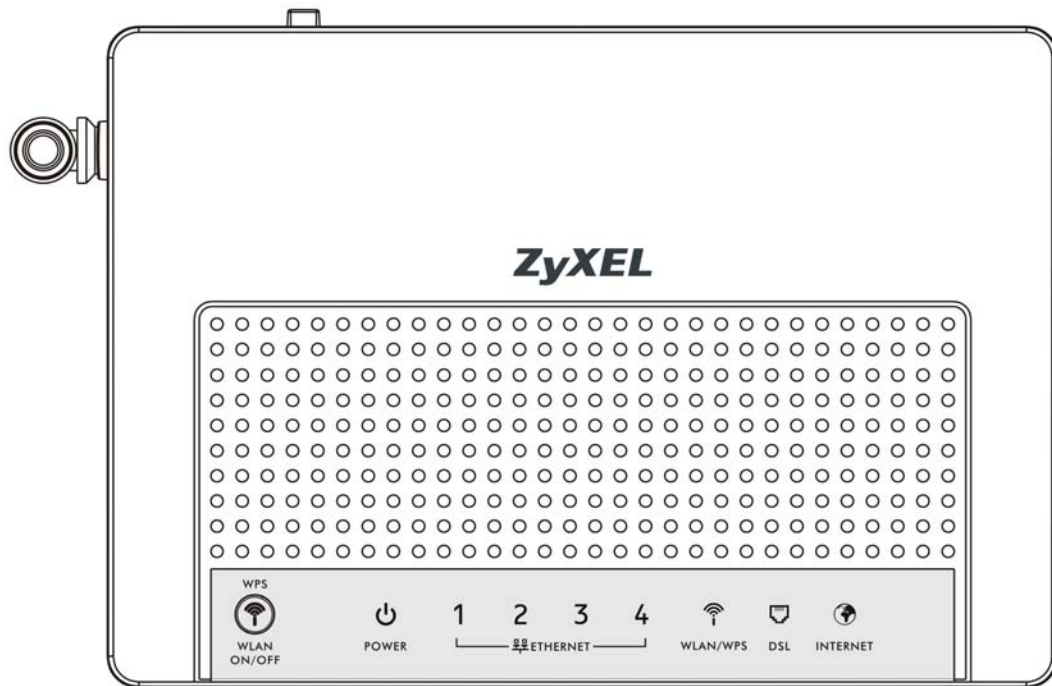


You can also configure IP filtering on the ZyXEL Device for secure Internet access. When the IP filter is on, all incoming traffic from the Internet to your network is blocked by default unless it is initiated from your network. This means that probes from the outside to your network are not allowed,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

## 1.5 LEDs (Lights)

The following graphic displays the labels of the LEDs.

**Figure 2** LEDs on the Top of the Device



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.

**Table 1** LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
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	On	The ZyXEL Device attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
		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". You can also use the

### 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

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 7.9.4 on page 98](#) 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

<b>SSID</b>	SSID_Example3
<b>Security</b>	WPA-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)
<b>802.11 mode</b>	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 3** AP: Wireless LAN

The screenshot displays the 'General' tab of the AP's web configurator. The 'Wireless Setup' section includes the following settings:

- ☒ Active Wireless LAN
- ☐ Auto Generate Key
- Network Name(SSID): SSID\_Example3
- ☐ Hide Network Name(SSID)
- Channel Selection: 6

The 'Security' section includes the following settings:

- Security Mode: WPA-PSK
- Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey
- WPA Group Key Update Timer: 1800 sec.
- WPA Encryption: TKIP

At the bottom of the Security section, 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 **54g Auto** in the **54g™ Mode** field. Click **Apply**.

**Figure 4** AP: Wireless LAN > Advanced Setup

The screenshot shows the 'Advanced Setup' tab for the Wireless LAN configuration. The fields are as follows:

- RTS/CTS Threshold: 2344
- Fragmentation Threshold: 2344
- Number of Wireless Stations Allowed: 16
- Output Power: 100%
- 54g™ Mode: 54g Auto
- 54g™ Protection: Auto
- Preamble: Long

Buttons: 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 5** AP: Status

The screenshot shows the 'Status' page with the following sections:

- System Information:** Host Name: 1234, Model Number: P-870HW-51a V2, MAC Address: 00:19:cb:d1:79:04, ZyNOS Firmware Version: 1.00(AWZ.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 Table:**

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.

- 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 6** AP: Status: WLAN Station List

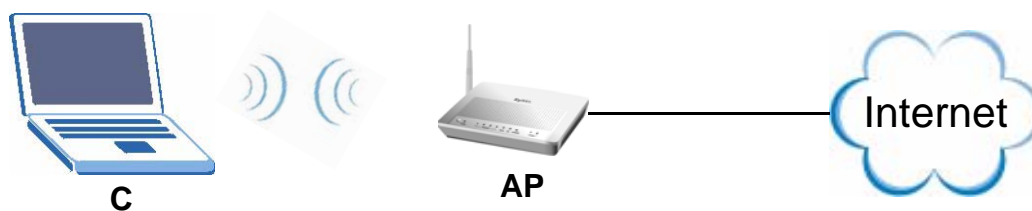
WLAN Station List				
MAC	Associated	Authorized	SSID	Interface
00:03:7F:BF:16:8C	Yes	Yes	SSID_Example3	wl0
Refresh Interval : <input type="text"/> sec <input type="button" value="Set Interval"/> <input type="button" value="Stop"/>				

## 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.

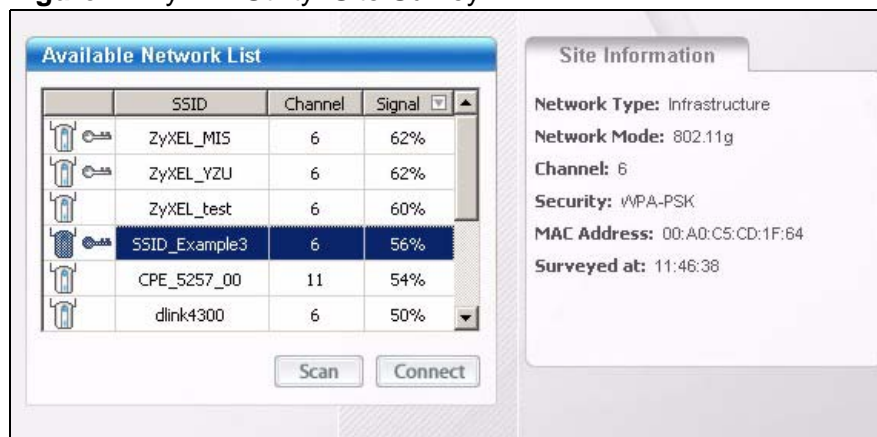
- Configure nothing and leave the wireless client to automatically scan for and connect to any available network that has no wireless security configured.
- Manually connect to a network.
- Configure a profile to have the wireless client automatically connect to a specific network or peer computer.

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 7** ZyXEL Utility: Site Survey

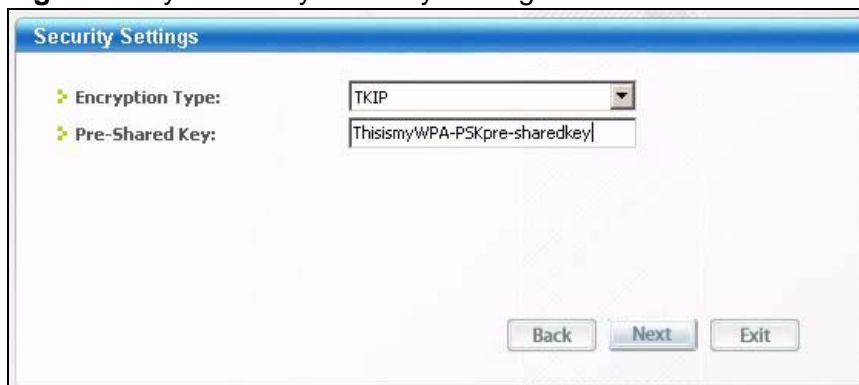


- 2 The wireless client automatically searches for available wireless networks. Click **Scan** if you want to search again. If no entry displays in the **Available Network List**, that means there is no wireless network available within range. Make sure the AP or peer computer is turned on or move the 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 8** ZyXEL Utility: Security Settings

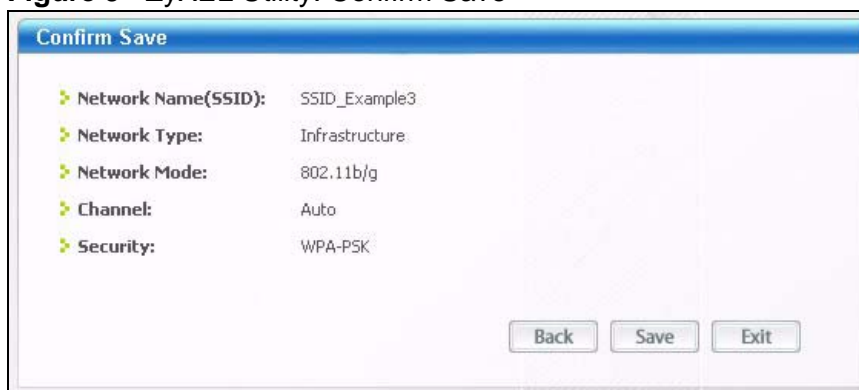


The 'Security Settings' window displays two configuration fields. The 'Encryption Type' is set to 'TKIP' via a dropdown menu. The 'Pre-Shared Key' field contains the text 'ThisismyWPA-PSKpre-sharedkey'. At the bottom right, there are three buttons: 'Back', 'Next', and 'Exit'.

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

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

**Figure 9** ZyXEL Utility: Confirm Save

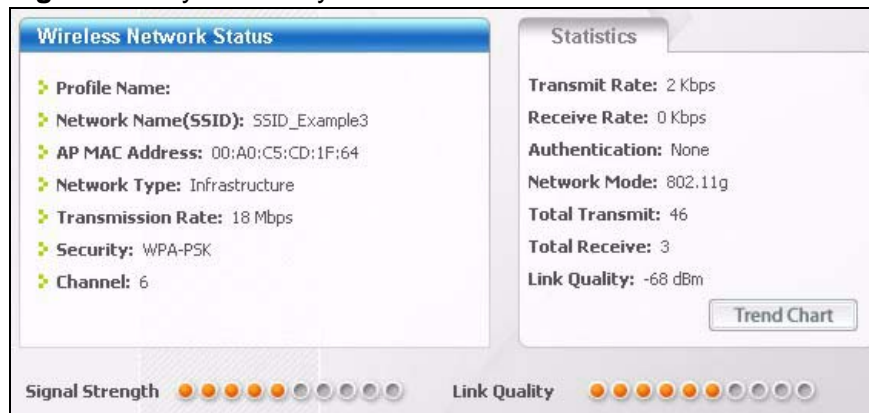


The 'Confirm Save' window displays a summary of the network settings. The fields are: Network Name(SSID): SSID\_Example3, Network Type: Infrastructure, Network Mode: 802.11b/g, Channel: Auto, and Security: WPA-PSK. At the bottom right, there are three buttons: 'Back', 'Save', and 'Exit'.

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

- 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 10** 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.

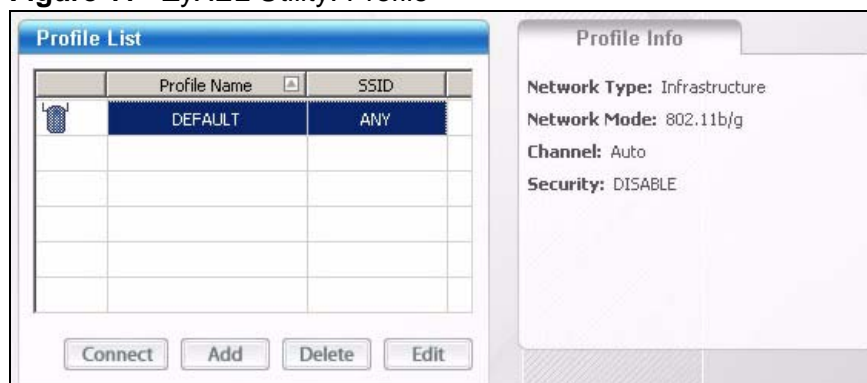
### 2.1.3.2 Creating and Using a Profile

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".

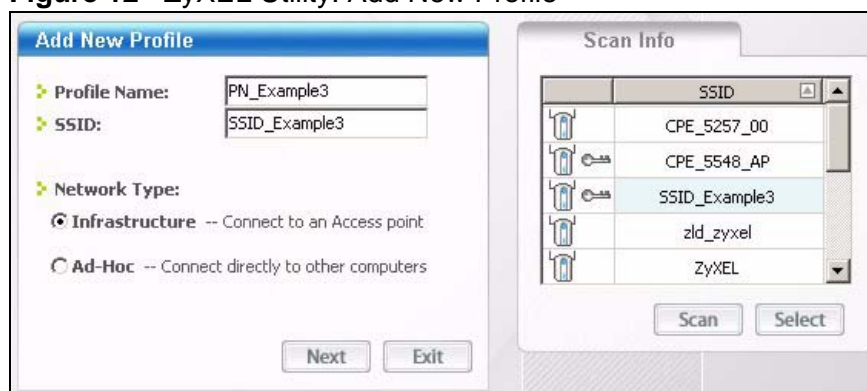
- 1 Open the ZyXEL utility and click the **Profile** tab to open the screen shown next. Click **Add** to configure a new profile.

**Figure 11** 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 12** ZyXEL Utility: Add New Profile

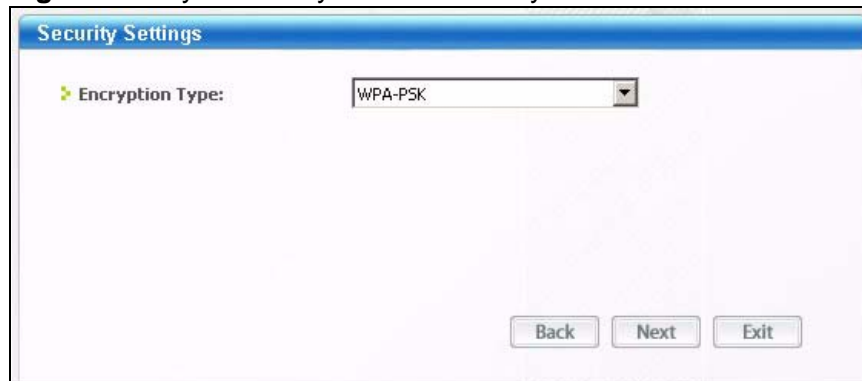


- 3 Give the profile a descriptive name (of up to 32 printable ASCII characters). Select **Infrastructure** and either manually enter or select the AP's SSID in the **Scan Info** table and click **Select**.



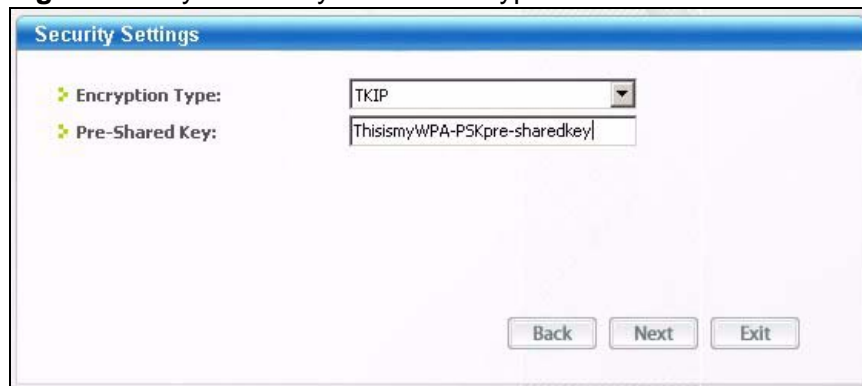
- 4 Choose the same encryption method as the AP to which you want to connect (In this example, WPA-PSK).

**Figure 13** ZyXEL Utility: Profile Security



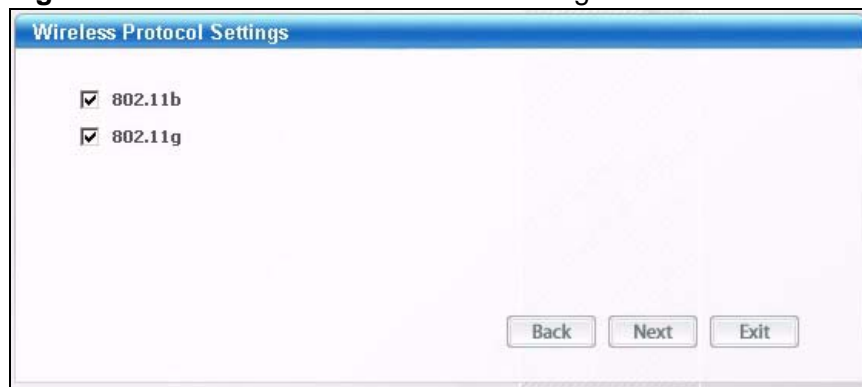
- 5 This screen varies depending on the encryption method you selected in the previous screen. Enter the pre-shared key and leave the encryption type at the default setting.

**Figure 14** ZyXEL Utility: Profile Encryption



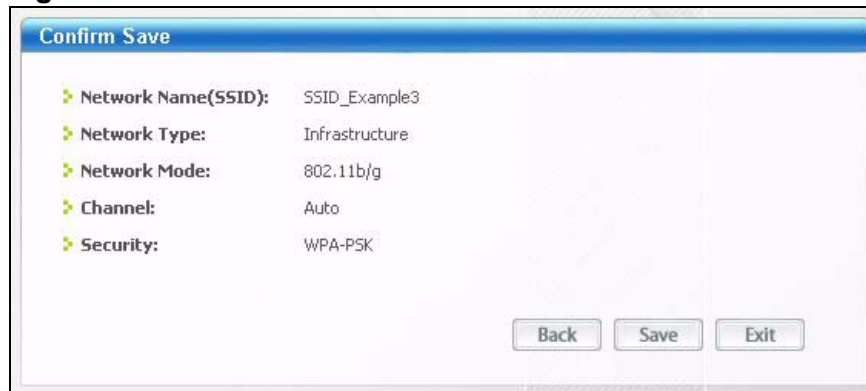
- 6 In the next screen, leave both boxes checked.

**Figure 15** 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 16** 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 17** 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.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

See [Appendix B on page 225](#) 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.

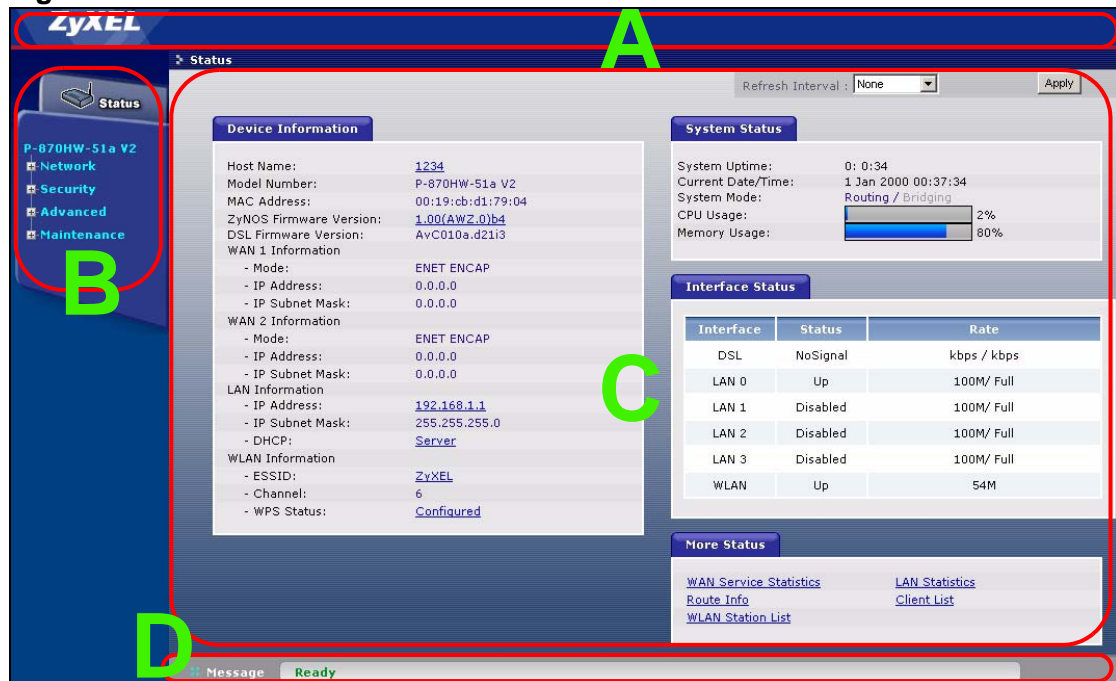
- 4 A password screen displays. Enter the default user name **1234** and default password **1234**. The password displays in non-readable characters. If you have changed the password, enter your password and click **Login**. Click **Cancel** to revert to the default password in the password field.

Figure 18 Password Screen



## 3.2 Web Configurator Main Screen

Figure 19 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	Internet Connection	Use this screen to configure ISP parameters, WAN IP address assignment, DNS servers and other advanced properties.
	More Connections	Use this screen to configure additional WAN connections.
LAN	IP	Use this screen to configure LAN TCP/IP DHCP settings.
	Client List	Use this screen to view current DHCP client information and to always assign specific IP addresses to individual MAC addresses (and host names).
	IP Alias	Use this screen to partition your LAN interface into subnets.
Wireless LAN	General	Use this screen to configure the wireless LAN settings and WLAN authentication/security settings.
	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.
	MAC Filter	Use this screen to configure the ZyXEL Device to give exclusive access to specific wireless clients or exclude specific wireless clients from accessing the ZyXEL Device.
	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.
	DMZ Host	Use this screen to configure a default server which receives packets from ports that are not specified in the <b>Port Forwarding</b> screen.
Security		
IP Filter	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.
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.

**Table 2** Navigation Panel Summary

LINK	TAB	FUNCTION
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.
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).
	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.
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.
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.

## 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 39](#) 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.

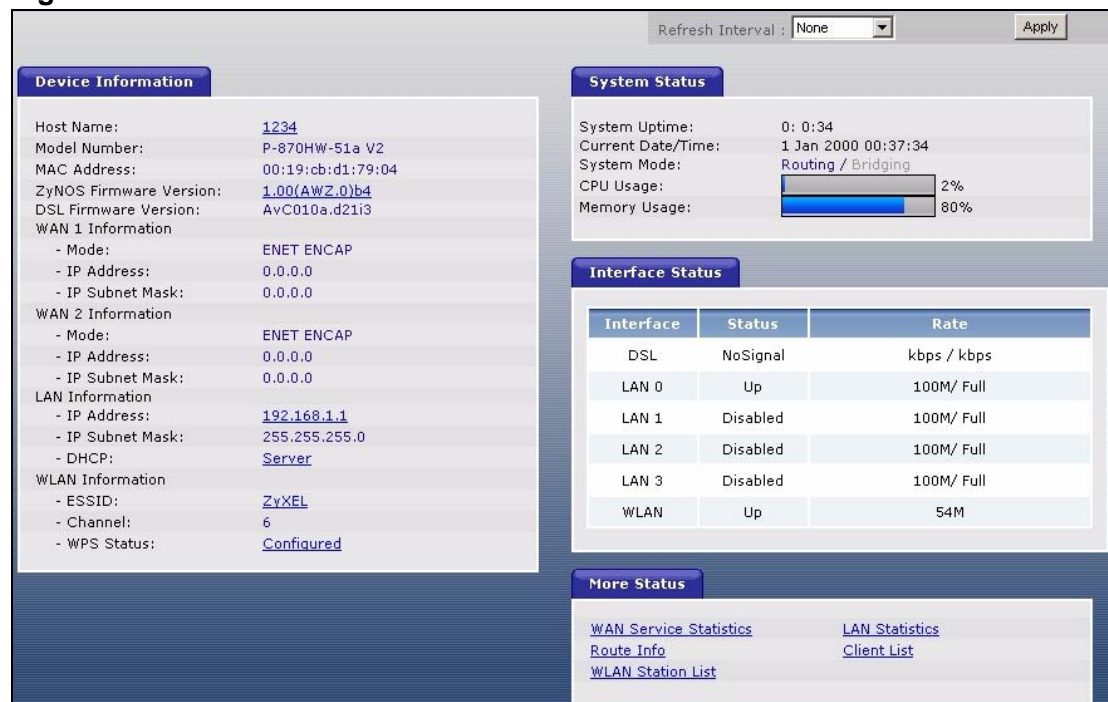
# Status Screens

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 20** 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.

**Table 3** Status Screen

LABEL	DESCRIPTION
Device Information	
Host 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.
ZyNOS 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. Click this to go to the screen where you can change it.
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><b>Server</b> - The ZyXEL Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN.</p> <p><b>None</b> - The ZyXEL Device is not providing any DHCP services to the LAN.</p> <p>Click this to go to the screen where you can change it.</p>
WLAN Information	
ESSID	This is the descriptive name used to identify the ZyXEL Device in the wireless LAN. Click this to go to the screen where you can change it.
Channel	This is the channel number used by the ZyXEL Device now.
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.
System Status	



**Table 3** Status Screen

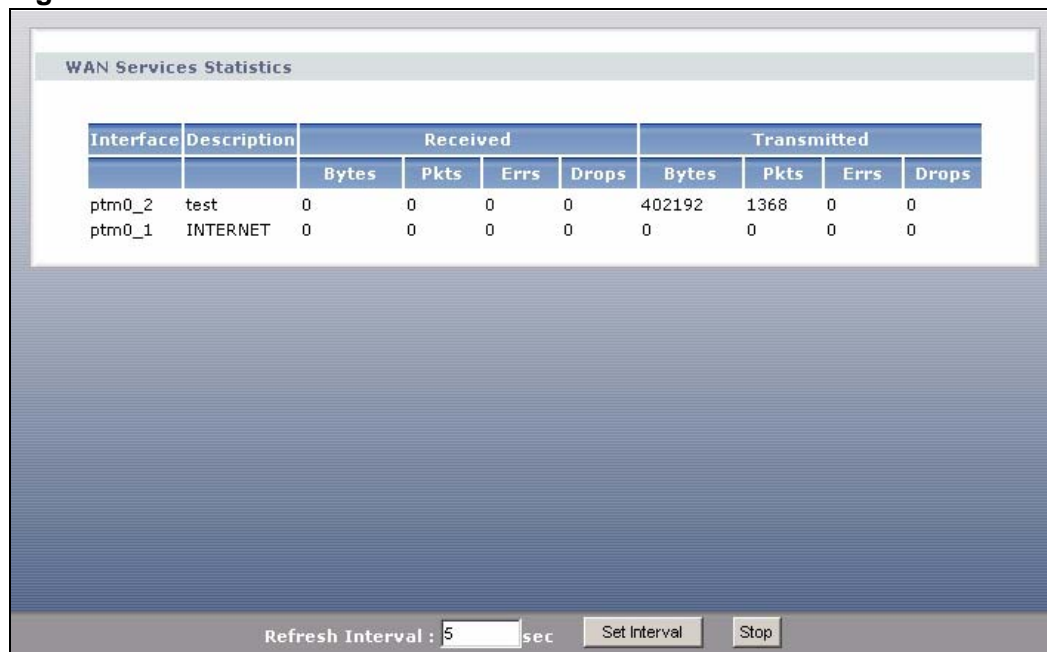
LABEL	DESCRIPTION
System Uptime	This field displays how long the ZyXEL Device has been running since it last started up. The ZyXEL Device starts up when you plug it in, when you restart it ( <b>Maintenance &gt; Tools &gt; Restart</b> ), or when you reset it (see <a href="#">Section 1.6 on page 22</a> ).
Current Date/Time	This field displays the current date and time in the ZyXEL Device. You can change this in <b>Maintenance &gt; System &gt; Time Setting</b> .
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 <a href="#">Chapter 11 on page 129</a> ).
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 <a href="#">Section 17.4 on page 178</a> , or turn off the device (unplug the power) for a few seconds.
Interface Status	
Interface	This column displays each interface the ZyXEL Device has.
Status	<p>This field indicates whether or not the ZyXEL Device is using the interface.</p> <p>For the DSL interface, this field displays <b>NoSignal</b> (line is down) or <b>Up</b> (line is up or connected).</p> <p>For the LAN interface, this field displays <b>Up</b> when the ZyXEL Device is using the interface and <b>Disabled</b> when the ZyXEL Device is not using the interface.</p> <p>For the WLAN interface, it displays <b>Up</b> when WLAN is enabled or <b>Disabled</b> when WLAN is not active.</p>
Rate	<p>For the LAN interface, this displays the port speed and duplex setting.</p> <p>For the DSL interface, it displays the downstream and upstream transmission rate.</p> <p>For the WLAN interface, it displays the maximum transmission rate.</p>
More Status	
WAN Service Statistics	Click this link to view packet specific statistics of the WAN connection(s). See <a href="#">Section 4.1.1 on page 42</a> .
Route Info	Click this link to view the internal routing table on the ZyXEL Device. See <a href="#">Section 4.1.2 on page 43</a> .
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 <a href="#">Section 4.1.3 on page 45</a> .

**Table 3** Status Screen

LABEL	DESCRIPTION
LAN Statistics	Click this link to view packet specific statistics on the LAN and WLAN interfaces. See <a href="#">Section 4.1.4 on page 46</a> .
Client List	Click this link to view current DHCP client information. See <a href="#">Section 4.1.5 on page 47</a> .

## 4.1.1 WAN Service Statistics

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

**Figure 21** Status > WAN Service Statistics

The following table describes the labels in this screen.

**Table 4** Status > WAN Service Statistics

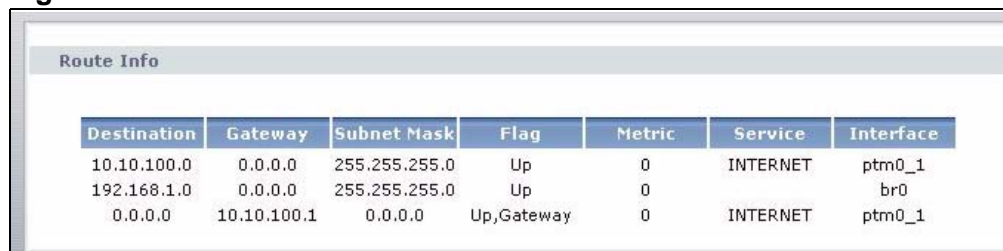
LABEL	DESCRIPTION
Interface	This shows the name of the WAN interface used by this connection.  The default name <b>ptm0</b> indicates the DSL port. The last number represents the index number of connections over the same PVC or the VLAN ID number assigned to traffic sent through this connection.
Description	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.

**Table 4** Status > WAN Service Statistics (continued)

LABEL	DESCRIPTION
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.
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 <b>Refresh Interval</b> field.
Stop	Click <b>Stop</b> 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 22** Status > Route Info


Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
10.10.100.0	0.0.0.0	255.255.255.0	Up	0	INTERNET	ptm0_1
192.168.1.0	0.0.0.0	255.255.255.0	Up	0	INTERNET	br0
0.0.0.0	10.10.100.1	0.0.0.0	Up, Gateway	0	INTERNET	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.

**Table 5** Status > Route Info (continued)

LABEL	DESCRIPTION
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>
Metric	<p>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".</p>
Service	<p>This indicates the name of the service used to forward the route.</p>
Interface	<p>This indicates the name of the interface through which the route is forwarded.</p> <p><b>br0</b> indicates the LAN interface.</p> <p><b>ptm0</b> indicates the WAN interface using ENET ENCAP or in bridge mode.</p> <p><b>ppp0</b> indicates the WAN interface using PPPoE.</p>

### 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 23** Status > WLAN Station List

MAC	Associated	Authorized	SSID	Interface
00:03:7F:BF:16:8C	Yes	Yes	WLAN_EE	wl0

Refresh Interval :  sec

The following table describes the labels in this screen.

**Table 6** Status > WLAN Station List

LABEL	DESCRIPTION
MAC Address	This field shows the MAC (Media Access Control) address of an associated wireless station.
Associated	This field shows whether the wireless station is currently associated to the ZyXEL Device ( <b>Yes</b> ) or not ( <b>No</b> ).
Authorized	This field shows whether the wireless station is allowed to access network resources behind the ZyXEL Device ( <b>Yes</b> ) or not ( <b>No</b> ).
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.
Set Interval	Click this button to apply the new poll interval you entered in the <b>Refresh Interval</b> field.
Stop	Click <b>Stop</b> 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 24** Status > LAN Statistics

The screenshot shows a web interface titled "LAN Statistics". It contains 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	4926342	46860	0	0	34742350	50897	0	0
eth1	0	0	0	0	67460	291	0	0
eth2	0	0	0	0	67332	289	0	0
eth3	0	0	0	0	67268	288	0	0
WLAN	0	0	0	0	139535	1034	15	0

Below the table, there is a "Refresh Interval" field set to "5" seconds, with "Set Interval" and "Stop" buttons.

The following table describes the labels in this screen.

**Table 7** Status > LAN Statistics

LABEL	DESCRIPTION
Interface	This shows the LAN or WLAN interface. <b>eth0~3</b> 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.
Drops	This indicates the number of outgoing packets dropped on this interface.
Refresh Interval	Enter the time interval for refreshing statistics in this field.


**Table 7** Status > LAN Statistics (continued)

LABEL	DESCRIPTION
Set Interval	Click this button to apply the new poll interval you entered in the <b>Refresh Interval</b> field.
Stop	Click <b>Stop</b> 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 25** Status > Client List


Client List		
Hostname	MAC Address	IP Address
	00:00:e8:7c:14:80	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

# Network

---

WAN Setup (51)

LAN Setup (69)

Wireless LAN (79)

Network Address Translation (NAT) (107)



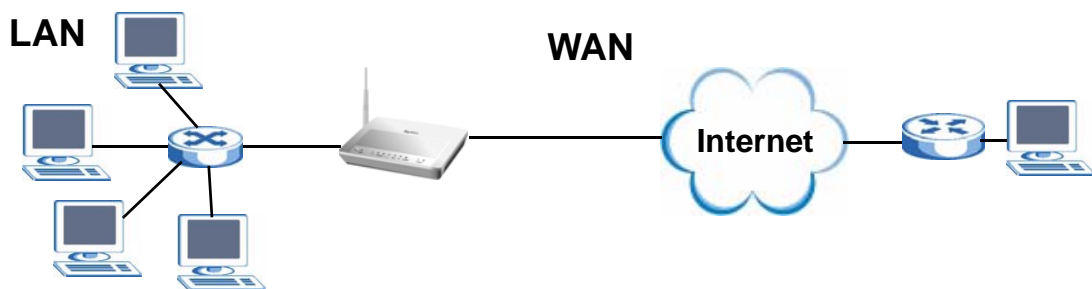
# WAN Setup

## 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 26** LAN and WAN



- See [Section 5.6 on page 63](#) for advanced technical information on WAN.

### 5.1.1 What You Can Do in this Chapter

- The **Internet Connection** screen lets you configure the WAN settings on the ZyXEL Device for Internet access ([Section 5.4 on page 53](#)).
- The **More Connections** screen lets you set up additional Internet access connections ([Section 5.5 on page 57](#)).

## 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 Internet Connection Screen

Use this screen to change your ZyXEL Device's WAN settings. Click **Network > WAN > Internet Connection**. The screen differs by the mode you select.

**Figure 27** WAN > Internet Connection (PPPoE)

The screenshot shows the 'Internet Connection' configuration page for a ZyXEL device. The 'General' tab is active, showing settings for a connection named 'INTERNET' using 'PPPoE' mode. Fields for 'User Name', 'Password', and 'Service Name' are present but empty. A checkbox for 'Retry when the authentication fails' is unchecked, and the 'Retry Interval' is set to 0. The 'IP Address' section has 'Obtain an IP Address Automatically' selected. The 'Connection' section has 'Nailed-Up Connection' selected, with a 'Max Idle Time' of 0 minutes. The 'NAT' section has 'Active NAT' checked, with 'Symmetric' and 'Fullcone' also checked. The 'DNS Servers' section has 'From ISP' selected, with both 'First DNS Server' and 'Second DNS Server' set to 0.0.0.0. At the bottom, there are 'Apply', 'Reset', and 'Advanced Setup' buttons.

The following table describes the labels in this screen.

**Table 9** WAN > Internet Connection

LABEL	DESCRIPTION
General	
Name	Specify a name for this connection. You can use up to 32 letters, numerals and any printable character found on a typical English language keyboard.

**Table 9** WAN > Internet Connection (continued)

LABEL	DESCRIPTION
Mode	<p>The ZyXEL Device is in routing mode by default. This allows multiple computers to share an Internet account. Select the method of encapsulation (<b>ENET ENCAP</b> or <b>PPPoE</b>) used by your ISP from the drop-down list box.</p> <p>Otherwise, select <b>Bridge</b> when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. If you select <b>Bridge</b>, you cannot use IP filter, DHCP server and NAT on the ZyXEL Device.</p>
User Name	(PPPoE encapsulation only) Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	(PPPoE encapsulation only) Enter the password associated with the user name above.
Service Name	(PPPoE encapsulation only) Type the name of your PPPoE service here.
Retry when the authentication fails	(PPPoE encapsulation only) Select this to have the ZyXEL Device send the password for authentication again if an attempt fails.
Retry Interval	(PPPoE encapsulation only) Type a number of seconds for the ZyXEL Device to wait before resending the password for authentication after an attempt has failed.
IP Address	<p>A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet.</p> <p>Select <b>Obtain an IP Address Automatically</b> if you have a dynamic IP address; otherwise select <b>Static IP Address</b> and type your ISP assigned IP address in the <b>IP Address</b> field below.</p>
IP Address	Enter the IP address assigned by your ISP if you select <b>Static IP Address</b> .
Subnet Mask	Enter a subnet mask in dotted decimal notation when you select <b>ENET ENCAP</b> in the <b>Mode</b> field.
Gateway IP address	You must specify a gateway IP address (supplied by your ISP) when you select <b>ENET ENCAP</b> in the <b>Mode</b> field.
Connection (PPPoE only)	
Nailed-Up Connection	Select <b>Nailed-Up Connection</b> when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select <b>Connect on Demand</b> when you don't want the connection up all the time and specify an idle time-out in the <b>Max Idle Time</b> field.
Max Idle Time	Specify an idle time-out in the <b>Max Idle Time</b> field when you select <b>Connect on Demand</b> . The default setting is 0, which means the Internet session will not timeout.
NAT	
Active NAT	Select this check box to enable NAT on this connection.

**Table 9** WAN > Internet Connection (continued)

LABEL	DESCRIPTION
Symmetric	Select this option to enable symmetric NAT on this connection. This field is available only when you select <b>Active NAT</b> .
Fullcone	Select this option to enable full cone NAT on this connection. This field is available only when you select <b>Active NAT</b> .
DNS Servers	Select <b>From ISP</b> if your ISP dynamically assigns DNS server information (and the ZyXEL Device's WAN IP address). Select <b>Static IP</b> if you have the IP address of a DNS server.
First DNS Server Second DNS Server	If you select <b>Static IP</b> , enter the DNS server's IP address in the field to the right.
VLAN	This section is available in this screen only when you select <b>Bridge</b> in the <b>Mode</b> field.
VLAN Active	Select this option to enable VLAN 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. All WAN connections share one MAC address. This allows the backbone switch to classify and service traffic based on the VLAN tag, instead of the MAC address.  Otherwise, disable VLAN multiplexing and each WAN connection has its own MAC address.  <b>Note:</b> This field is only configurable for the first WAN connection. When you change the setting here, all existing WAN connections will be removed except for the first WAN connection.
VLAN ID	Enter a VLAN ID number for traffic that goes through this connection.
Priority	Enter a priority level for traffic that goes through this connection.
Apply	Click this to save the changes.
Reset	Click this to begin configuring this screen afresh.
Advanced Setup	Click this button to display the <b>Advanced WAN Setup</b> screen and edit more details of your WAN setup.  This button is not available when you select <b>Bridge</b> in the <b>Mode</b> field.

## 5.4.1 Advanced Internet Connection Setup

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

**Figure 28** WAN > Internet Connection: Advanced Setup

The screenshot shows the 'WAN > Internet Connection: Advanced Setup' configuration page. It features three main sections: 'Multicast Setup', 'IP Filter', and 'VLAN'. In the 'Multicast Setup' section, 'IGMP Multicast' is set to 'Disable' and 'PPPoE Passthrough' is set to 'No'. The 'IP Filter' section has 'IP Filter Active' unchecked. The 'VLAN' section has 'VLAN Active' checked, 'VLAN ID' set to '1234', and 'Priority' set to '4'. At the bottom of the page are three buttons: 'Back', 'Apply', and 'Reset'.

The following table describes the labels in this screen.

**Table 10** WAN > Internet Connection: Advanced Setup

LABEL	DESCRIPTION
RIP & Multicast Setup	This section is not available when you configure the ZyXEL Device to be in bridge mode.
RIP Version	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers.  This field is available only when you select <b>ENET ENCAP</b> .  This shows the RIP version used for this WAN connection.
RIP Operation	This field is available only when you select <b>ENET ENCAP</b> .  This shows whether RIP is enabled ( <b>Active</b> ) or not ( <b>Disable</b> ) on this WAN connection.
IGMP Multicast	Multicast packets are sent to a group of computers on the LAN and are an alternative to unicast packets (packets sent to one computer) and broadcast packets (packets sent to every computer).  IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports both IGMP version 1 and version 2. Select <b>Enable</b> to turn on IGMP. Otherwise, select <b>Disable</b> .



**Table 10** WAN > Internet Connection: Advanced Setup (continued)

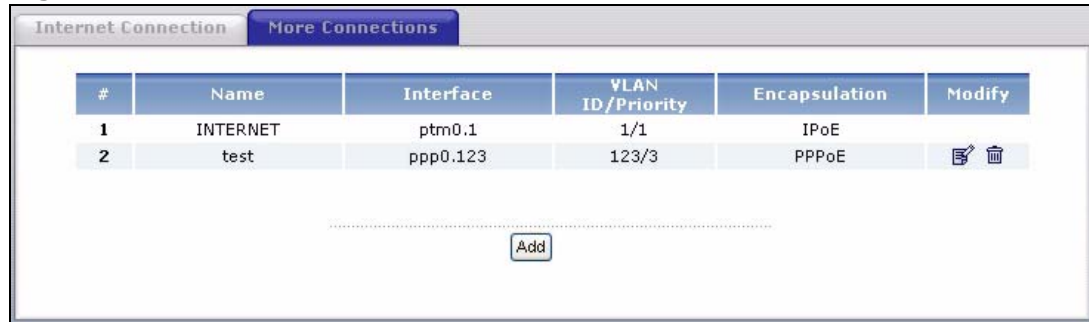
LABEL	DESCRIPTION
PPPoE Passthrough (PPPoE encapsulation only)	<p>This field is available when you select <b>PPPoE</b> encapsulation.</p> <p>In addition to the ZyXEL Device's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their 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>PPPoE pass through is an alternative to NAT for application where NAT is not appropriate.</p> <p>Disable PPPoE pass through 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>
IP Filter	This section is not available when you configure the ZyXEL Device to be in bridge mode.
IP Filter Active	Select this option to enable IP filtering on this connection.
VLAN	
VLAN Active	<p>Select this option to enable VLAN 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. All WAN connections share one MAC address. This allows the backbone switch to classify and service traffic based on the VLAN tag, instead of the MAC address.</p> <p>Otherwise, disable VLAN multiplexing and each WAN connection has its own MAC address.</p> <p><b>Note:</b> This field is only configurable for the first WAN connection. When you change the setting here, all existing WAN connections will be removed except for the first WAN connection.</p>
VLAN ID	Enter a VLAN ID number for traffic that goes through this connection.
Priority	Enter a priority level for traffic that goes through this connection.
Back	Click this to return to the previous screen.
Apply	Click this to save the changes.
Reset	Click this to restore your last-saved settings.

## 5.5 The More Connections Screen

The ZyXEL Device allows you to configure more than one Internet access connection. To configure additional Internet access connections click **Network > WAN > More Connections**. The screen differs by the encapsulation you select.

When you use the **WAN > Internet Connection** screen to set up Internet access, you are configuring the first WAN connection.

**Figure 29** WAN > More Connections



The following table describes the labels in this screen.

**Table 11** WAN > More Connections

LABEL	DESCRIPTION
#	This is an index number indicating the number of the corresponding connection.
Name	This is the name you gave to the Internet connection.
Interface	<p>This shows the name of the ZyXEL Device's interface used by this connection.</p> <p><b>ptm0</b> indicates the WAN using ENET ENCAP or in bridge mode.  <b>ppp0</b> indicates the WAN interface using PPPoE.</p> <p>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>
VLAN ID/ Priority	This field shows the VLAN ID number and priority configured for this WAN connection when VLAN multiplexing is enabled. Otherwise, it shows <b>disable</b> .
Encapsulation	This field indicates the encapsulation method of the Internet connection.
Modify	<p>The first (ISP) connection is read-only in this screen. Use the <b>WAN &gt; Internet Connection</b> screen to edit it.</p> <p>Click the edit icon to edit the Internet connection settings. Click this icon on an empty configuration to add a new Internet access setup.</p> <p>Click the remove icon to delete the Internet access setup from your connection list.</p>
Add	Click this to add a new connection.

## 5.5.1 More Connections Edit

Click the edit icon or **Add** button in the **More Connections** screen to configure a connection.

**Figure 30** WAN > More Connections: Edit

**General**

☒ Active

Name:

Mode: PPPoE

User Name:

Password:

Service Name:

☐ Retry when the authentication fails

Retry Interval:

**IP Address**

☒ Obtain an IP Address Automatically

☐ Static IP Address

IP Address:

**Connection**

☒ Nailed-Up Connection

☐ Connect on Demand

Max Idle Time:  Mins.

**NAT**

☐ Active NAT

☒ Symmetric

☐ Fullcone

The following table describes the labels in this screen.

**Table 12** WAN > More Connections: Edit

LABEL	DESCRIPTION
General	
Active	Select the check box to activate or clear the check box to deactivate this connection.
Name	Specify a name for this connection. You can use up to 32 letters, numerals and any printable character found on a typical English language keyboard.

**Table 12** WAN > More Connections: Edit (continued)

LABEL	DESCRIPTION
Mode	<p>The ZyXEL Device is in routing mode by default. This allows multiple computers to share an Internet account. Select the method of encapsulation (<b>ENET ENCAP</b> or <b>PPPoE</b>) used by your ISP from the drop-down list box.</p> <p>Otherwise, select <b>Bridge</b> when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. If you select <b>Bridge</b>, you cannot use IP filter, DHCP server and NAT on the ZyXEL Device.</p>
User Name	(PPPoE encapsulation only) Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	(PPPoE encapsulation only) Enter the password associated with the user name above.
Service Name	(PPPoE encapsulation only) Type the name of your PPPoE service here.
Retry when the authentication fails	(PPPoE encapsulation only) Select this to have the ZyXEL Device send the password for authentication again if an attempt fails.
Retry Interval	(PPPoE encapsulation only) Type a number of seconds for the ZyXEL Device to wait before resending the password for authentication after an attempt has failed.
IP Address	<p>A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet.</p> <p>Select <b>Obtain an IP Address Automatically</b> if you have a dynamic IP address; otherwise select <b>Static IP Address</b> and type your ISP assigned IP address in the <b>IP Address</b> field below.</p>
IP Address	Enter the IP address assigned by your ISP if you select <b>Static IP Address</b> .
Subnet Mask	Enter a subnet mask in dotted decimal notation when you select <b>ENET ENCAP</b> in the <b>Mode</b> field.
Gateway IP address	You must specify a gateway IP address (supplied by your ISP) when you select <b>ENET ENCAP</b> in the <b>Mode</b> field.
Connection (PPPoE only)	
Nailed-Up Connection	Select <b>Nailed-Up Connection</b> when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select <b>Connect on Demand</b> when you don't want the connection up all the time and specify an idle time-out in the <b>Max Idle Time</b> field.
Max Idle Time	Specify an idle time-out in the <b>Max Idle Time</b> field when you select <b>Connect on Demand</b> . The default setting is 0, which means the Internet session will not timeout.
NAT	
Active NAT	Select this check box to enable NAT on this connection.

**Table 12** WAN > More Connections: Edit (continued)

LABEL	DESCRIPTION
Symmetric	Select this option to enable symmetric NAT on this connection. This field is available only when you select <b>Active NAT</b> .
Fullcone	Select this option to enable full cone NAT on this connection. This field is available only when you select <b>Active NAT</b> .
VLAN	This section is available in this screen only when you select <b>Bridge</b> in the <b>Mode</b> field.
VLAN Active	Select this option to enable VLAN 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. All WAN connections share one MAC address. This allows the backbone switch to classify and service traffic based on the VLAN tag, instead of the MAC address.  Otherwise, disable VLAN multiplexing and each WAN connection has its own MAC address.  <b>Note:</b> This field is only configurable for the first WAN connection. When you change the setting here, all existing WAN connections will be removed except for the first WAN connection.
VLAN ID	Enter a VLAN ID number for traffic that goes through this connection.
Priority	Enter a priority level for traffic that goes through this connection.
Back	Click this to return to the <b>More Connections</b> screen with saving your changes.
Apply	Click this to save the changes.
Reset	Click this to begin configuring this screen afresh.
Advanced Setup	Click this button to display the <b>More Connections Advanced Setup</b> screen and edit more details of your WAN setup.  This button is not available when you select <b>Bridge</b> in the <b>Mode</b> field.

## 5.5.2 Configuring More Connections Advanced Setup

To edit your ZyXEL Device's advanced WAN settings, click the **Advanced Setup** button in the **More Connections Edit** screen. The screen appears as shown.

**Figure 31** WAN > More Connections: Edit: Advanced Setup

**RIP & Multicast Setup**

RIP Version: RIPv1  
 RIP Operation: Disabled  
 IGMP Multicast: Disable

**IP Filter**

☐ IP Filter Active

**VLAN**

☒ VLAN Active  
 VLAN ID: [0-4095]  
 Priority: [0-7]

Back Apply Reset

The following table describes the labels in this screen.

**Table 13** WAN > More Connections: Edit: Advanced Setup

LABEL	DESCRIPTION
RIP & Multicast Setup	This section is not available when you configure the ZyXEL Device to be in bridge mode.
RIP Version	<p>RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The version field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). RIP-1 is universally supported; but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.</p> <p>This field is available only when you select <b>ENET ENCAP</b>.</p> <p>Select the RIP version from <b>RIPv1</b>, <b>RIPv2</b> and <b>RIPv1v2</b>.</p>
RIP Operation	<p>This field is available only when you select <b>ENET ENCAP</b>.</p> <p>Select <b>Active</b> to enable RIP. Otherwise, select <b>Disable</b>.</p>
IGMP Multicast	<p>Multicast packets are sent to a group of computers on the LAN and are an alternative to unicast packets (packets sent to one computer) and broadcast packets (packets sent to every computer).</p> <p>IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports both IGMP version 1 and version 2. Select <b>Enable</b> to turn on IGMP. Otherwise, select <b>Disable</b>.</p>

**Table 13** WAN > More Connections: Edit: Advanced Setup (continued)

LABEL	DESCRIPTION
PPPoE Passthrough (PPPoE encapsulation only)	<p>This field is available when you select <b>PPPoE</b> encapsulation.</p> <p>In addition to the ZyXEL Device's built-in PPPoE client, you can enable PPPoE pass through 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>PPPoE pass through is an alternative to NAT for application where NAT is not appropriate.</p> <p>Disable PPPoE pass through 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>
IP Filter	This section is not available when you configure the ZyXEL Device to be in bridge mode.
IP Filter Active	Select this option to enable IP filtering on this connection.
VLAN	
VLAN Active	<p>Select this option to enable VLAN 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. All WAN connections share one MAC address. This allows the backbone switch to classify and service traffic based on the VLAN tag.</p> <p>Otherwise, disable VLAN multiplexing and each WAN connection has its own MAC address.</p> <p><b>Note:</b> This field is only configurable for the first WAN connection. When you change the setting here, all existing WAN connections will be removed except for the first WAN connection.</p>
VLAN ID	Enter a VLAN ID number for traffic that goes through this connection.
Priority	Enter a priority level for traffic that goes through this connection.
Back	Click this to return to the previous screen.
Apply	Click this to save the changes.
Reset	Click this to restore your last-saved settings.

## 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.

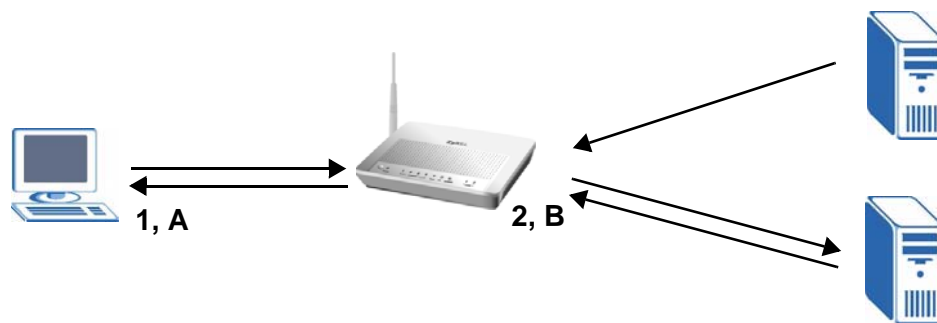


## Full Cone NAT

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 32** Full Cone NAT Example



## Symmetric NAT

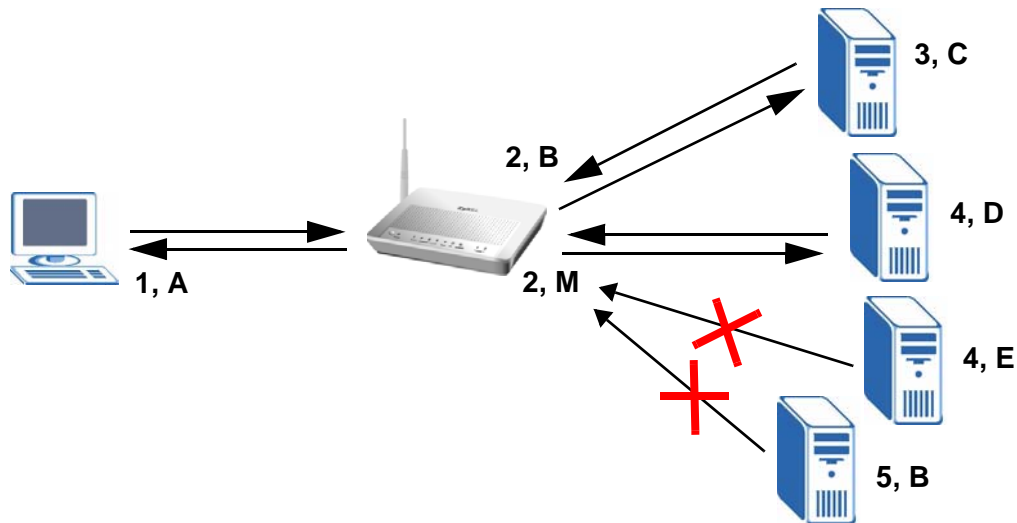
The full, restricted and port restricted cone NAT types use the same mapping for an outgoing packet's source address regardless of the destination IP address and port. In symmetric NAT, the mapping of an outgoing packet's source address to a source address in another network is different for each different 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 33** 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](http://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.

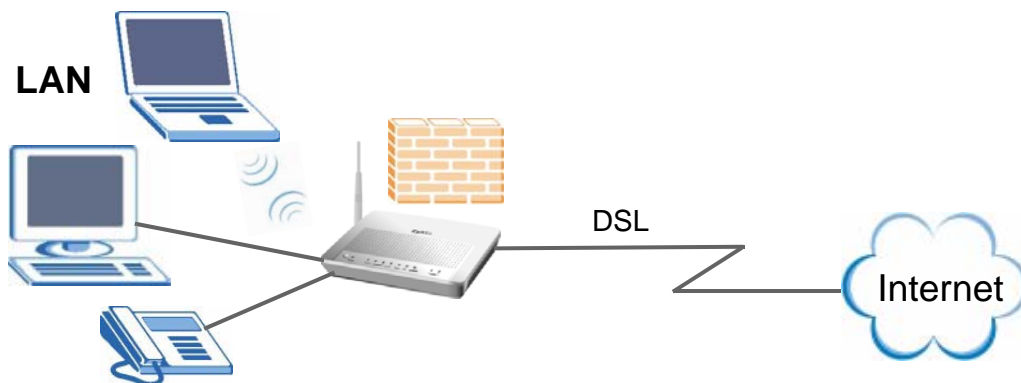
- 1** The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
- 2** If your ISP dynamically assigns the DNS server IP addresses (along with the ZyXEL Device's WAN 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 6.7 on page 75](#) for more information on LANs.
- See [Appendix D on page 247](#) 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 the ZyXEL Device's DHCP settings ([Section 6.4 on page 71](#)).
- The **Client List** screen lets you assign IP addresses on the LAN to specific individual computers based on their MAC Addresses ([Section 6.5 on page 72](#)).
- The **IP Alias** screen lets you change your ZyXEL Device's IP alias settings ([Section 6.6 on page 73](#)).

## 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.

### 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 Before You Begin

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

## 6.4 The LAN IP Screen

Click **Network > LAN** to open the **IP** screen. See [Section 6.7 on page 75](#) for background information. Use this screen to set the Local Area Network IP address and subnet mask of your ZyXEL Device.

Follow these steps to configure your LAN settings.

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

**Figure 34** LAN > IP

IP	
Client List IP Alias	
LAN TCP/IP	
IP Address	192.168.1.1
IP Subnet Mask	255.255.255.0
DHCP Setup	
<input checked="" type="checkbox"/> Active DHCP Server	
IP Pool Starting Address	192.168.1.33
Pool Size	222
IGMP Snooping	
<input checked="" type="checkbox"/> Active IGMP Snooping	
Apply	

The following table describes the fields in this screen.

**Table 14** LAN > IP

LABEL	DESCRIPTION
LAN TCP/IP	
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 Server	<p>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.</p> <p>Otherwise, deselect this to not have the ZyXEL Device provide any DHCP services. The DHCP server will be disabled.</p> <p>When the ZyXEL Device acts as a DHCP server, the following items need to be set:</p>
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
IGMP Snooping	
Active IGMP Snooping	Select this option to enable IGMP snooping. This allows the ZyXEL Device to passively learn multicast group.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.

## 6.5 The Client List Screen

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

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



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

**Figure 35** LAN > Client List

IPClient ListIP Alias

DHCP Client Table

IP Address0.0.0.0MAC Address00:00:00:00:00:00Add Entries

#	IP Address	MAC Address	Remove
0	192.168.1.99	00:35:12:34:56:e8	<input type="checkbox"/>
1	192.168.1.55	00:c5:01:23:45:67	<input type="checkbox"/>
2	192.168.1.33	00:21:85:0c:44:4b	<input type="checkbox"/>

The following table describes the labels in this screen.

**Table 15** LAN > Client List

LABEL	DESCRIPTION
IP Address	Enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify.
MAC Address	Enter the MAC address of a computer on your LAN.
Add Entries	Click this to add a static DHCP entry before the dynamic DHCP entry(ies).
#	This is the index number of the static IP table entry (row).
IP Address	This field displays the IP address relative to the # field listed above.
MAC Address	<div>The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation).</div> <div>A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.</div>
Remove	Click this to delete a static DHCP entry. You cannot delete a dynamic DHCP entry. A window displays asking you to confirm that you want to delete the selected entry.

## 6.6 The IP Alias Screen

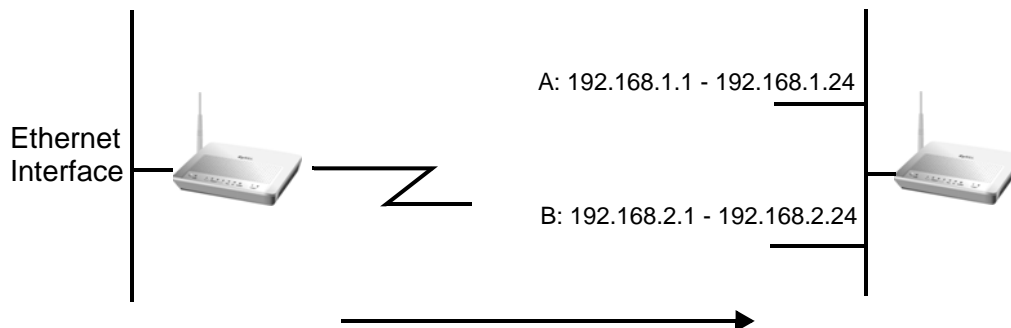
IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The ZyXEL Device supports three logical LAN interfaces via its single physical Ethernet interface with the ZyXEL Device itself as the gateway for each LAN network.

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 36** Physical Network & Partitioned Logical Networks



## 6.6.1 Configuring the LAN IP Alias Screen

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

**Figure 37** Network > LAN > IP Alias

The screenshot shows the 'IP Alias' configuration screen. It features a tabbed interface with 'IP Alias' selected. Below the tab, there is a section titled 'IP Alias' with a checkbox labeled 'Active IP Alias'. Below the checkbox are two input fields: 'IP Address' and 'IP Subnet Mask', both containing '0.0.0.0'. An 'Apply' button is located at the bottom right of the section.

The following table describes the labels in this screen.

**Table 16** Network > LAN > IP Alias

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 this to save your changes back to the ZyXEL Device.

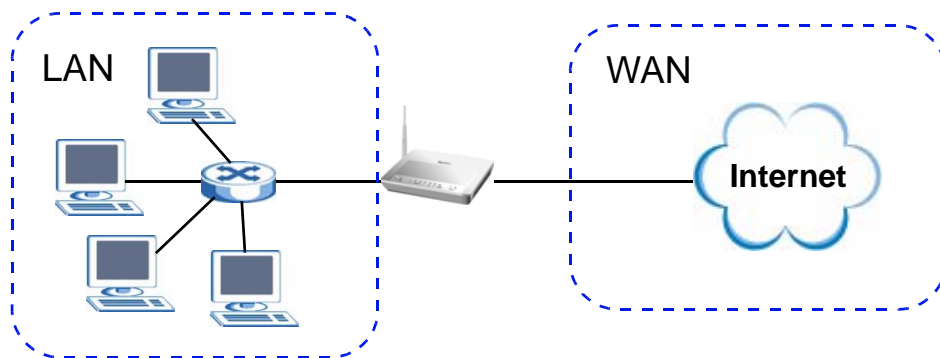
## 6.7 Technical Reference

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 38** 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.



# 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 25](#) for a tutorial showing how to set up your wireless connection in an example scenario.

See [Section 7.9 on page 94](#) 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 82](#)).
- 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 7.5 on page 89](#)) 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 7.6 on page 91](#)) screen to set up WPS by pressing a button or using a PIN.

- The **MAC Filter** screen lets you configure the MAC filter to allow or block access to the ZyXEL Device based on the MAC addresses of the wireless stations ([Section 7.7 on page 91](#)).

- The **Advanced Setup** screen lets you change the wireless mode, and make other advanced wireless configuration changes ([Section 7.8 on page 93](#)).

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 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 80](#) 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 39** Network > Wireless LAN > General

The following table describes the labels in this screen.

**Table 17** Network > Wireless LAN > General

LABEL	DESCRIPTION
Active Wireless LAN	Click the check box to activate wireless LAN.
Network Name (SSID)	<p>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.</p> <p><b>Note:</b> 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 <b>Apply</b> to confirm. You must then change the wireless settings of your computer to match the ZyXEL Device's new settings.</p>
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.
Channel Selection	<p>Set the operating frequency/channel depending on your particular region.</p> <p>Select a channel from the drop-down list box.</p>
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.
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 40** Wireless LAN > General: No Security

The screenshot shows the 'General' tab of the Wireless LAN configuration interface. Under the 'Wireless Setup' section, 'Active Wireless LAN' is checked, 'Network Name(SSID)' is 'ZyXEL', 'Hide Network Name(SSID)' is unchecked, 'Channel Selection' is '6', and 'BSSID' is '00:19:CB:D1:79:05'. Under the 'Security' section, 'Security Mode' is set to 'No Security'. 'Apply' and 'Reset' buttons are at the bottom.

The following table describes the labels in this screen.

**Table 18** Wireless LAN > General: No Security

LABEL	DESCRIPTION
Security Mode	Choose <b>No Security</b> 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 41** Wireless LAN > General: Static WEP Encryption

The screenshot shows the 'General' tab of the 'Wireless LAN' configuration interface. The 'Wireless Setup' section includes:
 

- ☒ Active Wireless LAN
- Network Name(SSID): ZyXEL
- ☐ Hide Network Name(SSID)
- Channel Selection: 6
- BSSID: 00:19:CB:D1:79:05

 The 'Security' section includes:
 

- Security Mode: WEP
- WEP Encryption: 128-bit WEP
- 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.)
- Four radio buttons for Key 1, Key 2, Key 3, and Key 4, each followed by an empty text input field. Key 1 is selected.
- 'Apply' and 'Reset' buttons at the bottom.

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

**Table 19** Network > Wireless LAN > General: Static WEP Encryption

LABEL	DESCRIPTION
Security Mode	Choose <b>Static WEP</b> from the drop-down list box.

**Table 19** Network > Wireless LAN > General: Static WEP Encryption

LABEL	DESCRIPTION
WEP Encryption	WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network. Select <b>64-bit WEP</b> or <b>128-bit WEP</b> to enable data encryption.
Key 1 to Key 4	If you chose <b>64-bit WEP</b> in the <b>WEP Encryption</b> 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 <b>128-bit WEP</b> in the <b>WEP Encryption</b> field, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.  There are four data encryption keys 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.

### 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 42** Wireless LAN > General: WPA(2)-PSK

The screenshot shows the 'Wireless LAN > General' configuration page. The 'General' tab is selected. Under 'Wireless Setup', 'Active Wireless LAN' is checked, 'Network Name(SSID)' is 'ZyXEL', 'Hide Network Name(SSID)' is unchecked, 'Channel Selection' is '6', and 'BSSID' is '00:19:CB:D1:79:05'. Under 'Security', 'Security Mode' is 'WPA2-PSK', 'Active Compatible' is checked, 'WPA-PSK Compatible' is checked, 'Pre-Shared Key' is '12345678', 'Group Key Update Timer' is '1800 sec', and 'WPA Encryption' is 'TKIP'. 'Apply' and 'Cancel' buttons are at the bottom.

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

**Table 20** Wireless LAN > General: WPA(2)-PSK

LABEL	DESCRIPTION
Security Mode	Choose <b>WPA-PSK</b> or <b>WPA2-PSK</b> 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.
Pre-Shared Key	<p>The encryption mechanisms used for <b>WPA(2)</b> and <b>WPA(2)-PSK</b> are the same. The only difference between the two is that <b>WPA(2)-PSK</b> uses a simple common password, instead of user-specific credentials.</p> <p>Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).</p>
(WPA) Group Key Update Timer	<p>The <b>(WPA) Group Key Update Timer</b> is the rate at which the AP (if using <b>WPA(2)-PSK</b> key management) or <b>RADIUS</b> server (if using WPAWPA(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 <b>(WPA) Group Key Update Timer</b> is also supported in <b>WPA(2)-PSK</b> mode. The ZyXEL Device default is <b>1800</b> seconds (30 minutes).</p>
WPA Encryption	Select the encryption type ( <b>TKIP</b> or <b>AES</b> ) for data encryption.

## 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 43** Wireless LAN > General: WPA(2)

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

**Table 21** Wireless LAN > General: WPA(2)

LABEL	DESCRIPTION
Security Mode	Choose <b>WPA</b> or <b>WPA2</b> 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.
WPA Encryption	Select the encryption type ( <b>TKIP</b> or <b>AES</b> ) for data encryption.
WPA2 Preauthentication	This field is available only when you select <b>WPA2</b> . 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 <b>Enabled</b> to turn on preauthentication in WAP2. Otherwise, select <b>Disabled</b> .



**Table 21** Wireless LAN > General: WPA(2)

LABEL	DESCRIPTION
ReAuthentication Timer	<p>This field is available only when you select <b>WPA2</b>.</p> <p>Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes).</p> <p><b>Note:</b> If wireless station authentication is done using a <b>RADIUS</b> server, the reauthentication timer on the <b>RADIUS</b> server has priority.</p>
Group Key Update Timer	<p>This field is available only when you select <b>WPA</b>.</p> <p>The <b>Group Key Update Timer</b> is the rate at which the AP (if using <b>WPA(2)-PSK</b> key management) or <b>RADIUS</b> 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 <b>Group Key Update Timer</b> is also supported in <b>WPA(2)-PSK</b> mode. The ZyXEL Device default is <b>1800</b> seconds (30 minutes).</p>
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	<p>Enter the port number of the external authentication server. The default port number is <b>1812</b>.</p> <p>You need not change this value unless your network administrator instructs you to do so with additional information.</p>
Shared Secret	<p>Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the ZyXEL Device.</p> <p>The key must be the same on the external authentication server and your ZyXEL Device. The key is not sent over the network.</p>

## 7.5 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 44** Network > Wireless LAN > WPS

The following table describes the labels in this screen.

**Table 22** 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 <b>Configured</b> when the ZyXEL Device has connected to a wireless network using WPS or <b>Enable WPS</b> 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 <b>Unconfigured</b> if WPS is disabled and there is no wireless or wireless security changes on the ZyXEL Device or you click <b>Release_Configuration</b> to remove the configured wireless and wireless security settings.
Release_Configuration	This button is available when the WPS status is <b>Configured</b> .  Click this button to remove all configured wireless and wireless security settings for WPS connections on the ZyXEL Device.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Refresh	Click <b>Refresh</b> to reload the previous configuration for this screen.

## 7.6 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 45** Network > Wireless LAN > WPS Station

**General** **WPS** **WPS Station** **MAC Filter** **Advanced Setup**

**Add Station by WPS**

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

**Push-Button**

Or input station's PIN number:  **Start**

**Note :**

1. The Push Button Configuration requires pressing a button on both the station and AP within 120 seconds.
2. You may find the PIN number in the station's utility.
3. This feature is available only when WPA-PSK, WPA2 PSK or OPEN mode is configured.

The following table describes the labels in this screen.

**Table 23** 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 <b>Push Button</b> on this screen.</p> <p><b>Note:</b> 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 <b>Start</b> 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><b>Note:</b> You must also activate WPS on that device within two minutes to have it present its PIN to the ZyXEL Device.</p>

## 7.7 The MAC Filter Screen

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 **Network > Wireless LAN > MAC Filter**. The following screen displays.

**Figure 46** Wireless LAN > MAC Filter

The following table describes the labels in this screen.

**Table 24** Wireless LAN > MAC Filter

LABEL	DESCRIPTION
Active MAC Filter	Select the check box to enable MAC address filtering.
MAC Restrict Mode	Define the filter action for the list of MAC addresses in the table below. Select <b>Allow</b> to permit access to the ZyXEL Device, MAC addresses not listed will be denied access to the ZyXEL Device. Select <b>Deny</b> to block access to the ZyXEL Device, MAC addresses not listed will be allowed to access the ZyXEL Device
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.
Add Entries	Click this to save and insert the entry to the table below.
Set	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.
Remove	Select the entry(ies) that you want to delete in the <b>Remove</b> column, then click the <b>Remove</b> button.
Apply	Click this to save your changes back to the ZyXEL Device.
Remove	Click this to delete the selected entry(ies).

## 7.8 The Advanced Setup Screen

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

**Figure 47** Wireless LAN > Advanced Setup

The screenshot shows the 'Wireless Advanced Setup' configuration page. It includes the following settings:

- RTS/CTS Threshold:** 2344
- Fragmentation Threshold:** 2344
- Number of Wireless Stations Allowed:** 16
- Output Power:** 100%
- Multicast Rate:** 1 Mbps
- 54g™ Mode:** 54g Auto
- 54g™ Protection:** Auto
- Preamble:** Long

Buttons for 'Apply' and 'Reset' are located at the bottom right of the configuration area.

The following table describes the labels in this screen.

**Table 25** 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 <b>20%</b> , <b>40%</b> , <b>60%</b> , <b>80%</b> or <b>100%</b> .
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.

**Table 25** Wireless LAN > Advanced Setup

LABEL	DESCRIPTION
54g <sup>TM</sup> Mode	<p>Select <b>54g Auto</b> 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.</p> <p>Select <b>54g Performance</b> to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device.</p> <p>Select <b>802.11b Only</b> 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.</p>
54g <sup>TM</sup> Protection	<p>Enabling this feature can help prevent collisions in mixed-mode networks (networks with both IEEE 802.11b and IEEE 802.11g traffic).</p> <p>Select <b>Auto</b> to have the wireless devices transmit data after a RTS/CTS handshake. This helps improve IEEE 802.11g performance.</p> <p>Select <b>Off</b> to disable 54g protection. The transmission rate of your ZyXEL Device might be reduced in a mixed-mode network.</p> <p>This field displays <b>Off</b> and is not configurable when you set <b>54g<sup>TM</sup> Mode</b> to <b>802.11b Only</b>.</p>
Preamble	<p>Select a preamble type from the drop-down list menu. Choices are <b>Long</b> or <b>Short</b>. The default setting is <b>Long</b>. See the appendix for more information.</p> <p>This field displays <b>Short</b> and is not configurable when you set <b>54g<sup>TM</sup> Mode</b> to <b>54g Performance</b>.</p>
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to reload the previous configuration for this screen.

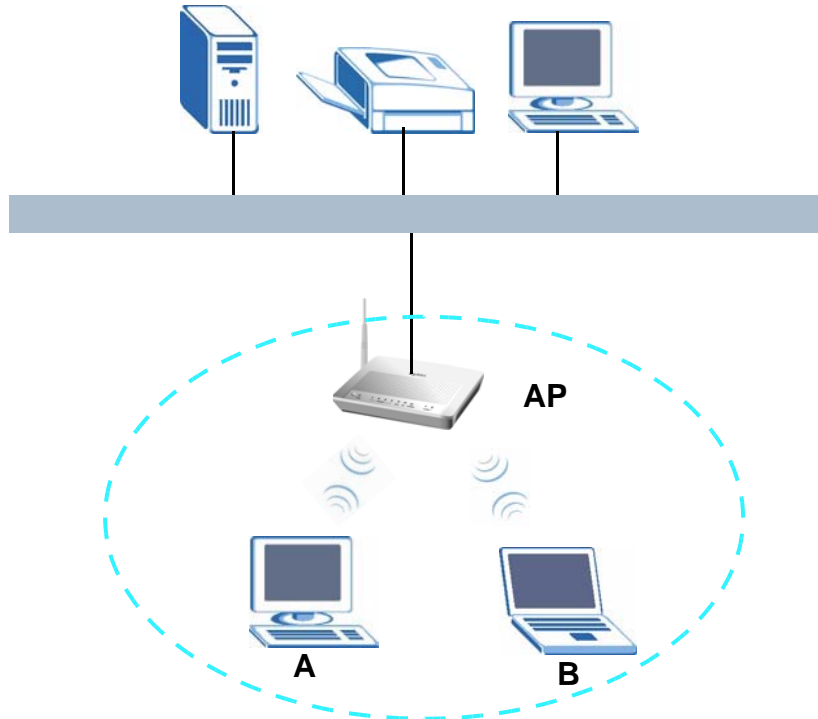
## 7.9 Technical Reference

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

## 7.9.1 Wireless Network Overview

The following figure provides an example of a wireless network.

**Figure 48** 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.

## 7.9.2 Additional Wireless Terms

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

**Table 26** Additional Wireless Terms

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

## 7.9.3 Wireless Security Overview

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

### 7.9.3.1 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.

### 7.9.3.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.<sup>1</sup> A MAC address is usually written using twelve hexadecimal



characters<sup>2</sup>; 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.

### 7.9.3.3 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.

### 7.9.3.4 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.

- 
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.

The types of encryption you can choose depend on the type of authentication. (See [Section 7.9.3.3 on page 97](#) for information about this.)

**Table 27** 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.

## 7.9.4 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.

#### **7.9.4.1 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 7.6 on page 91](#)).
- 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.

#### **7.9.4.2 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 7.5 on page 89](#)).
- 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.

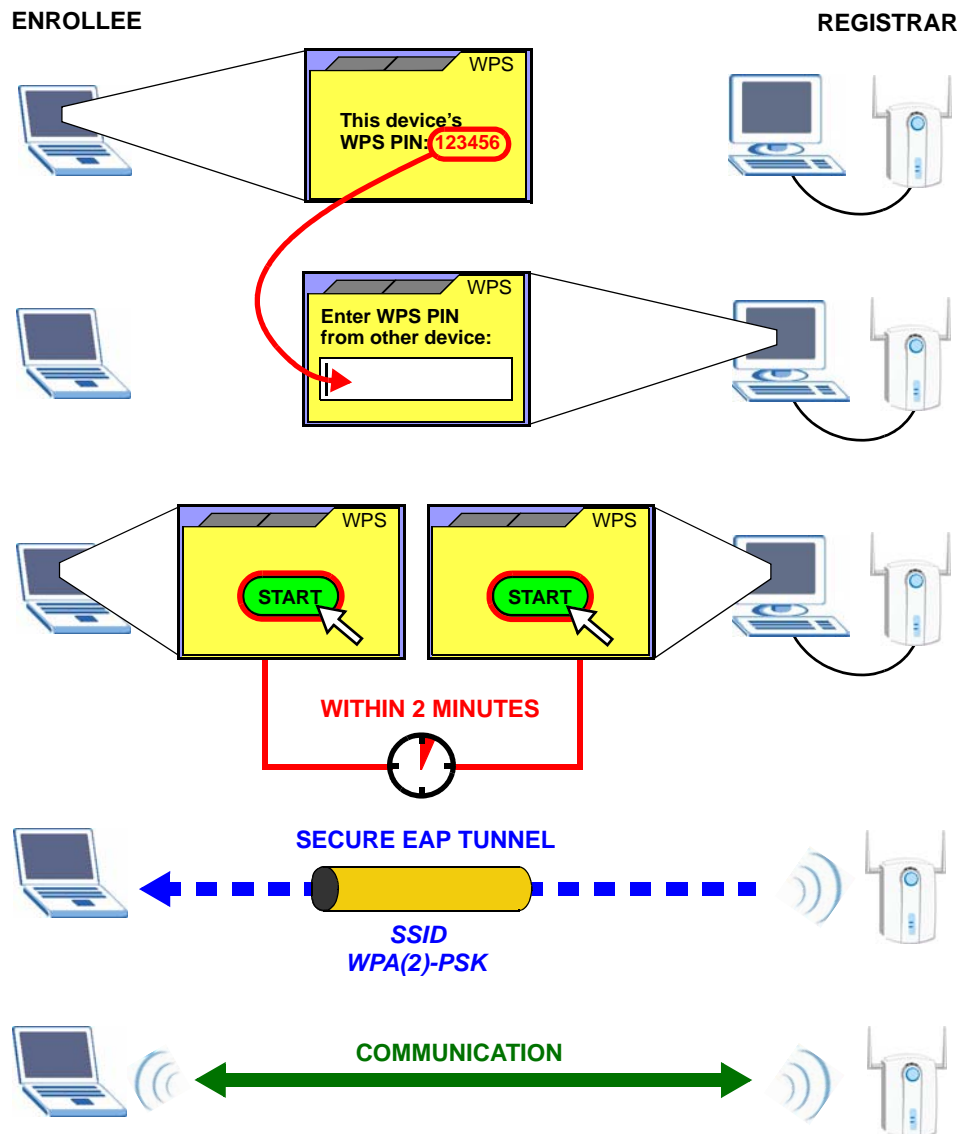
**Note:** Use the configuration utility to activate WPS, not the push-button on the device itself.

- 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 49** Example WPS Process: PIN Method

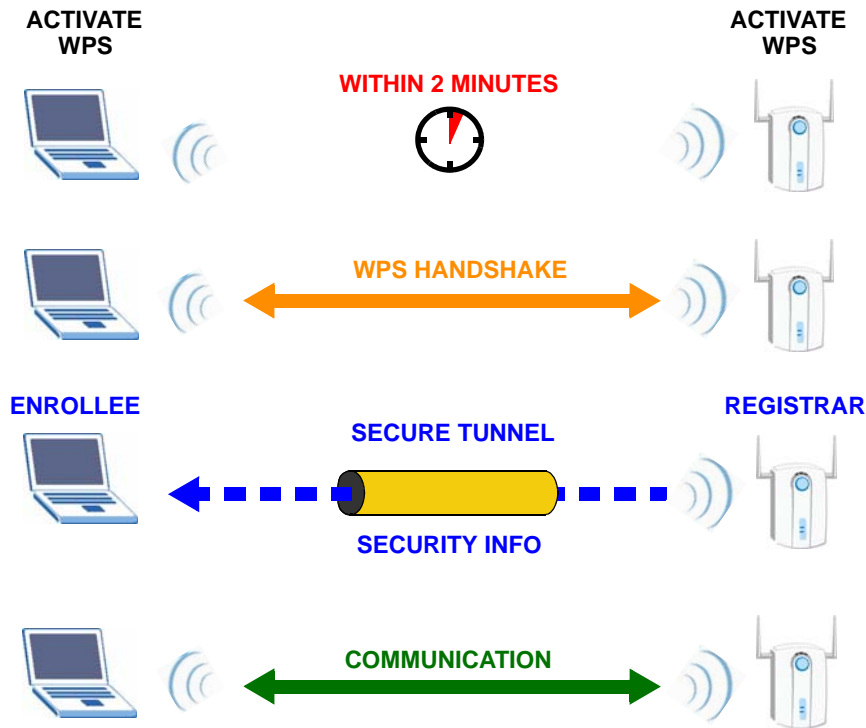


### 7.9.4.3 How WPS Works

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 50** 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.

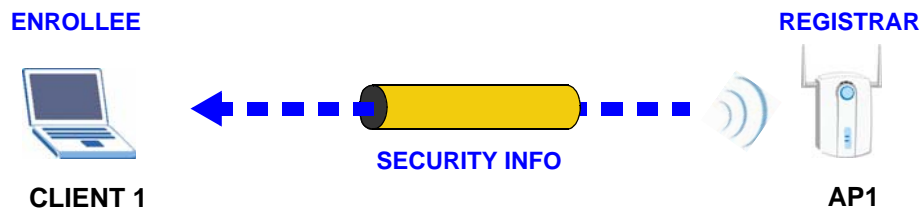
By default, a WPS device is "unconfigured". This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled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

### 7.9.4.4 Example WPS Network Setup

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

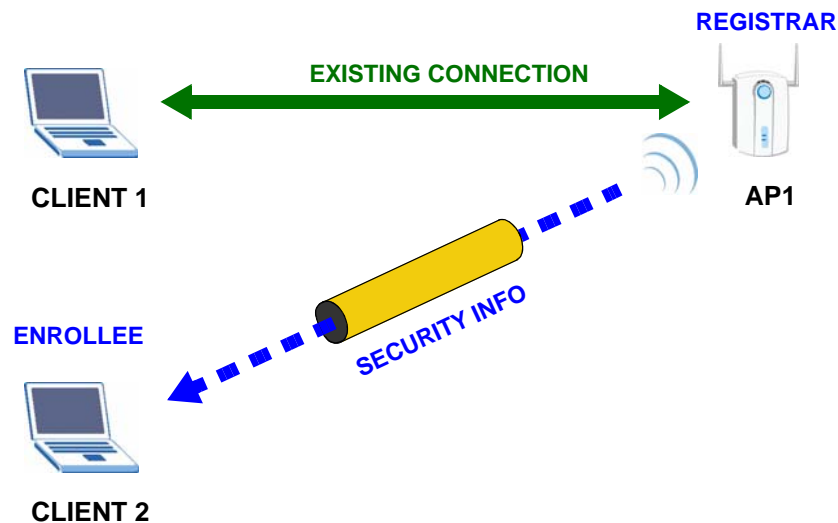
The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information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

**Figure 51** 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**.

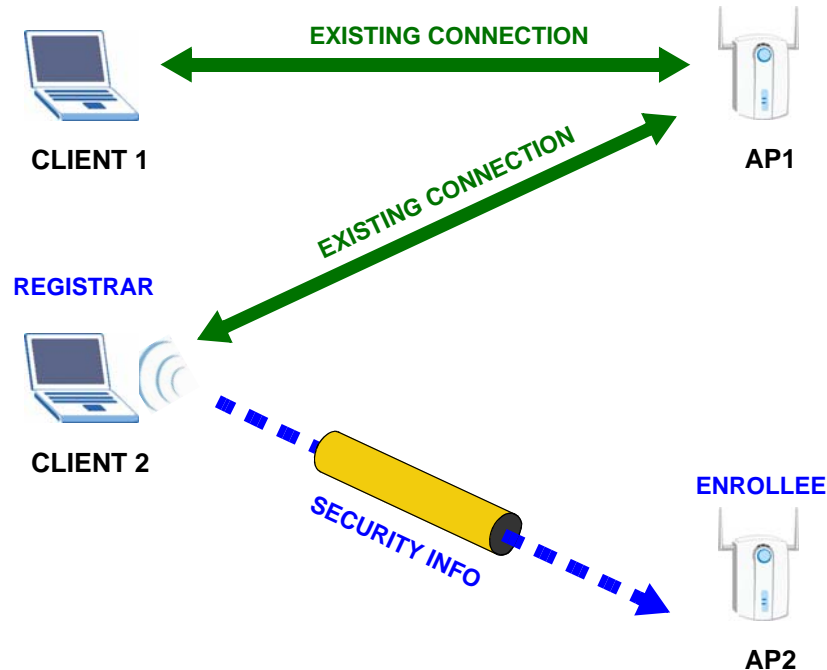
**Figure 52** WPS: Example Network Step 2



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 53** WPS: Example Network Step 3



#### 7.9.4.5 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 108](#)).
- The **DMZ Host** screen lets you configure a default server ([Section 8.4 on page 111](#)).

## 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 54** NAT Port Forwarding

The screenshot shows the 'Port Forwarding' configuration window. It has two tabs: 'Port Forwarding' (selected) and 'DMZ Host'. The 'Port Forwarding' tab contains a form for adding new rules and a table of existing rules.

**Form Fields:**

- Service Name: WWW (dropdown)
- WAN Interface: INTERNET/ptm0\_1 (dropdown)
- Server IP Address: 192.168.1. (text)
- External port: Start: 80, End: 80
- Internal port: Start: 80, End: 80
- Protocol: TCP (dropdown)
- Add button

**Table of Port Forwarding Rules:**

No.	Active	Service Name	WAN Interface	External Start Port	External End Port	Internal Start Port	Internal End Port	Server IP Address	Modify
1	<input checked="" type="checkbox"/>	RealAudio	ptm0_1	6790	32000	6790	32000	192.168.1.100	

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

The following table describes the labels in this screen.

**Table 28** 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 <b>External port</b>, <b>Internal port</b> and <b>Protocol</b> fields.</p> <p>Otherwise, select <b>User Define</b> to open the <b>Rule Setup</b> 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.
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 <b>External Port End</b> field.</p> <p>To forward a series of ports, enter the start port number here and the end port number in the <b>External Port End</b> 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 <b>External Port Start</b> 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 <b>External Port Start</b> 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 <b>Internal Port End</b> 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 shows the WAN interface through which the service is forwarded.
External Port Start	This is the first external port number that identifies a service.
External Port End	This is the last external port number that identifies a service.
Internal Port Start	This is the first internal port number that identifies a service.

**Table 28** NAT Port Forwarding (continued)

LABEL	DESCRIPTION
Internal Port End	This is the last internal port number that identifies a service.
Server IP Address	This field displays the destination IP address for the packet.
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 <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> 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 55** Port Forwarding Edit

The following table describes the labels in this screen.

**Table 29** 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 <b>Port Forwarding</b> screen.
WAN Interface	Select a WAN interface for which you want to configure port forwarding rules.

**Table 29** Port Forwarding Edit (continued)

LABEL	DESCRIPTION
External Start Port	Enter the original destination port for the packets.  To forward only one port, enter the port number again in the <b>External End Port</b> field.  To forward a series of ports, enter the start port number here and the end port number in the <b>External End Port</b> 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 <b>External Start Port</b> 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 <b>External Start Port</b> 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.
Server IP Address	Enter the inside IP address of the virtual server here.
Protocol	Select the protocol supported by this virtual server. Choices are <b>TCP</b> , <b>UDP</b> , or <b>TCP/UDP</b> .
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 8.4 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 56** NAT - DMZ Host

Port Forwarding **DMZ Host**

**DMZ Host**

Default Server

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

Save

The following table describes the fields in this screen.

**Table 30 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 <b>NAT Port Forwarding</b> screen.  Note: If you do not assign a <b>Default Server</b> , the ZyXEL Device discards all packets received for ports that are not specified in the <b>NAT Port Forwarding</b> screen.
Save	Click <b>Save</b> to save your changes back to the ZyXEL Device.

## 8.5 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 31 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
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

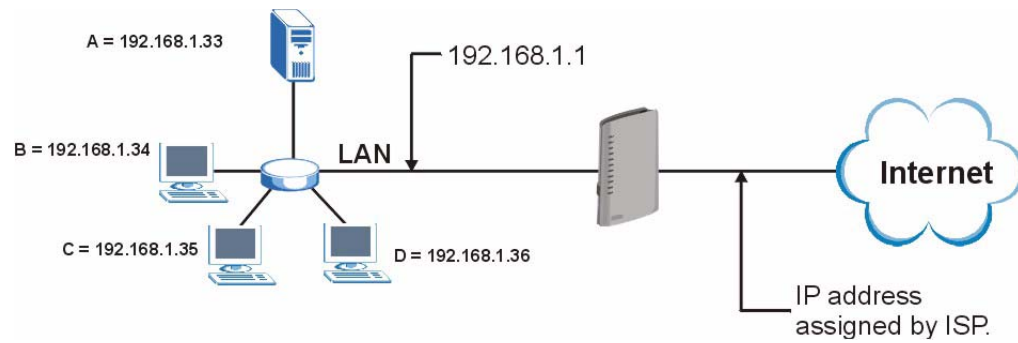
### Port Forwarding Example

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 57** Multiple Servers Behind NAT Example





---

# PART III

## Security

---

[IP Filter \(117\)](#)



# IP Filter

## 9.1 Overview

This chapter shows you how to enable and configure the ZyXEL Device IP filtering 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.

### 9.1.1 What You Can Do in this Chapter

The **IP Filtering Incoming** screen lets you view and configure incoming IP filtering rules ([Section 9.3 on page 118](#)).

## 9.2 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 32** 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.

## 9.3 The Incoming IP Filtering Screen

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

**Figure 58** Incoming IP Filter

**Incoming**

**Incoming IP Filtering Setup**

When the firewall is enabled on a WAN or LAN 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 IP filters.

Active	Filter Name	Interfaces	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
<input checked="" type="checkbox"/>	example	ptm0_1	None			192.168.1.99 / 255.255.255.0		<input type="checkbox"/>

The following table describes the labels in this screen.

**Table 33** Incoming IP Filtering

<b>LABEL</b>	<b>DESCRIPTION</b>
Active	Select this check box to enable the rule.
Filter Name	This displays the name of the rule.
Interfaces	This displays the WAN interface 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 <b>Any</b> .
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 <b>Any</b> .
Dest. Port	This is the destination port number.
Remove	Select the rule(s) you want to delete in the <b>Remove</b> column and then click the <b>Remove</b> button.
Add	Click <b>Add</b> to create a new rule.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Remove	Click <b>Remove</b> to delete the selected rule(s).

### 9.3.1 Creating Incoming Filtering Rules

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

**Figure 59** Incoming IP Filtering: Add

The following table describes the labels in this screen.

**Table 34** Incoming IP Filtering: Add

LABEL	DESCRIPTION
Filter Name	Enter a descriptive name of up to 16 printable English keyboard characters, including spaces.
WAN Interfaces	Select the WAN interface to which this rule applies.
Protocol	Select the IP protocol ( <b>TCP/UDP</b> , <b>TCP</b> , <b>UDP</b> or <b>ICMP</b> ) and enter the protocol (service type) number in the port field.
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 34** Incoming IP Filtering: Add (continued)

LABEL	DESCRIPTION
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.



---

# PART IV

## Advanced

---

[Static Route \(125\)](#)

[Quality of Service \(QoS\) \(129\)](#)

[Dynamic DNS Setup \(141\)](#)

[Remote Management \(143\)](#)

[Universal Plug-and-Play \(UPnP\) \(149\)](#)



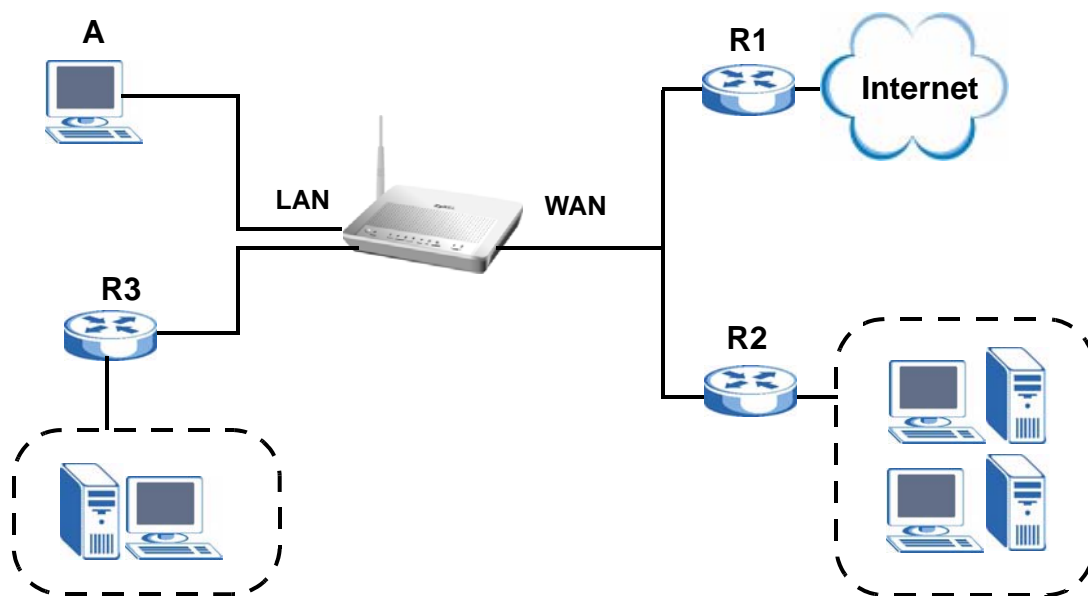
# Static Route

## 10.1 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 60** Example of Static Routing Topology



### 10.1.1 What You Can Do in this Chapter

The **Static Route** screens let you view and configure IP static routes on the ZyXEL Device ([Section 10.2 on page 126](#)).

## 10.2 The Static Route Screen

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

**Figure 61** Advanced > Static Route

The screenshot shows the 'IP Static Route' configuration window. At the top is a tab labeled 'IP Static Route'. Below it is a section titled 'Static Route Rules'. Inside this section is a table with the following data:

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

Below the table, there are two buttons: 'Add' and 'Apply'.

The following table describes the labels in this screen.

**Table 35** 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.

## 10.2.1 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 62** Static Route: Add

The following table describes the labels in this screen.

**Table 36** 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 <b>WAN</b> screens. If you select a WAN interface using <b>ENET ENCAP</b> you must specify the gateway IP address.
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 <b>Back</b> to return to the previous screen without saving.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.





# Quality of Service (QoS)

## 11.1 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.

### 11.1.1 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 11.3 on page 130](#)).
- The **Queue Setup** screen lets you configure QoS queue assignment ([Section 11.4 on page 131](#)).
- The **Class Setup** screen lets you add, edit or delete QoS classifiers ([Section 11.5 on page 133](#)).

## 11.2 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.

## 11.3 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 11.1 on page 129](#) for more information.

**Figure 63** QoS General

The screenshot shows a web-based configuration interface for Quality of Service (QoS). The interface has a top navigation bar with three tabs: 'General' (selected), 'Queue Setup', and 'Class Setup'. Below the tabs is a section titled 'General'. Inside this section, there is a checkbox labeled 'Active QoS' which is checked. Below the checkbox is a label 'Select Default DSCP Mark' followed by a dropdown menu that currently displays 'No Change(-1)'. At the bottom of the 'General' section, there are two buttons: 'Apply' and 'Cancel'.

The following table describes the labels in this screen.

**Table 37** QoS General

LABEL	DESCRIPTION
Active QoS	Select the check box to turn on QoS to improve your network performance.
Select Default DSCP Mark	This field is available only when you select <b>Enable QoS</b> .  If you enable QoS and incoming traffic does not match a class configured in the <b>Class Setup</b> screen, the ZyXEL Device sets the DSCP field in the packets with the value you select here. If you select <b>No Change</b> , the ZyXEL Device keeps the DSCP fields in the packets.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 11.4 The Queue Setup Screen

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

Use this screen to configure QoS queue assignment.

**Figure 64** QoS Queue Setup

Queue Key	Active	Name	Interface	Precedence	Modify
3	<input checked="" type="checkbox"/>	test	ptm0_1	1	

The following table describes the labels in this screen.

**Table 38** QoS Queue Setup

LABEL	DESCRIPTION
Add	Click this button to create a new entry.
Queue Key	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 entry.
Interface	This shows the name of the ZyXEL Device's interface through which traffic in this queue passes.
Precedence	This shows the priority queue of this entry.

**Table 38** QoS Queue Setup

LABEL	DESCRIPTION
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 <b>Apply</b> to save your changes back to the ZyXEL Device.

## 11.4.1 Adding a QoS Queue

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

**Figure 65** QoS Queue Setup: Add

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

- Active:** A checkbox that is currently unchecked.
- Queue Name:** A text input field.
- Queue Interface:** A dropdown menu.
- Queue Precedence:** A dropdown menu with the value "1" selected.
- Buttons:** Three buttons at the bottom: "Back", "Apply", and "Cancel".

The following table describes the labels in this screen.

**Table 39** QoS Queue Setup: Add

LABEL	DESCRIPTION
Active	Select to enable or disable this rule.
Queue Name	Enter the descriptive name of this rule.
Queue Interface	Select the interface to which this rule is applied.
Queue Precedence	Select the priority queue of this rule.  The smaller the number, the higher the priority level.
Back	Click <b>Back</b> to return to the previous screen without saving.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 11.5 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 66** QoS Class Setup

		CLASSIFICATION CRITERIA										CLASSIFICATION RESULTS							
Class Name	Order	Class Intf	Ether Type	SrcMAC/Mask	DstMAC/Mask	SrcIP/Mask	DstIP/Mask	Proto	Src Port	Dst Port	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	VlanID Tag	Rate Control (kbps)	Active	Modify
test	1	eth0	IP										3	default	3	123		<input checked="" type="checkbox"/>	

Apply

The following table describes the labels in this screen.

**Table 40** QoS Class Setup

LABEL	DESCRIPTION
Add	Click this button to create a new classifier.
Class Name	This is the name of the classifier.
Order	This field displays the index number of the classifier.
CLASSIFICATION CRITERIA	
This section shows criteria specified in this classifier.	
Class Intf	This shows the interface through which traffic that matches this classifier is forwarded out.
Ether Type	This is the service type.
SrcMAC /Mask	This shows the source MAC address and the mask of traffic of this class.

**Table 40** QoS Class Setup (continued)

LABEL	DESCRIPTION
DstMAC /Mask	This shows the destination MAC address and the mask of traffic of this class.
SrcIP/Mask	This shows the source IP address, the source subnet mask and DHCP option 60 or DHCP option 77.
DstIP/Mask	This shows the destination IP address and the destination subnet mask.
Proto	This shows the protocol type.
Src Port	This shows the source port number.
Dst Port	This shows the destination port number.
DSCP Check	This is the DSCP value of traffic of this class.
802.1P Check	This shows the 802.1P priority level.
CLASSIFICATION RESULTS	
Queue Key	This is the index number of a queue you configured in the <b>Queue Setup</b> screen.
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.
VlanID Tag	This is the VLAN ID number assigned to traffic of this classifier.
Rate Control	
Active	Select the check box to enable this classifier.
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 <b>Apply</b> to save your changes back to the ZyXEL Device.

## 11.5.1 QoS Class Edit

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

**Figure 67** QoS Class Setup: Add

**Class Configuration**

☐ Active

Name

Interface

Order

Ether Type

**Tag Configuration**

Assign Classification Queue

Mark Differentiated Service Code Point (DSCP)

Mark 802.1p priority

Tag VLAN ID

Set Rate Control(kbps):

**Filter Configuration**

**Source**

Address  Subnet Netmask

Port

MAC Address  MAC Mask

**Destination**

Address  Subnet Netmask

Port

MAC Address  MAC Mask

**Others**

Protocol

Differentiated Service Code Point (DSCP)

802.1p Priority

The following table describes the labels in this screen.

**Table 41** QoS Class Configuration

LABEL	DESCRIPTION
Active	Select to enable or disable this classifier.
Name	Enter a descriptive name of up to 20 printable English keyboard characters, including spaces.

**Table 41** QoS Class Configuration (continued)

LABEL	DESCRIPTION
Interface	Select from which Ethernet port traffic of this class should come. Select <b>Local</b> for any traffic from the LAN.
Order	Select an existing number for where you want to put this classifier to move the classifier to the number you selected after clicking <b>Apply</b> . Select <b>Last</b> to put this rule in the back of the classifier list.
Ether Type	Select a predefined application to configure a class for the matched traffic.  If you select <b>IP</b> , you also need to configure source or destination MAC address, IP address, DHCP options, DSCP value or the protocol type.  If you select <b>8021Q</b> , you can only configure a 802.1p priority level.
Tag Configuration	
Assign Classification Queue	Select a queue that applies to this class.  You should have configured a queue in the <b>Queue Setup</b> screen already.
Mark Differentiated Services Code Point (DSCP)	Select a DSCP value with which the ZyXEL Device replaces the DSCP field in the packets.  If you select <b>Auto Marking</b> 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.  Select <b>default</b> to set the DSCP value in the matched packets to 0.
Mark 802.1p priority	Select a priority level with which the ZyXEL Device replaces the IEEE 802.1 priority field in the packets.
Tag VLAN ID	Select a VLAN ID number (between 0 and 4095) with which the ZyXEL Device replaces the VLAN ID of the frames.
Set Rate Control(kbps)	Enter the transmission rate (in Kbps) for traffic that matches this QoS class
Filter Configuration	
Use the following fields to configure the criteria for traffic classification.	
Source	
Address	Enter the source IP address in dotted decimal notation.
Subnet Mask	Enter the source subnet mask.
Port	If you select a protocol type, enter the port number(s) of the source. 0 means any source port number.
MAC Address	Enter the source MAC address of the packet.



**Table 41** QoS Class Configuration (continued)

LABEL	DESCRIPTION
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> <p>You cannot put a "0" pair before an "f" pair. For example, ff:ff:00:ff:00:00 is invalid.</p>
Destination	
Address	Enter the destination IP address in dotted decimal notation.
Subnet Mask	Enter the destination subnet mask.
Port	If you select a protocol type, enter the port number(s) of the destination. 0 means any destination port number.
MAC Address	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 destination 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> <p>You cannot put a "0" pair before an "f" pair. For example, ff:ff:00:ff:00:00 is invalid.</p>
Others	
Protocol	Select the protocol (service type) from <b>TCP</b> , <b>UDP</b> , <b>ICMP</b> or <b>IGMP</b> .
Differentiated Services Code Point (DSCP)	<p>Select a DSCP value from the drop-down list box.</p> <p><b>default</b> represents the default DSCP value 000000 or 0x00.</p>
802.1p Priority	<p>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>
Back	Click <b>Back</b> to return to the previous screen without saving.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 11.6 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 42** 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.

DSCP (6 bits)	Unused (2 bits)
---------------	-----------------

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

## 12.1 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](http://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.

### 12.1.1 What You Can Do in this Chapter

Use the **Dynamic DNS** screen ([Section 12.3 on page 142](#)) to enable DDNS and configure the DDNS settings on the ZyXEL Device.

## 12.2 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.

## 12.3 The Dynamic DNS Screen

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

**Figure 68** Advanced > Dynamic DNS

The following table describes the fields in this screen.

**Table 43** 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 <b>TZO</b> in the <b>Service Provider</b> field, enter the user name you used to register for this service.
Key	If you select <b>TZO</b> in the <b>Service Provider</b> field, enter the password you used to register for this service.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

# Remote Management

## 13.1 Overview

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

### 13.1.1 What You Can Do in this Chapter

- The **TR-069 Client** screen lets you configure the ZyXEL Device's TR-069 auto-configuration settings ([Section 13.2 on page 143](#)).
- The **Service Control** screens let you configure through which interface(s) users can use which service(s) to manage the ZyXEL Device ([Section 13.3 on page 145](#)).
- The **IP Address** screens let you configure from which IP address(es) users can use a service to manage the ZyXEL Device ([Section 13.4 on page 146](#)).

## 13.2 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 69** TR-069

The following table describes the fields in this screen.

**Table 44** TR-069

LABEL	DESCRIPTION
Inform	Select <b>Enable</b> to activate remote management via TR-069 on the WAN. Otherwise, select <b>Disable</b> .
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.
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 44** 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 <b>Cancel</b> to begin configuring this screen afresh.

## 13.3 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 70** Service Control

TR069 **ServiceControl** IPAddress

Access Control -- Services

Service Control Mode: ☐ Disable ☒ Enable

Services	LAN	WAN
FTP	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
HTTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
SNMP	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable
SSH	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
TELNET	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
TFTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable

**Note :**  
Active IP Filter on WAN before enable Access Control.

Save/Apply

The following table describes the fields in this screen.

**Table 45** Access Control: Services

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

## 13.4 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 71** IP Address

TR069 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 46** IP Address

LABEL	DESCRIPTION
Access Control Mode	Select <b>Enable</b> to activate the secured client list. Select <b>Disable</b> 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.

**Table 46** IP Address (continued)

LABEL	DESCRIPTION
Remove	Select this check box and click the <b>Remove</b> 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.

### 13.4.1 Adding an IP Address

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

**Figure 72** IP Address: Add

The following table describes the fields in this screen.

**Table 47** 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)

## 14.1 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.

### 14.1.1 What You Can Do in this Chapter

The **UPnP** screen lets you enable UPnP on the ZyXEL Device ([Section 14.3 on page 150](#)).

## 14.2 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.

## 14.3 The UPnP Screen

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

See [Section 14.1 on page 149](#) for more information.

**Figure 73** Advanced > UPnP



The following table describes the fields in this screen.

**Table 48** Advanced > UPnP

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

## 14.4 Installing UPnP in Windows Example

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

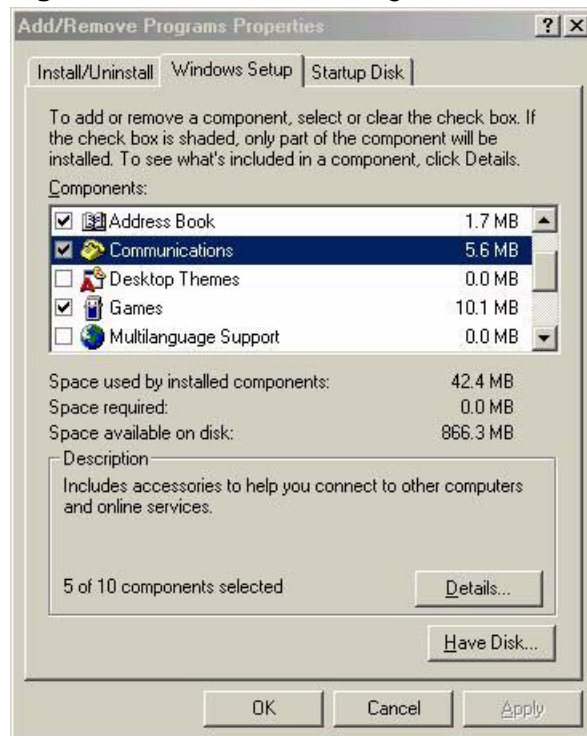
### Installing UPnP in Windows Me

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

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

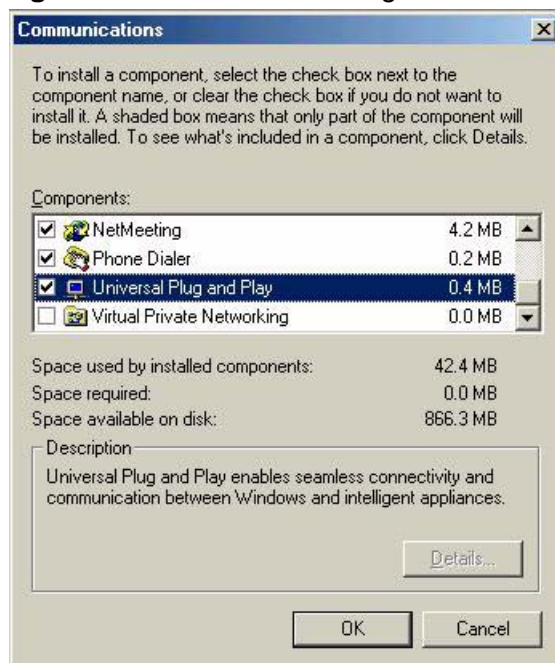
- 2 Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.

**Figure 74** 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 75** 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.

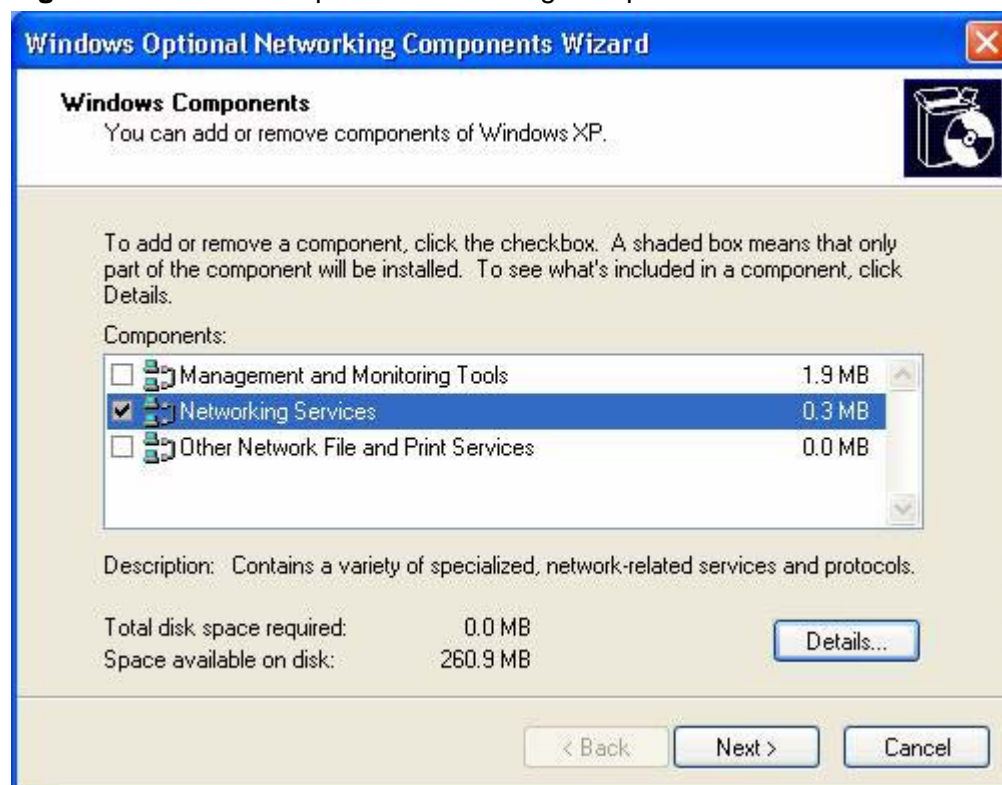
- 1 Click **Start** and **Control Panel**.
- 2 Double-click **Network Connections**.
- 3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ....**

**Figure 76** Network Connections



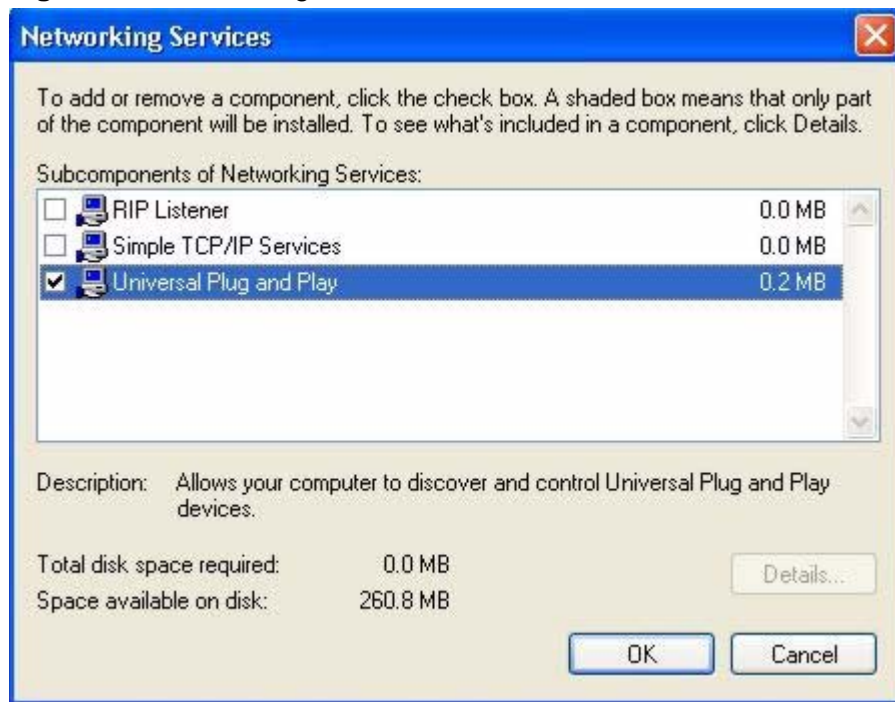
- 4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

**Figure 77** Windows Optional Networking Components Wizard



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

**Figure 78** Networking Services



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

## 14.5 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 79** Network Connections



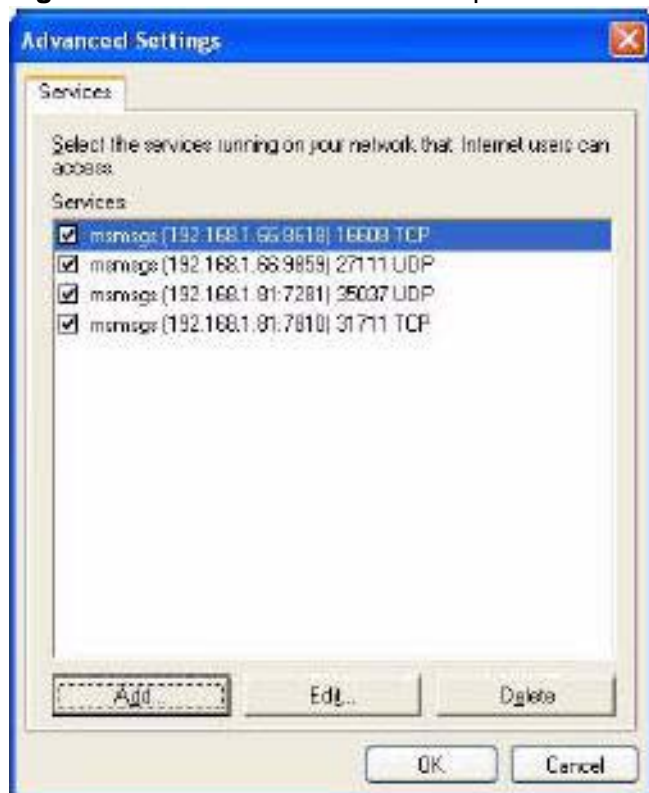
- 3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

**Figure 80** Internet Connection Properties

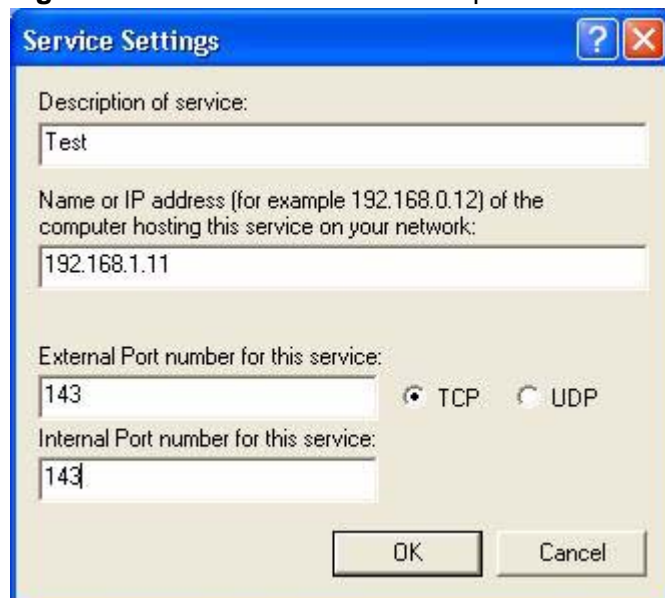


- 4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

**Figure 81** Internet Connection Properties: Advanced Settings



**Figure 82** 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 83** System Tray Icon



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

**Figure 84** 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.

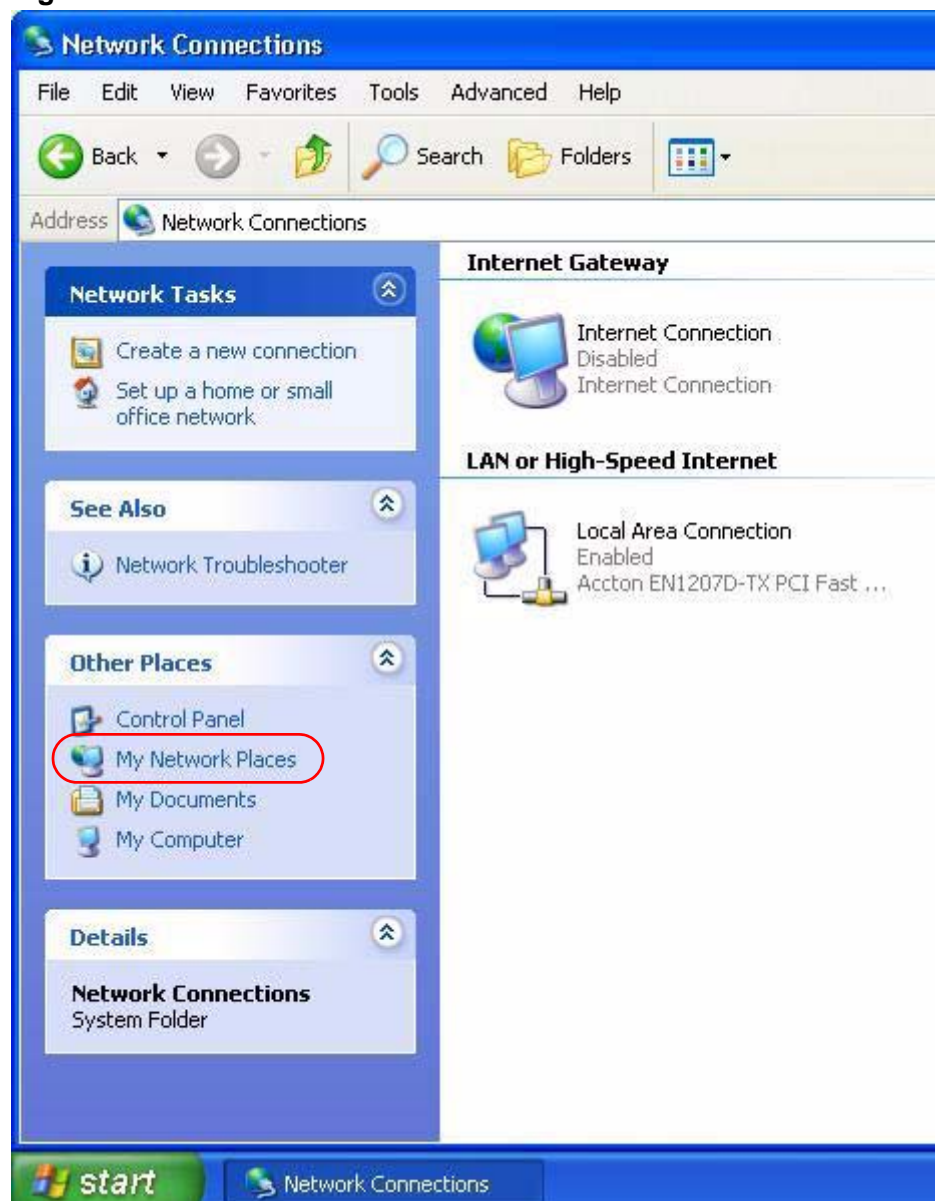
Follow the steps below to access the web configurator.

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



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

**Figure 85** Network Connections



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



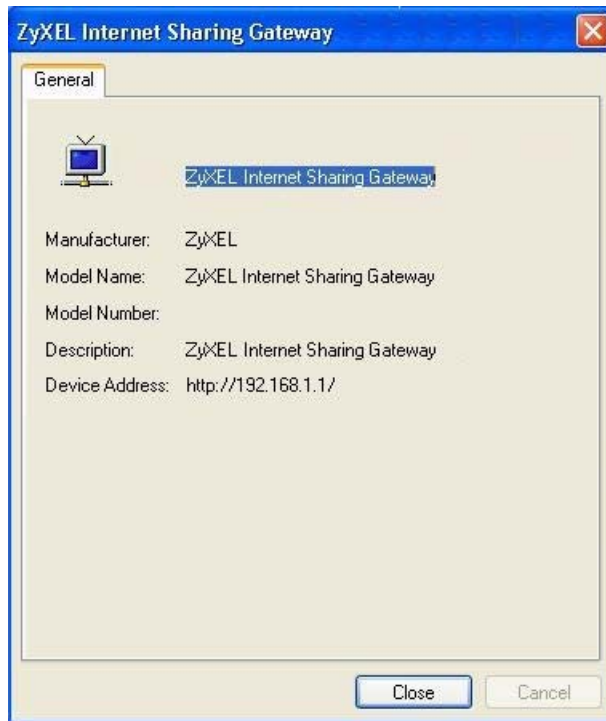
- 5 Right-click on the icon for your ZyXEL Device and select **Invoke**. The web configurator login screen displays.

**Figure 86** 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 87** Network Connections: My Network Places: Properties: Example





---

# PART V

## Maintenance, Troubleshooting and Specifications

---

System Settings (165)

Logs (169)

Tools (173)

Troubleshooting (181)

Product Specifications (187)



# System Settings

## 15.1 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.

### 15.1.1 What You Can Do in this Chapter

- The **General** screen lets you configure system settings ([Section 15.2 on page 166](#)).
- The **Time Setting** screen lets you set the system time ([Section 15.3 on page 167](#)).

### 15.1.2 What You Need to Know

#### Domain Name

This is a network address that identifies the owner of a network connection. For example, in the network address “www.zyxel.com/support/files”, the domain name is “www.zyxel.com”.

#### DHCP

DHCP (Dynamic Host Configuration Protocol) is a method of allocating IP addresses to devices on a network from a DHCP Server. Often your ISP or a router on your network performs this function.

#### LAN

A LAN (local area network) is typically a network which covers a small area, made up of computers and other devices which share resources such as Internet access, printers etc.

## 15.2 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 88** Maintenance > System > General

The following table describes the labels in this screen.

**Table 49** Maintenance > System > General

LABEL	DESCRIPTION
UserName	This shows 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 <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 15.3 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 89** Maintenance > System > Time Setting

The following table describes the fields in this screen.

**Table 50** 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 Zone Setup	
Automatically synchronize with Internet time servers	Select this radio button to have the ZyXEL Device get the time and date from the time server you specified below.

**Table 50** Maintenance > System > Time Setting (continued)

LABEL	DESCRIPTION
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 <b>Other</b> and enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server.  Select <b>None</b> 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 <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.



## 16.1 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.

### 16.1.1 What You Can Do in this Chapter

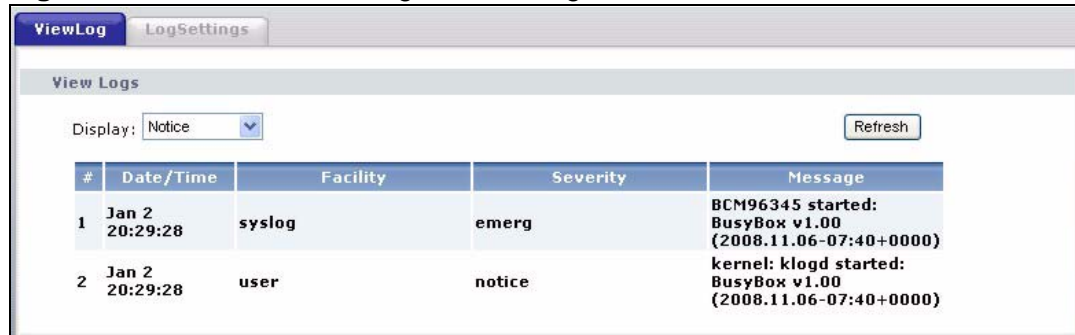
- The **View Log** screen lets you see the logs for the categories that you selected in the **Log Settings** screen ([Section 16.2 on page 169](#)).
- The **Log Settings** screen lets you configure to where the ZyXEL Device is to send logs and which logs and/or immediate alerts the ZyXEL Device is to record ([Section 16.3 on page 170](#)).

## 16.2 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 16.3 on page 170](#)).

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

**Figure 90** Maintenance > Logs > View Log



The following table describes the fields in this screen.

**Table 51** Maintenance > Logs > View Log

LABEL	DESCRIPTION
Display	Select a category of logs to view. The ZyXEL Device displays the logs with the severity level equal to or higher than what you selected.  The order of the log severity (from the highest to the lowest) is Emergency > Alert > Critical > Error > Warning > Notice > Informational > Debugging.
Refresh	Click this button to renew the log screen.
#	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.
Facility	This field displays the system module from which the logs come.
Severity	This field displays the severity type of the log.
Message	This field states the reason for the log.

## 16.3 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 91** Maintenance > Logs > Log Settings

The following table describes the fields in this screen.

**Table 52** Maintenance > Logs > Log Settings

LABEL	DESCRIPTION
Active	Select to enable or disable system logging.
Syslog Server IP Address	Enter the server name or the IP address of the log server. The logs will be stored in both the ZyXEL Device and the log server.  Otherwise, enter <b>0.0.0.0</b> to store the logs in the local memory of the ZyXEL Device only.
Log Severity	Select the severity level of the logs that you want the ZyXEL Device to record and send to the log server.  The ZyXEL Device records the logs with the severity level equal to or higher than what you selected.  The order of the log severity (from the highest to the lowest) is Emergency > Alert > Critical > Error > Warning > Notice > Informational > Debugging.
Apply	Click <b>Apply</b> to save your customized settings.
Cancel	Click <b>Cancel</b> to return to the previously saved settings.



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

## 17.1 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](http://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.**

### 17.1.1 What You Can Do in this Chapter

- The **Firmware Upgrade** screen lets you upload firmware to your device ([Section 17.2 on page 174](#)).
- The **Configuration** screen lets you backup and restore device configurations ([Section 17.3 on page 176](#)). You can also reset your device settings back to the factory default.
- The **Restart** screen lets you restart your ZyXEL Device ([Section 17.4 on page 178](#)).

## 17.2 The Firmware Upgrade 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 92** Maintenance > Tools > Firmware

The following table describes the labels in this screen.

**Table 53** 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 <b>Browse ...</b> to find it.
Browse...	Click <b>Browse...</b> to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click <b>Upload</b> 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 93** 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 94** 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 95** Error Message



## 17.3 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 96** Maintenance > Tools > Configuration

The screenshot shows a web interface with three tabs: 'Firmware', 'Configuration' (selected), and 'Restart'. The 'Configuration' tab is active and contains three sections:

- Backup Configuration**: A section with the instruction 'Click **Backup** to save the current configuration of your system to your computer.' and a '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 54** Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse ...</b> to find it.
Browse...	Click <b>Browse...</b> to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click <b>Upload</b> 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 97** 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 98** 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 195](#) 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 99** 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 100** 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 22](#) for more information on the **RESET** button.

## 17.4 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 101** Maintenance > Tools > Restart





# 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](#)

## 18.1 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 21](#).

- 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.

## 18.2 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 22](#).

---

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 22](#).

---

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 76](#)), 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 JavaScripts and Java enabled. See [Appendix B on page 225](#).
  - 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 22](#).
  - 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 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 18.1 on page 181](#).

## **18.3 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 21](#).

- 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 21](#).
- 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 21](#). 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.

## 19.1 Hardware Specifications

**Table 55** Hardware Specifications

Dimensions	(220 W) x (150 D) x (40 H) mm
Weight	485 g
Power Specification	18VDC 1A
Built-in Switch	Four auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports
RESET Button	Restores factory defaults
Antenna	One attached external dipole antenna, 3dBi
WPS Button	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

## 19.2 Firmware Specifications

**Table 56** Firmware Specifications

Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234

**Table 56** Firmware Specifications (continued)

DHCP Server IP Pool	192.168.1.33 to 192.168.1.254
Static DHCP Addresses	10
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.  <b>Note: Only upload firmware for your specific model!</b>
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, <a href="http://www.zyxel.com">www.zyxel.com</a> 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 56** 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
Multiple PVC (Permanent Virtual Circuits) Support	Your device supports up to 8 Permanent Virtual Circuits (PVCs).
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.
ADSL Standards	Support ITU G.992.1 G.dmt (Annex B, U-R2) EOC specified in ITU-T G.992.1 ADSL2 G.dmt.bis (G.992.3) ADSL2 G.lite.bis (G.992.4) ADSL 2/2+ AnnexM ADSL2+ (G.992.5) Reach-Extended ADSL (RE ADSL) SRA (Seamless Rate Adaptation) Auto-negotiating rate adaptation ADSL physical connection ATM AAL5 (ATM Adaptation Layer type 5) Multi-protocol over AAL5 (RFC 2684/1483) PPP over ATM AAL5 (RFC 2364) PPP over Ethernet (RFC 2516) Multiple PPPoE VC-based and LLC-based multiplexing Up to 8 PVCs (Permanent Virtual Circuits) I.610 F4/F5 OAM Zero configuration

**Table 56** 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 ATM QoS SNMP v1 and v2c with MIB II support (RFC 1213) IP Multicasting IGMP v1 and v2 IGMP Proxy
Management	Embedded Web Configurator Remote Firmware Upgrade Syslog TR-069

## 19.3 Wireless Features

**Table 57** 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 57** 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 64/128/256 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 58** Standards Supported

STANDARD	DESCRIPTION
RFC 867	Daytime Protocol
RFC 868	Time Protocol.
RFC 1058	RIP-1 (Routing Information Protocol)
RFC 1112	IGMP v1
RFC 1157	SNMPv1: Simple Network Management Protocol version 1
RFC 1305	Network Time Protocol (NTP version 3)
RFC 1441	SNMPv2 Simple Network Management Protocol version 2
RFC 1483	Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 1631	IP Network Address Translator (NAT)
RFC 1661	The Point-to-Point Protocol (PPP)
RFC 1723	RIP-2 (Routing Information Protocol)
RFC 1901	SNMPv2c Simple Network Management Protocol version 2c
RFC 2236	Internet Group Management Protocol, Version 2.
RFC 2364	PPP over AAL5 (PPP over ATM over ADSL)

**Table 58** Standards Supported (continued)

STANDARD	DESCRIPTION
RFC 2408	Internet Security Association and Key Management Protocol (ISAKMP)
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2684	Multiprotocol Encapsulation over ATM Adaptation Layer 5.
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
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
ANSI T1.413, Issue 2	Asymmetric Digital Subscriber Line (ADSL) standard.
G dmt(G.992.1)	G.992.1 Asymmetrical Digital Subscriber Line (ADSL) Transceivers
ITU G.992.1 (G.DMT)	ITU standard for ADSL using discrete multitone modulation.
ITU G.992.2 (G. Lite)	ITU standard for ADSL using discrete multitone modulation.
ITU G.992.3 (G.dmt.bis)	ITU standard (also referred to as ADSL2) that extends the capability of basic ADSL in data rates.
ITU G.992.4 (G.lite.bis)	ITU standard (also referred to as ADSL2) that extends the capability of basic ADSL in data rates.
ITU G.992.5 (ADSL2+)	ITU standard (also referred to as ADSL2+) that extends the capability of basic ADSL by doubling the number of downstream bits.
Microsoft PPTP	MS PPTP (Microsoft's implementation of Point to Point Tunneling Protocol)
MBM v2	Media Bandwidth Management v2
RFC 2383	ST2+ over ATM Protocol Specification - UNI 3.1 Version
TR-069	TR-069 DSL Forum Standard for CPE Wan Management.
1.363.5	Compliant AAL5 SAR (Segmentation And Re-assembly)



---

# PART VI

# Appendices and Index

---

Note: The appendices provide general information. Some details may not apply to your ZyXEL Device.

[Setting Up Your Computer's IP Address \(195\)](#)

[Pop-up Windows, JavaScripts and Java Permissions \(225\)](#)

[IP Addresses and Subnetting \(235\)](#)

[Wireless LANs \(247\)](#)

[Common Services \(263\)](#)

[Legal Information \(267\)](#)

[Index \(271\)](#)



# 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:

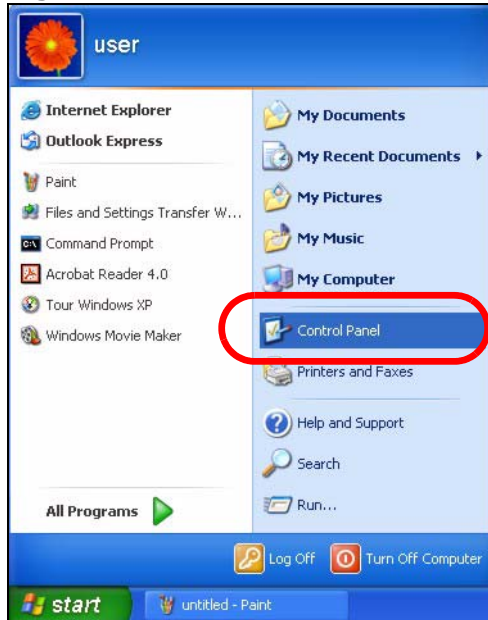
- [Windows XP/NT/2000](#) on [page 196](#)
- [Windows Vista](#) on [page 200](#)
- [Mac OS X: 10.3 and 10.4](#) on [page 205](#)
- [Mac OS X: 10.5](#) on [page 209](#)
- [Linux: Ubuntu 8 \(GNOME\)](#) on [page 212](#)
- [Linux: openSUSE 10.3 \(KDE\)](#) on [page 218](#)

## 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 102** Windows XP: Start Menu



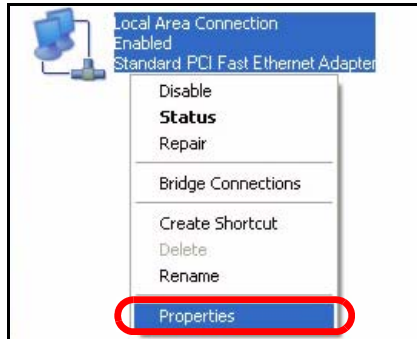
- 2 In the **Control Panel**, click the **Network Connections** icon.

**Figure 103** Windows XP: Control Panel



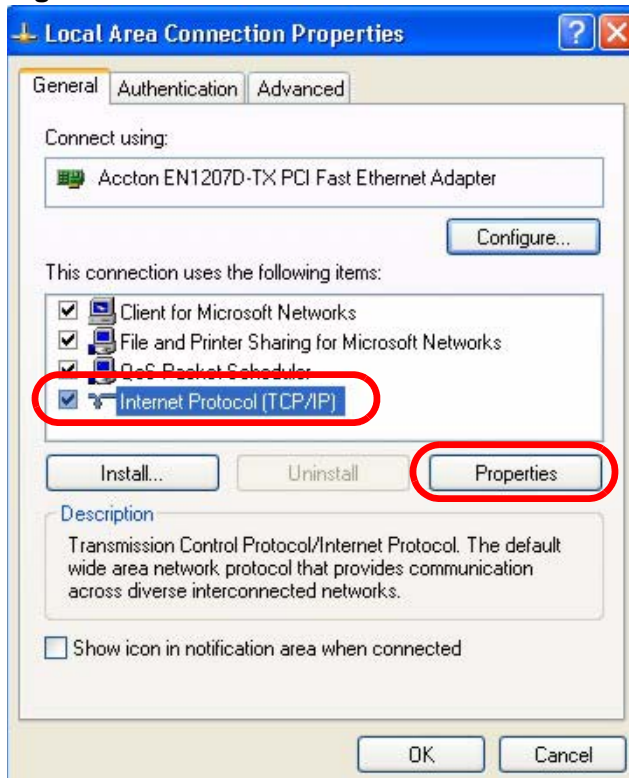
- 3 Right-click **Local Area Connection** and then select **Properties**.

**Figure 104** Windows XP: Control Panel > Network Connections > Properties



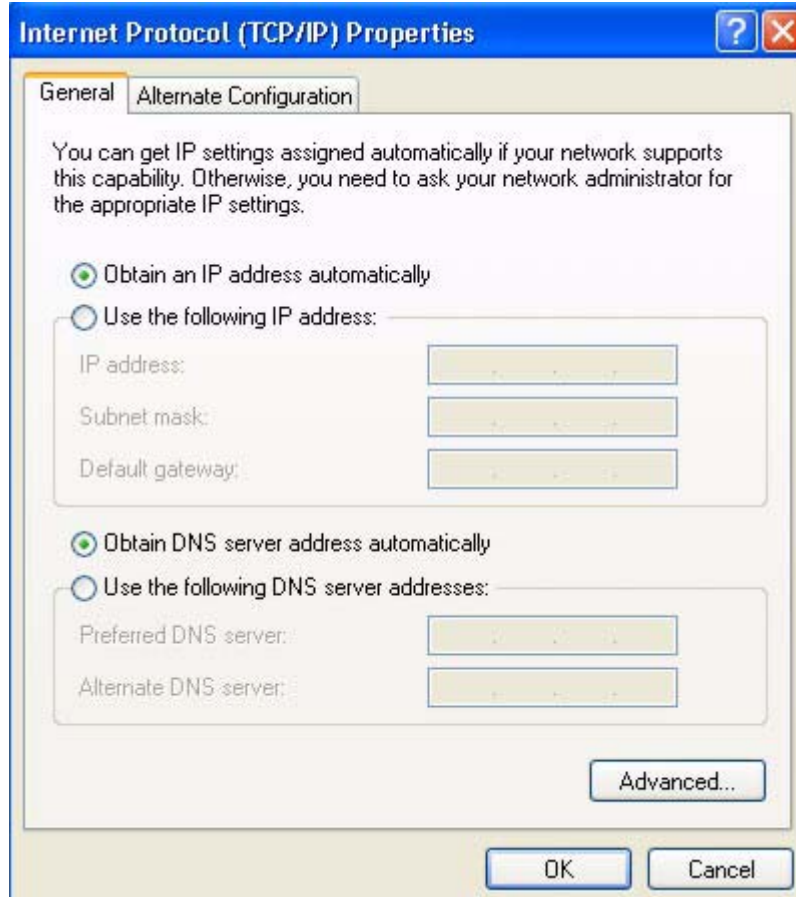
- 4 On the **General** tab, select **Internet Protocol (TCP/IP)** and then click **Properties**.

**Figure 105** Windows XP: Local Area Connection Properties



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

**Figure 106** 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].

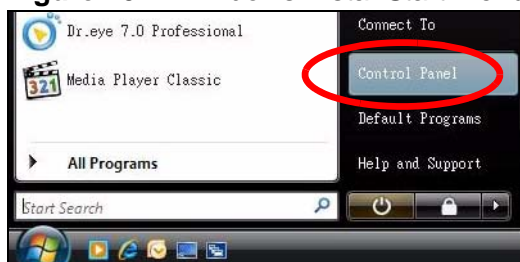
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

## Windows Vista

This section shows screens from Windows Vista Professional.

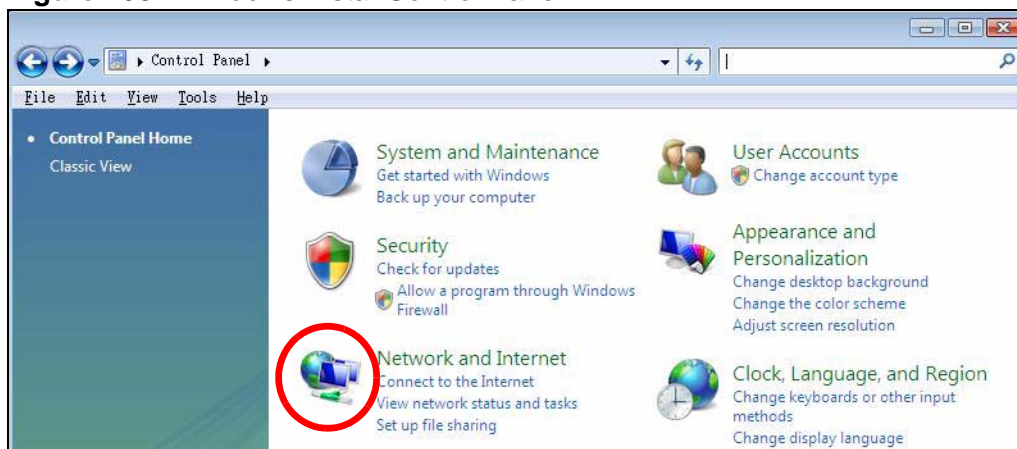
- 1 Click **Start > Control Panel**.

**Figure 107** Windows Vista: Start Menu



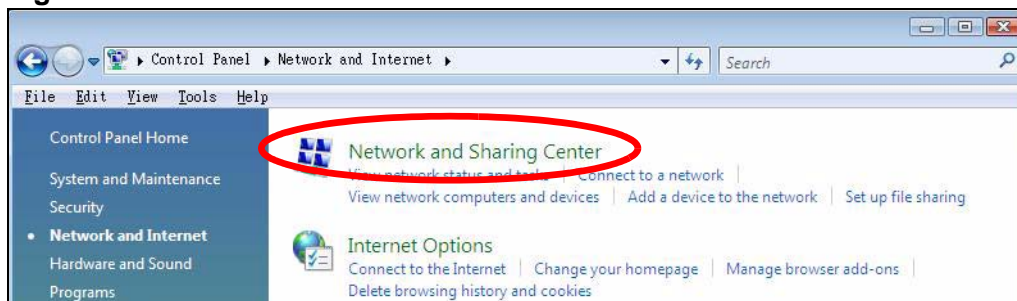
- 2 In the **Control Panel**, click the **Network and Internet** icon.

**Figure 108** Windows Vista: Control Panel



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

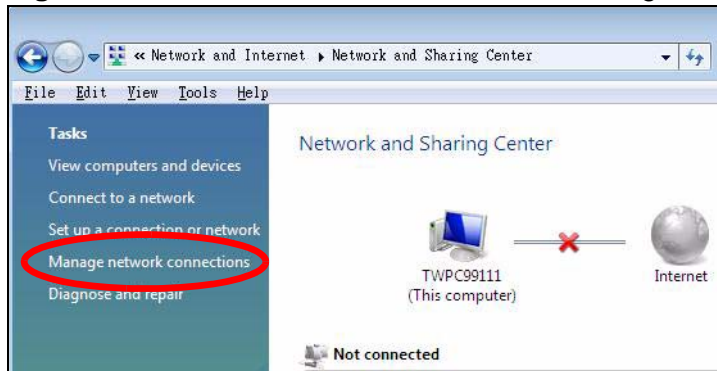
**Figure 109** Windows Vista: Network And Internet





- 4 Click **Manage network connections**.

**Figure 110** Windows Vista: Network and Sharing Center



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

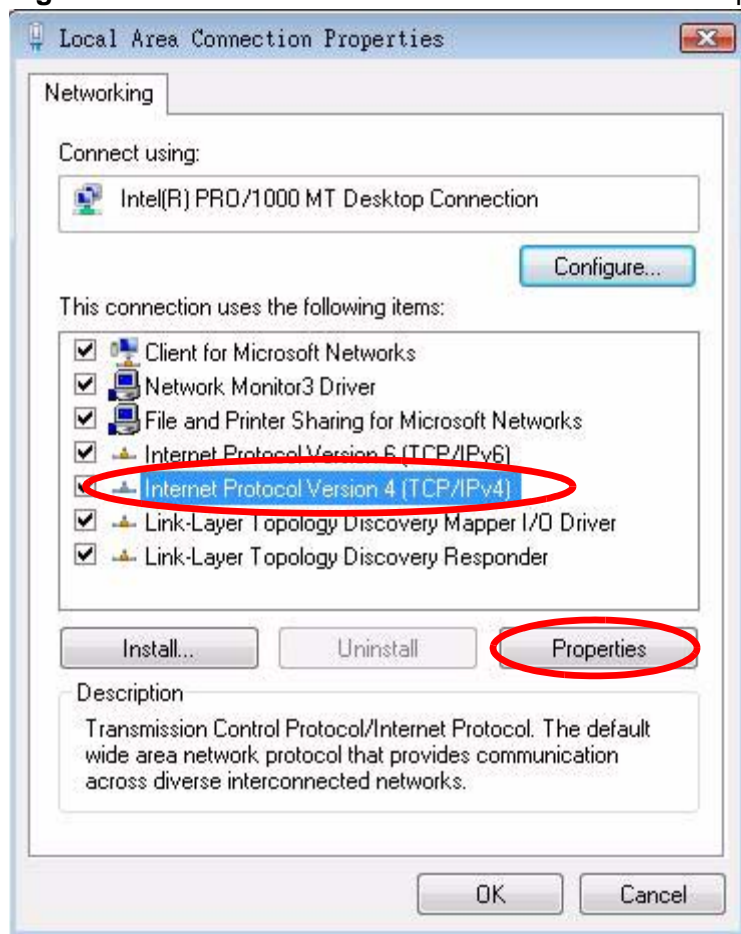
**Figure 111** Windows Vista: Network and Sharing Center



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

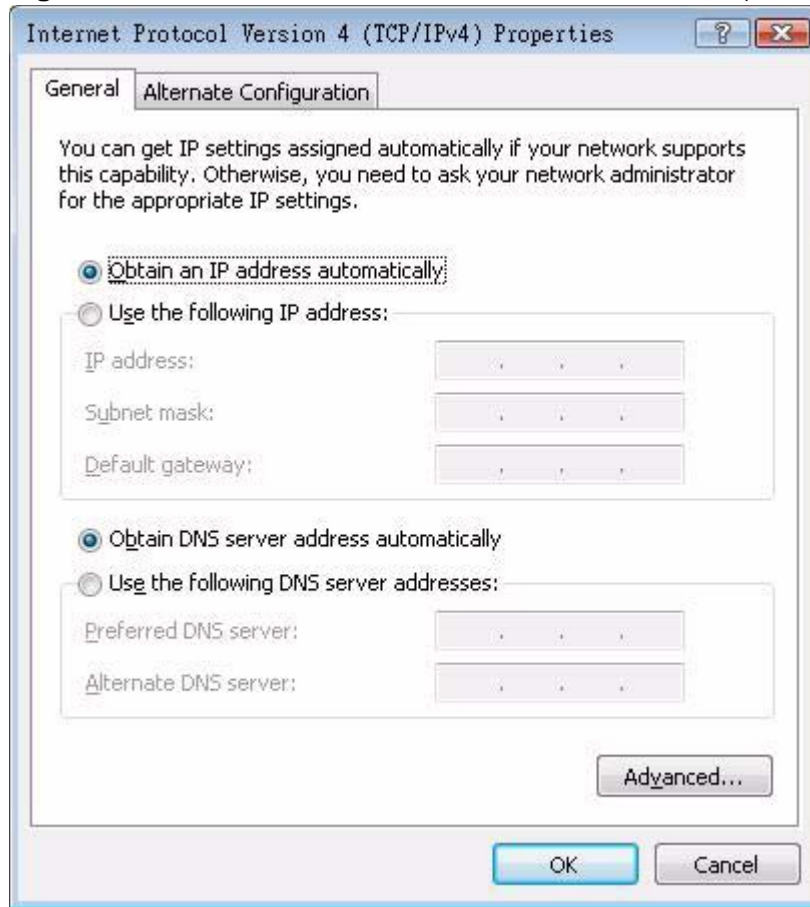
- 6 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

**Figure 112** Windows Vista: Local Area Connection Properties



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

**Figure 113** 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].

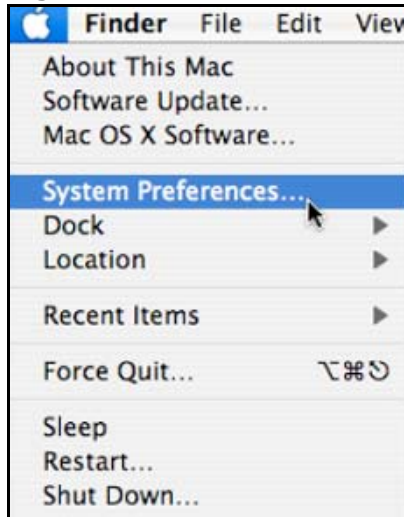
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

## 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 114** Mac OS X 10.4: Apple Menu



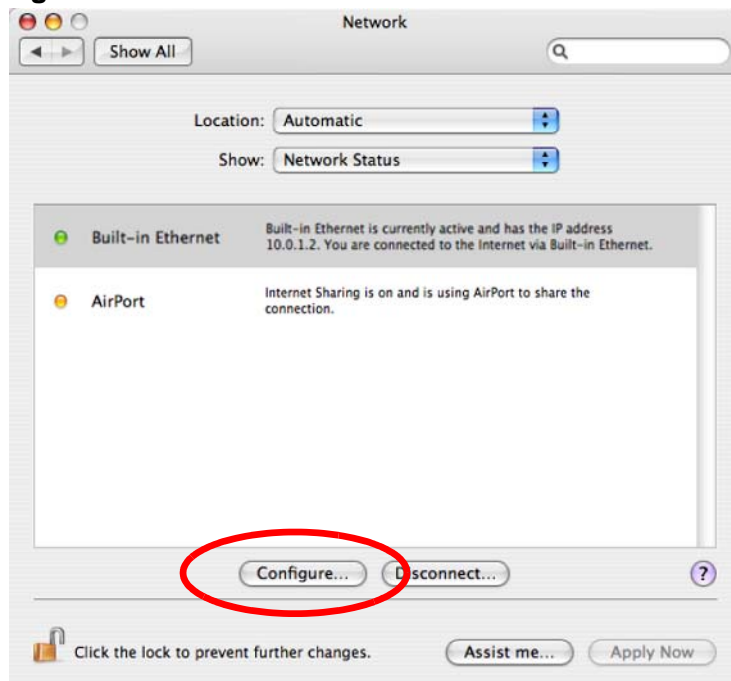
- 2 In the **System Preferences** window, click the **Network** icon.

**Figure 115** Mac OS X 10.4: System Preferences



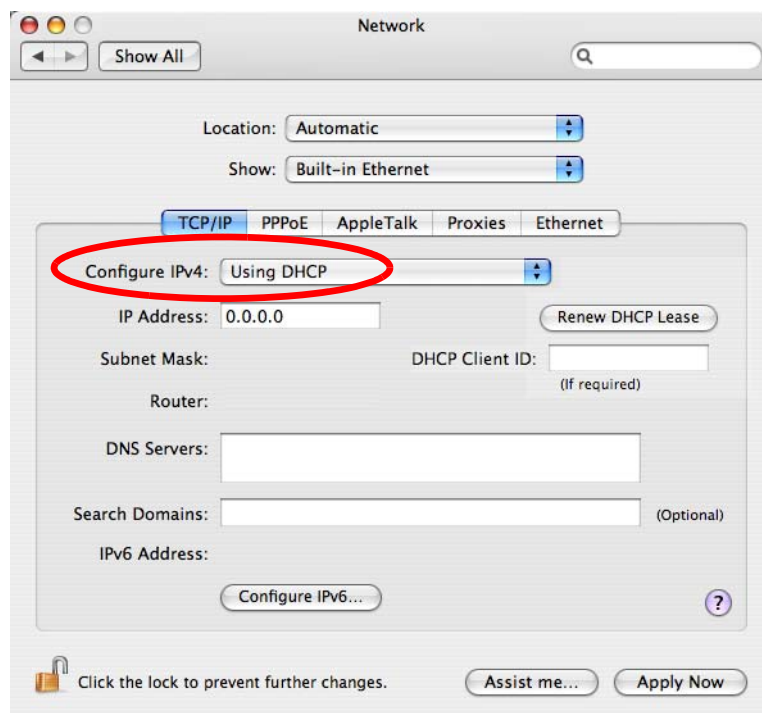
- 3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure**.

**Figure 116** Mac OS X 10.4: Network Preferences



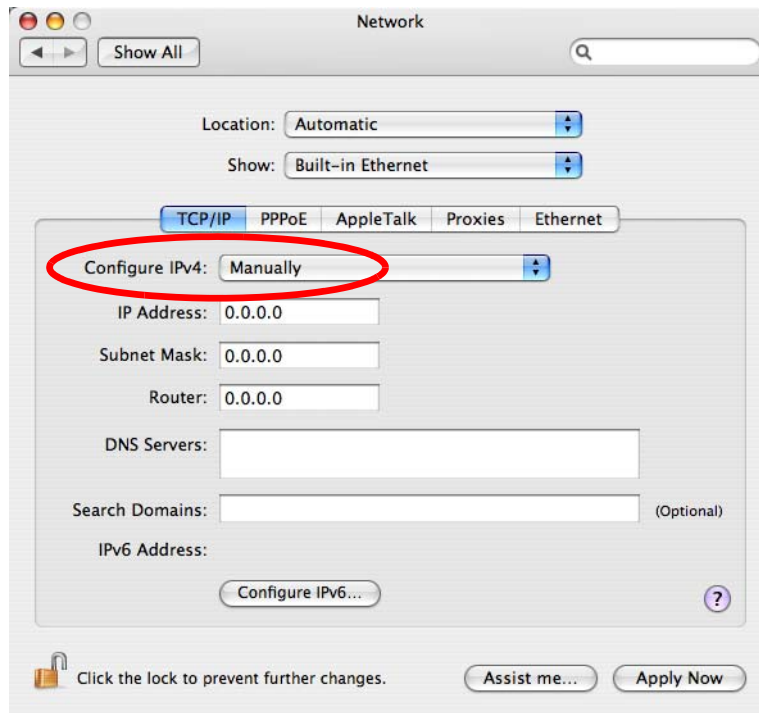
- 4 For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.

**Figure 117** 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 118** Mac OS X 10.4: Network Preferences > Ethernet

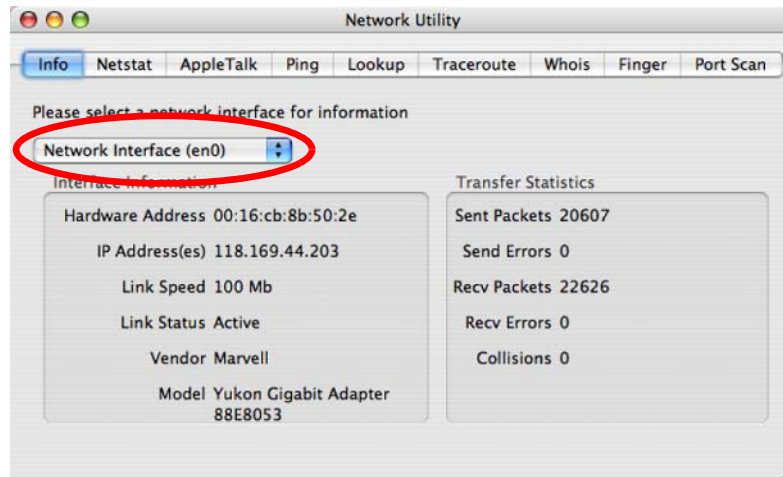


- 6 Click **Apply Now** and close the window.

## 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 119** Mac OS X 10.4: Network Utility



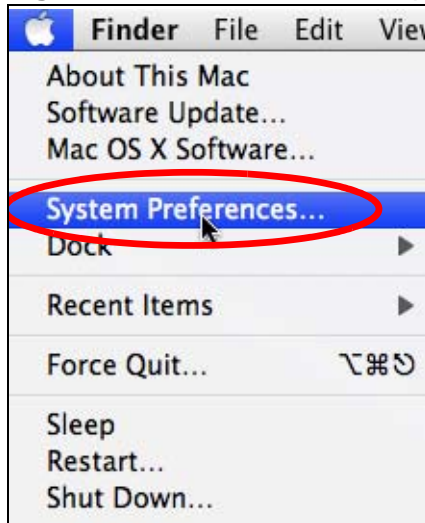


## Mac OS X: 10.5

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

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

**Figure 120** Mac OS X 10.5: Apple Menu



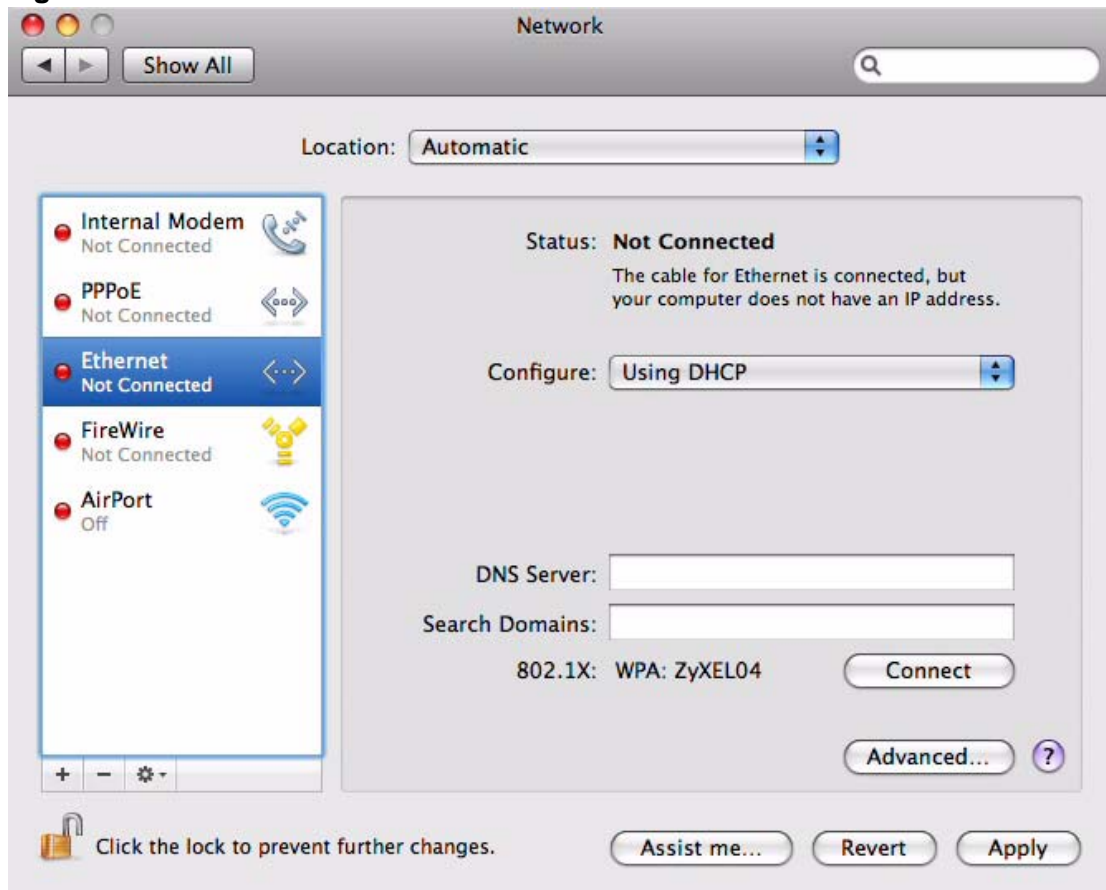
- 2 In **System Preferences**, click the **Network** icon.

**Figure 121** Mac OS X 10.5: Systems Preferences



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

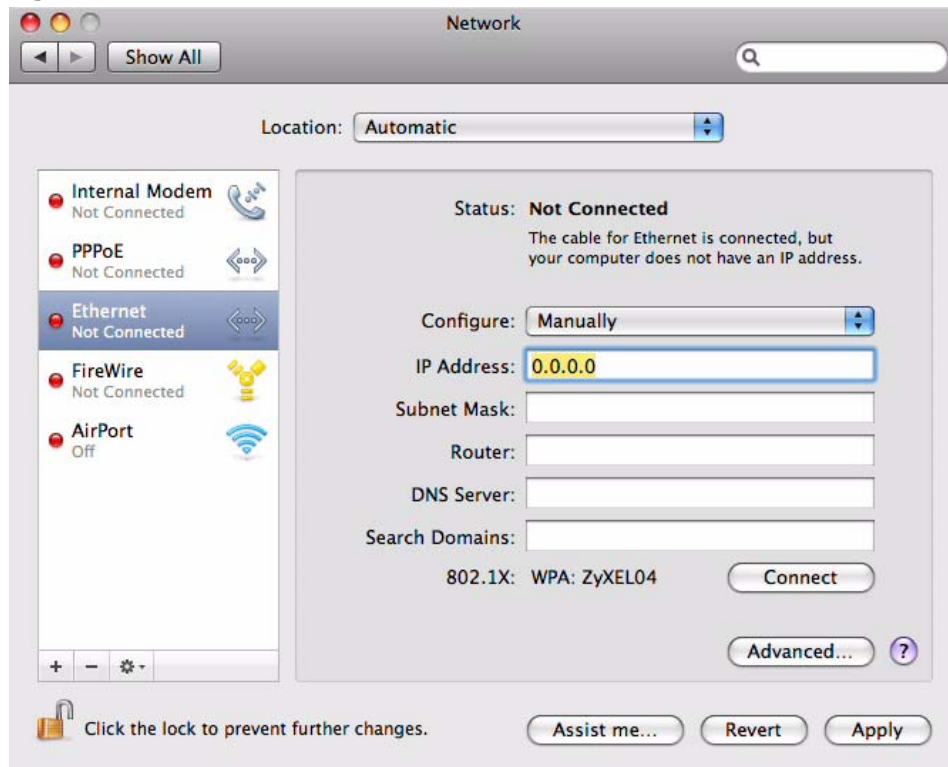
**Figure 122** Mac OS X 10.5: Network Preferences > Ethernet



- 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 123** Mac OS X 10.5: Network Preferences > Ethernet

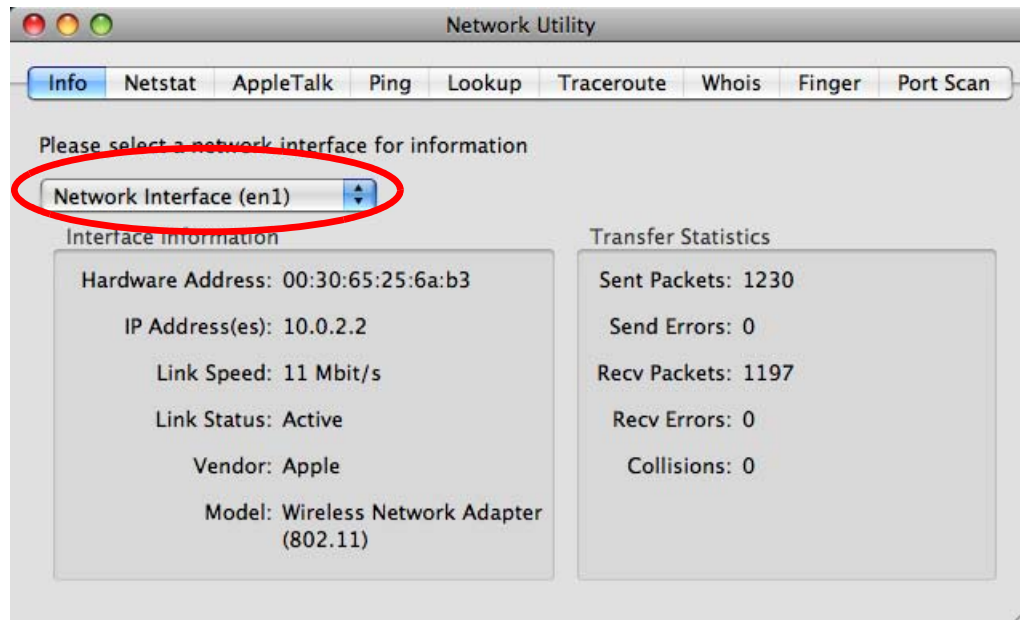


- 6 Click **Apply** and close the window.

## 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 124** Mac OS X 10.5: Network Utility



## Linux: Ubuntu 8 (GNOME)

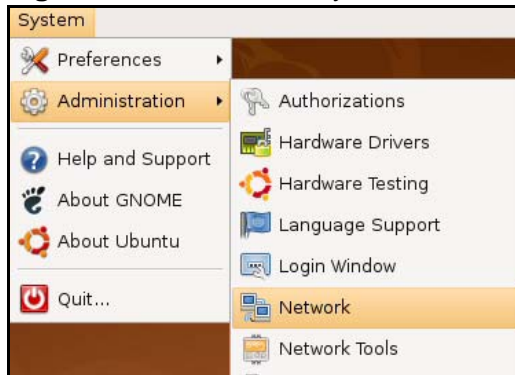
This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following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

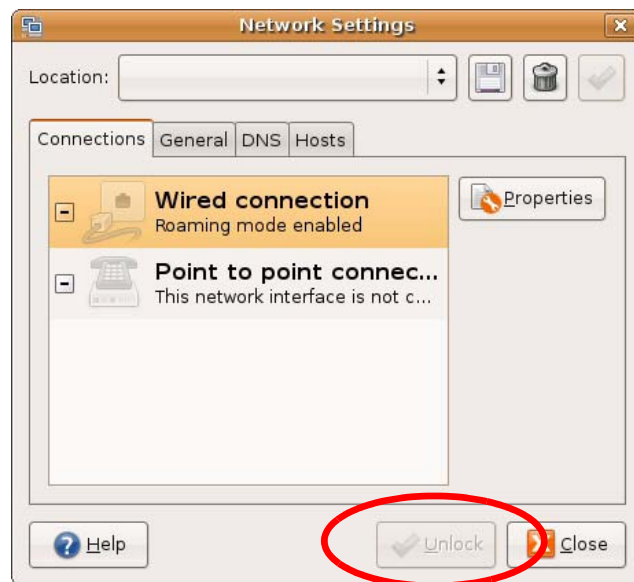
- 1 Click **System > Administration > Network**.

**Figure 125** 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 126** Ubuntu 8: Network Settings > Connections



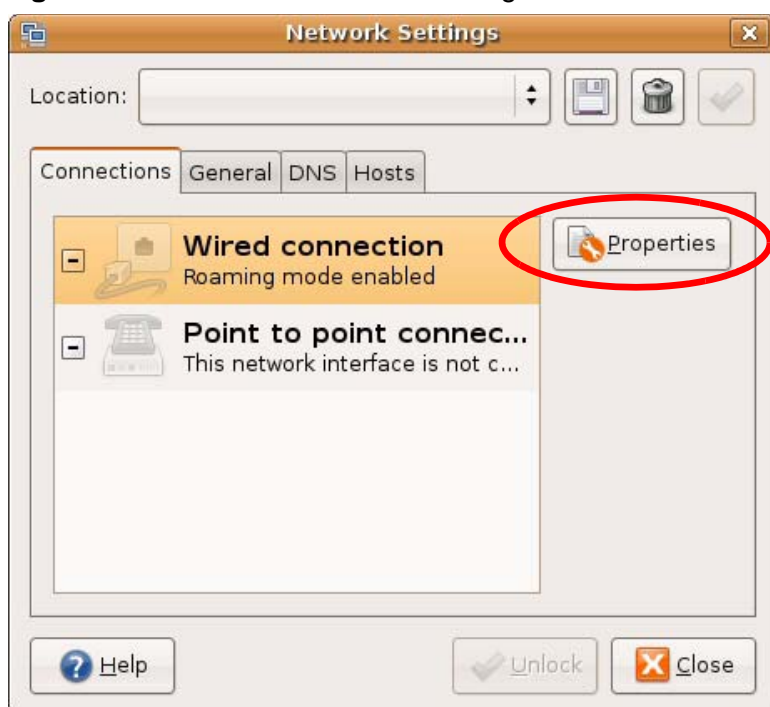
- 3 In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.

**Figure 127** Ubuntu 8: Administrator Account Authentication



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

**Figure 128** Ubuntu 8: Network Settings > Connections



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

**Figure 129** 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 130** Ubuntu 8: Network Settings > DNS



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

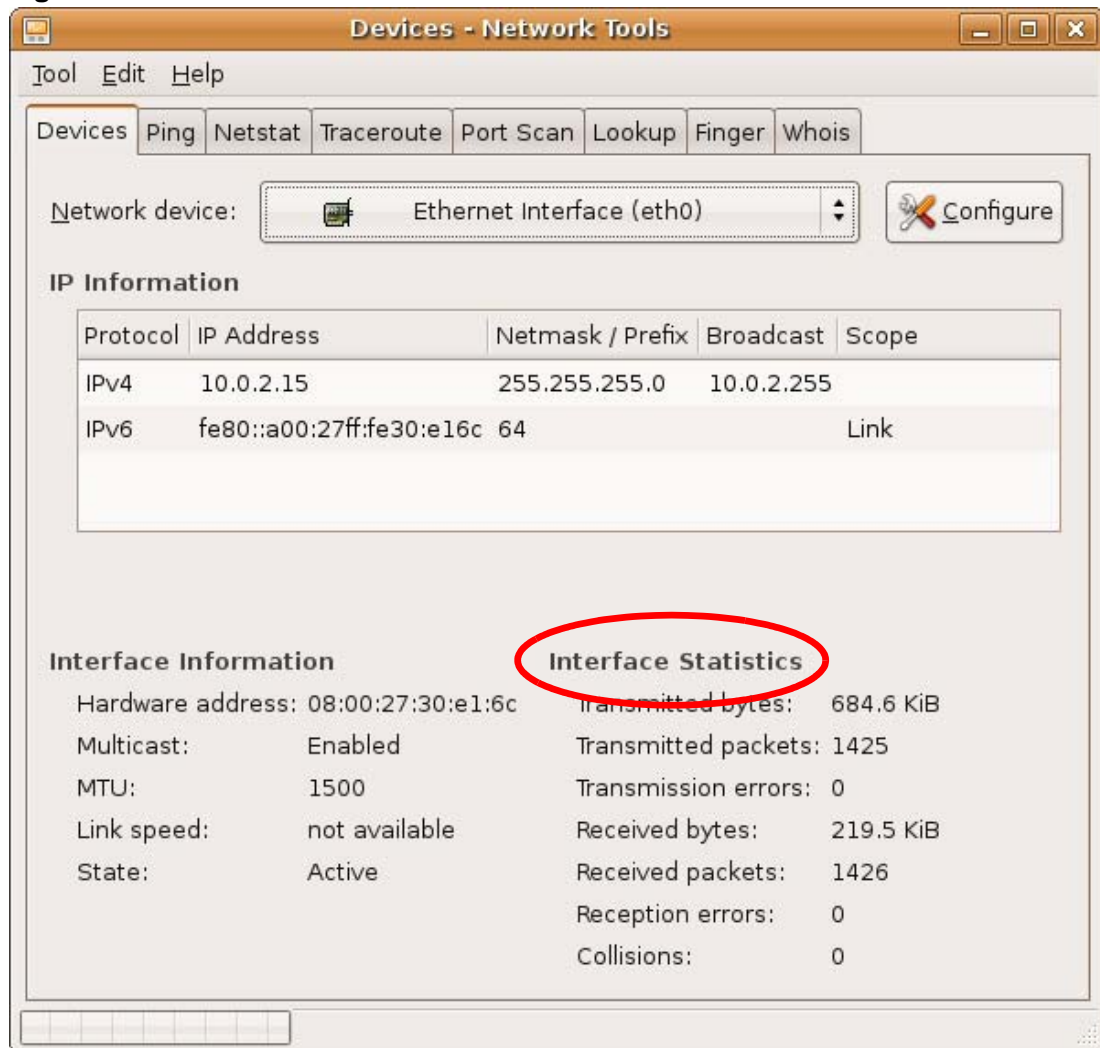
## Verifying Settings

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 131** Ubuntu 8: Network Tools



## Linux: openSUSE 10.3 (KDE)

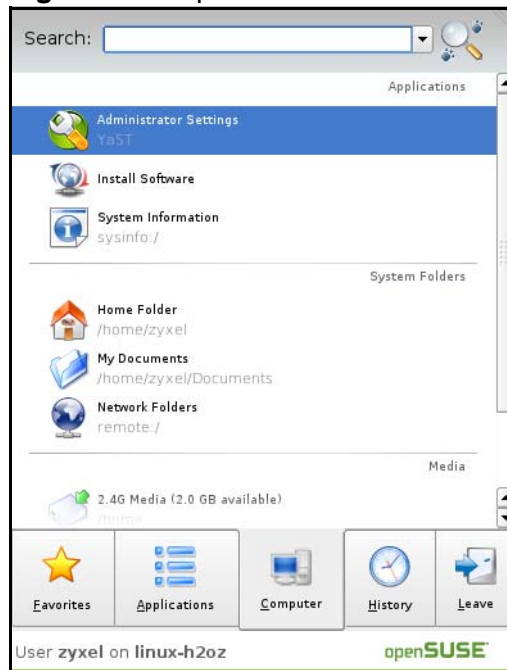
This section shows you how to configure your computer's TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following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

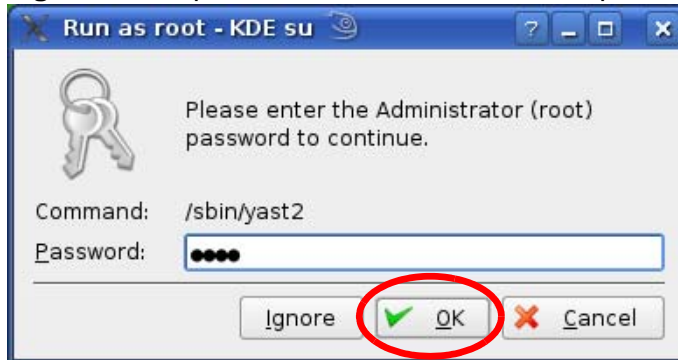
- 1 Click **K Menu > Computer > Administrator Settings (YaST)**.

**Figure 132** openSUSE 10.3: K Menu > Computer Menu



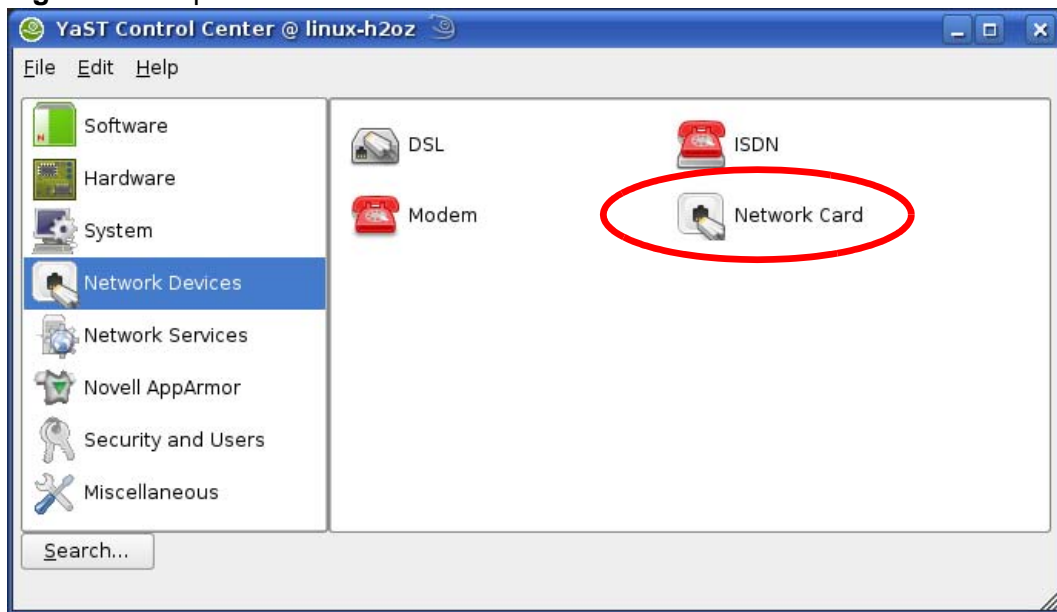
- 2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.

**Figure 133** openSUSE 10.3: K Menu > Computer Menu



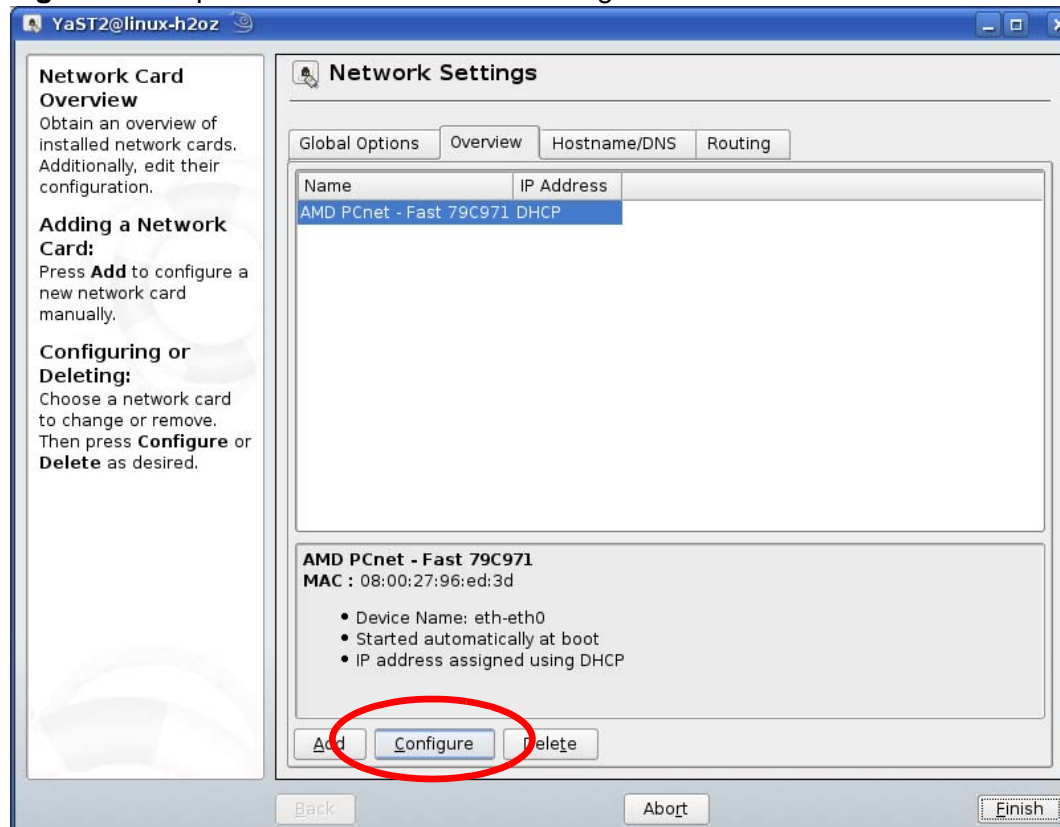
- 3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.

**Figure 134** openSUSE 10.3: YaST Control Center



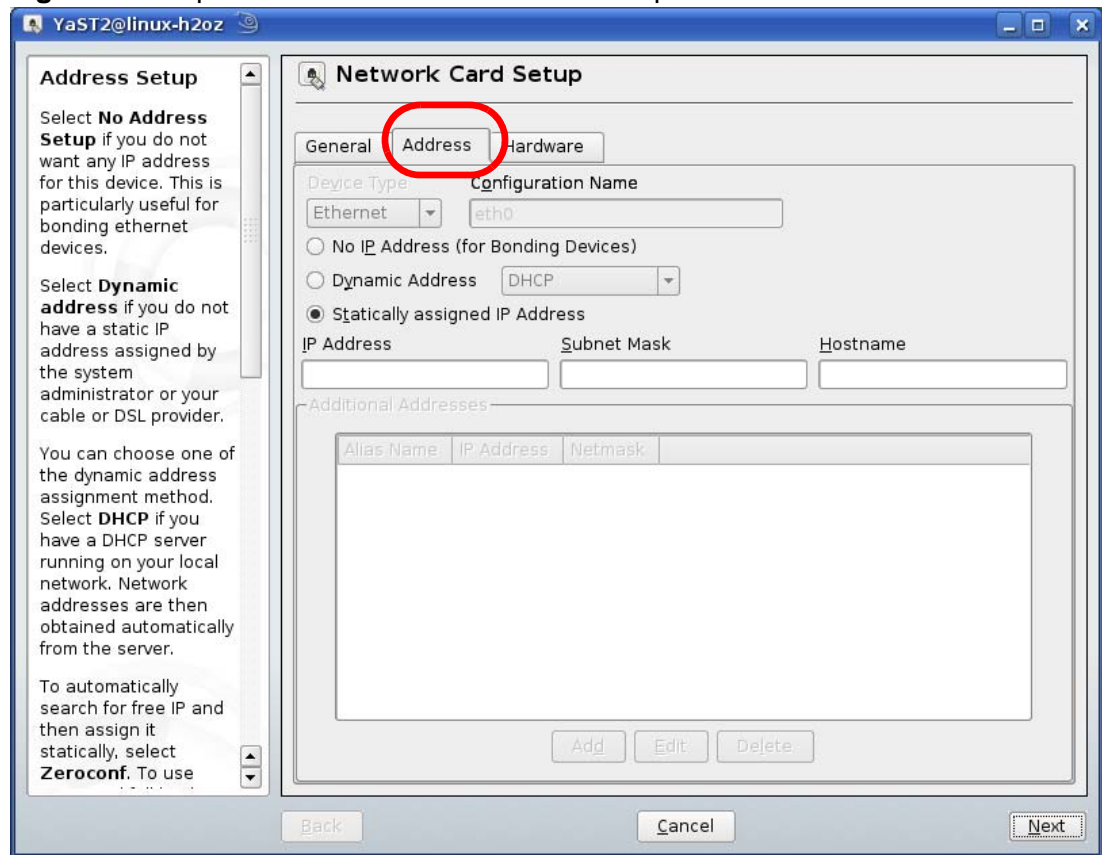
- 4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.

**Figure 135** openSUSE 10.3: Network Settings



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

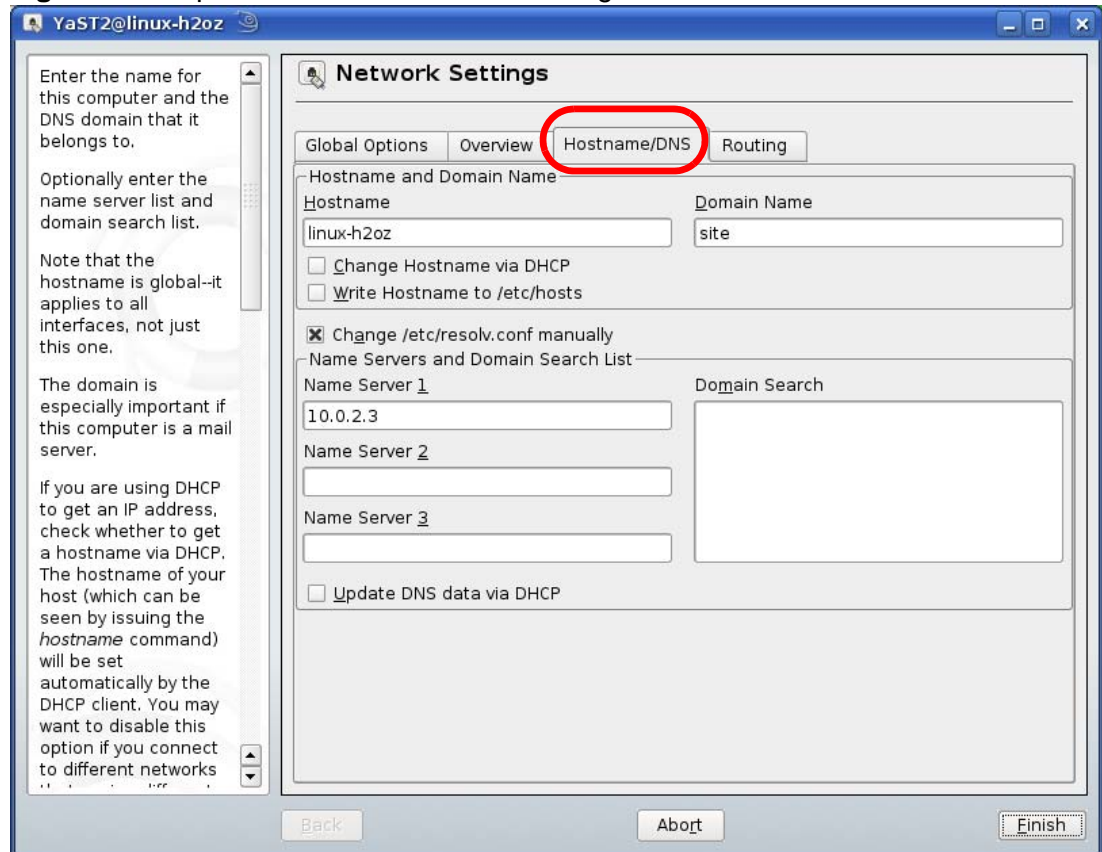
**Figure 136** openSUSE 10.3: Network Card Setup



- 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 137** openSUSE 10.3: Network Settings

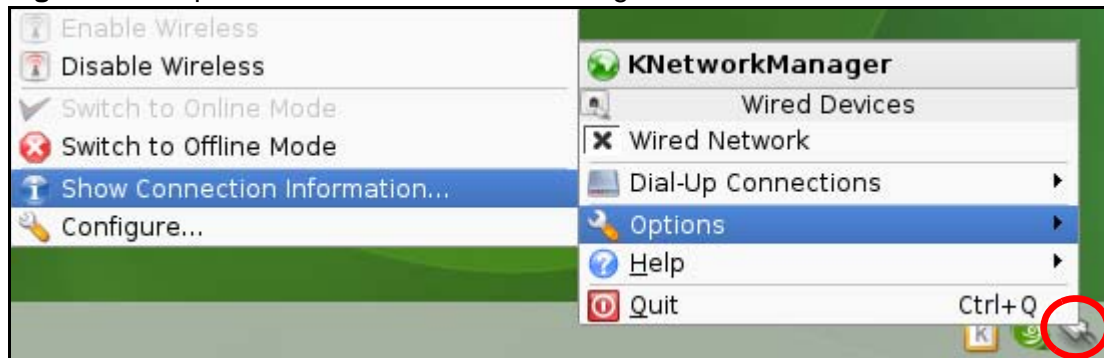


- 9 Click **Finish** to save your settings and close the window.

## Verifying Settings

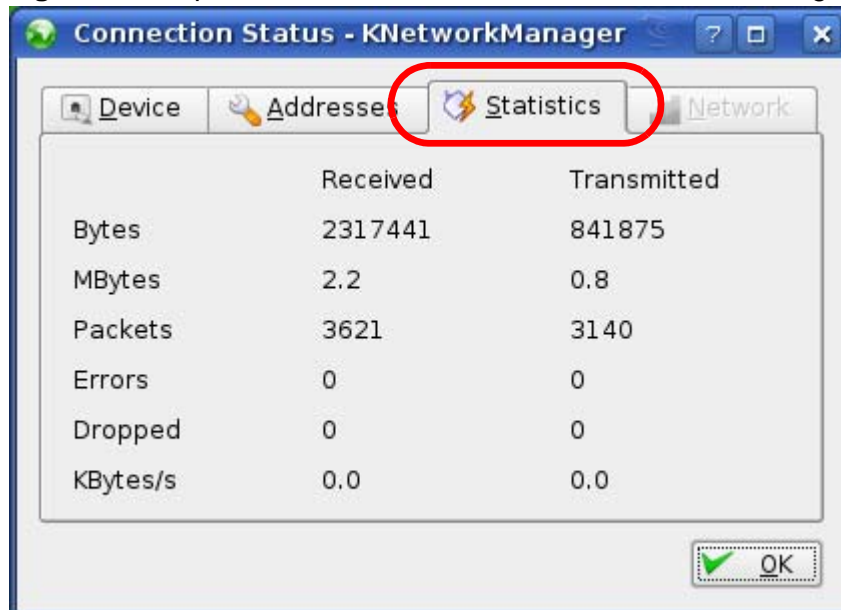
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

**Figure 138** 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 139** openSUSE: Connection Status - KNetwork Manager







# Pop-up Windows, JavaScripts and Java Permissions

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

- Web browser pop-up windows from your device.
- JavaScripts (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

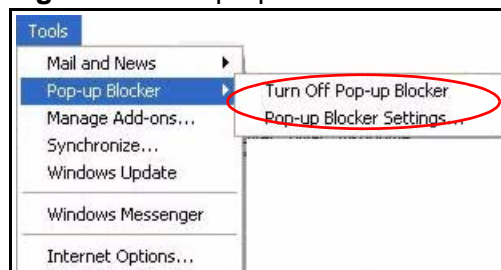
You may have to disable pop-up blocking to log into your device.

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**.

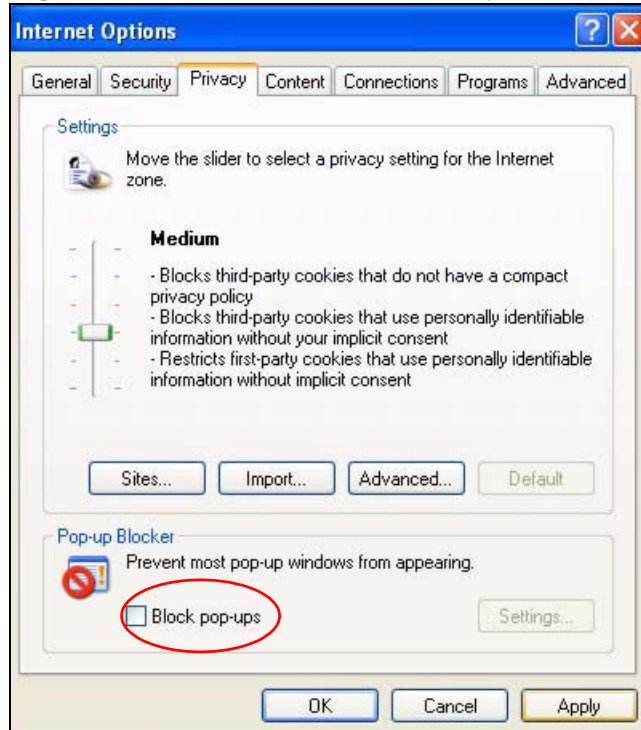
**Figure 140** Pop-up Blocker



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 141** Internet Options: Privacy



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

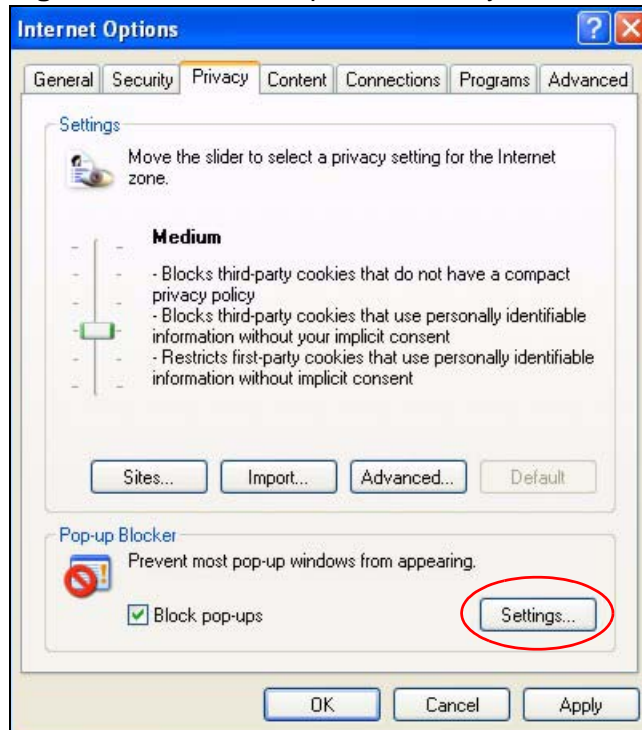
### Enable Pop-up Blockers with Exceptions

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.

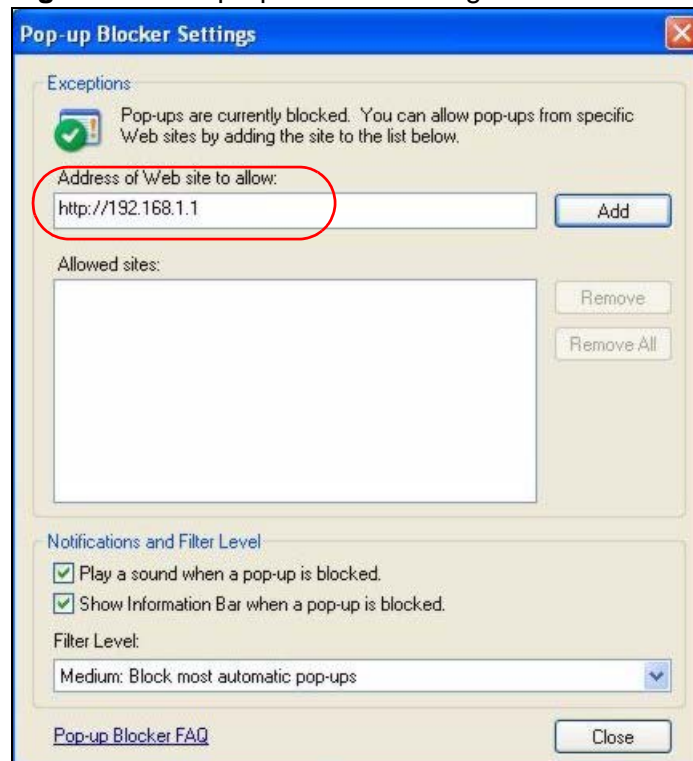
**Figure 142** Internet Options: Privacy



- 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 143** Pop-up Blocker Settings



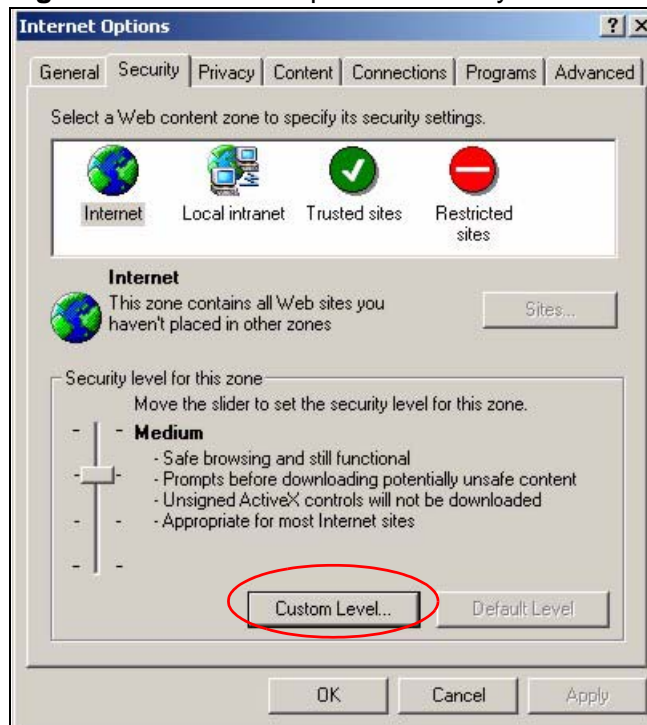
- 5 Click **Close** to return to the **Privacy** screen.
- 6 Click **Apply** to save this setting.

## JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

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

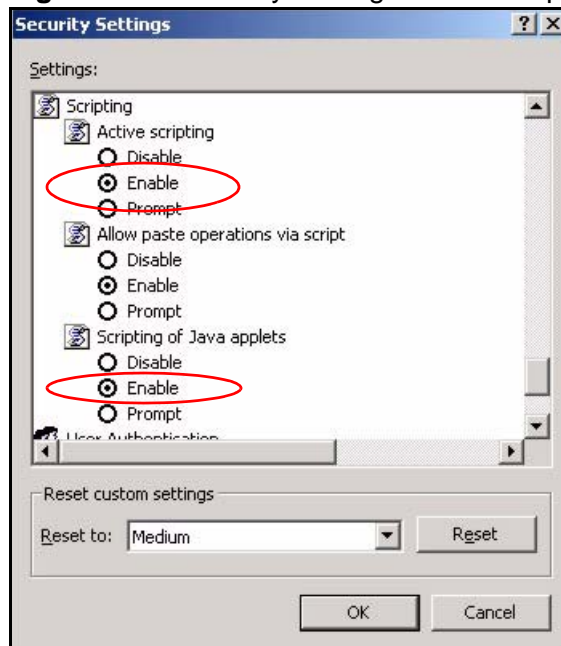
**Figure 144** Internet Options: Security



- 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 145** Security Settings - Java Scripting

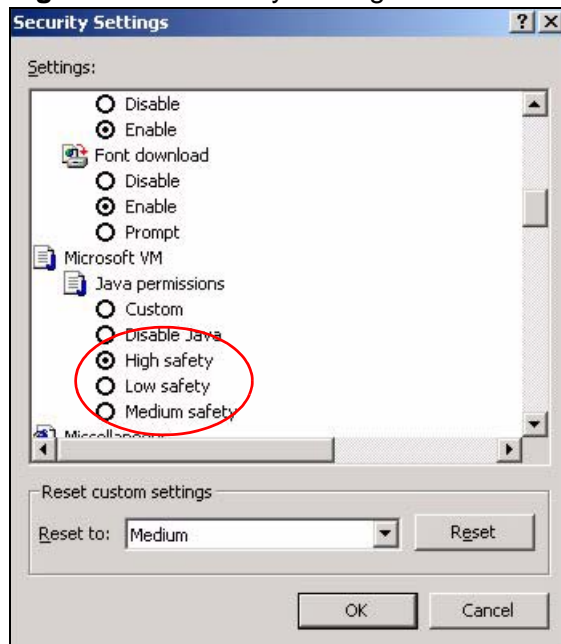


## Java Permissions

- 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.

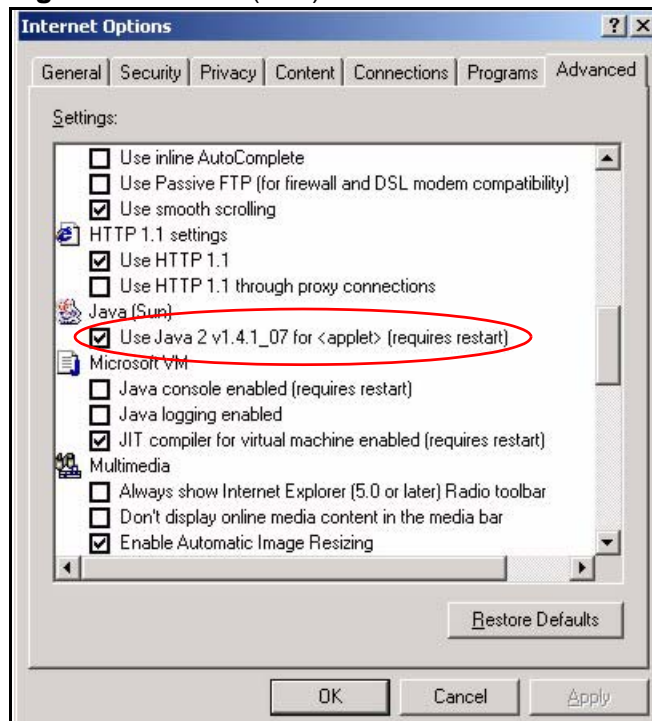
**Figure 146** Security Settings - Java



## 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.

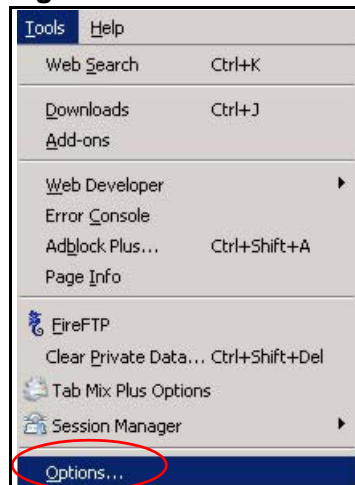
- 3 Click **OK** to close the window.

**Figure 147** Java (Sun)

## Mozilla Firefox

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

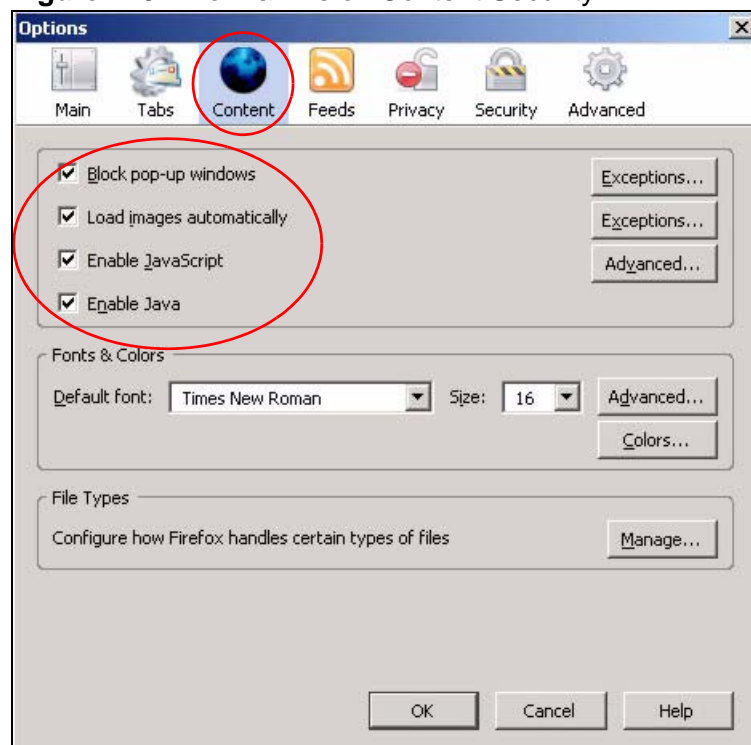
You can enable Java, Javascripts and pop-ups in one screen. Click **Tools**, then click **Options** in the screen that appears.

**Figure 148** Mozilla Firefox: Tools > Options



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

**Figure 149** 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.

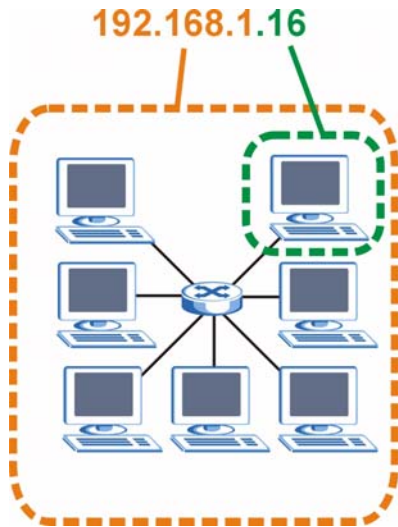
## Structure

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 150** 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 59** IP Address Network Number and Host ID Example

	<b>1ST OCTET: (192)</b>	<b>2ND OCTET: (168)</b>	<b>3RD OCTET: (1)</b>	<b>4TH OCTET (2)</b>
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	<b>11111111</b>	<b>11111111</b>	<b>11111111</b>	00000000
Network Number	<b>11000000</b>	<b>10101000</b>	<b>00000001</b>	
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 60** 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 61** 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 62** 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

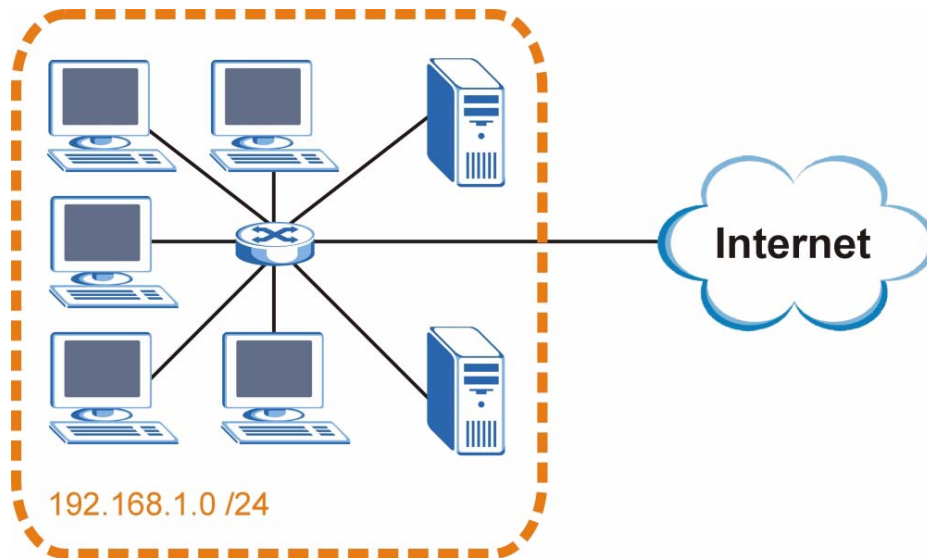
## Subnetting

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 151** Subnetting Example: Before Subnetting

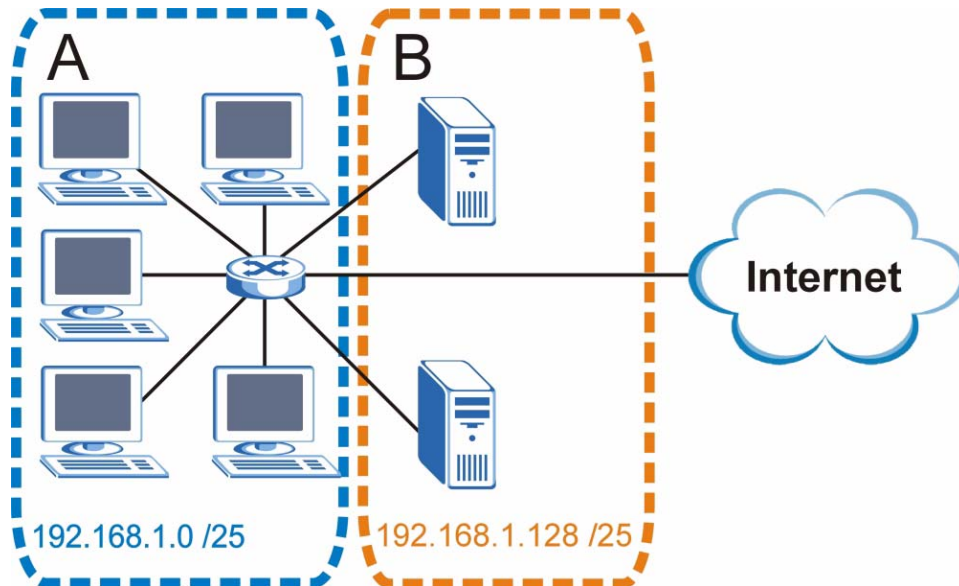


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

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 152** 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 63** 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 64** 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 65** 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 66** 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 66** 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 67** 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 68** 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 69** 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

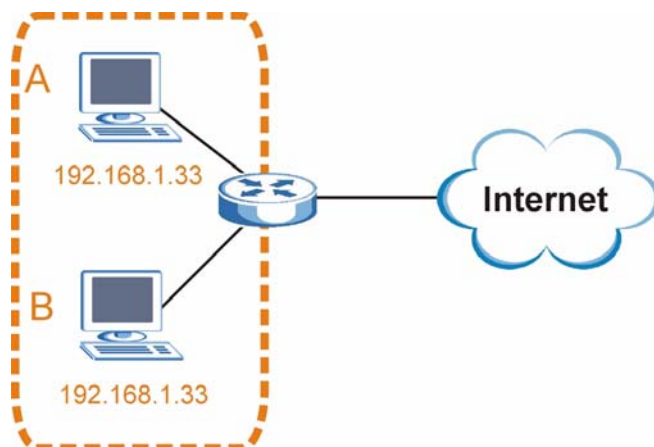
Each device on a network must have a unique IP address. Devices with duplicate IP addresses on the same network will not be able to access the Internet or other resources. The devices may also be unreachable through the network.

### 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.

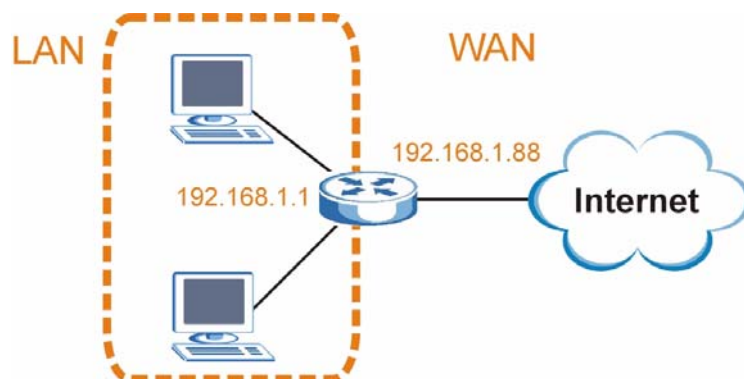
**Figure 153** Conflicting Computer IP Addresses Example



### 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 154** Conflicting Computer IP Addresses Example

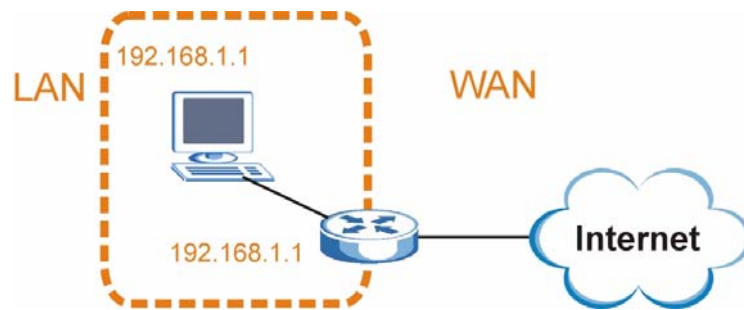


### Conflicting Computer and Router IP Addresses Example

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 155** Conflicting Computer and Router IP Addresses Example



# Wireless LANs

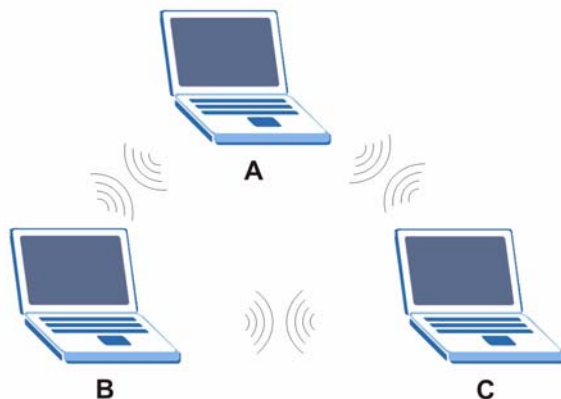
## Wireless LAN Topologies

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 156** Peer-to-Peer Communication in an Ad-hoc Network



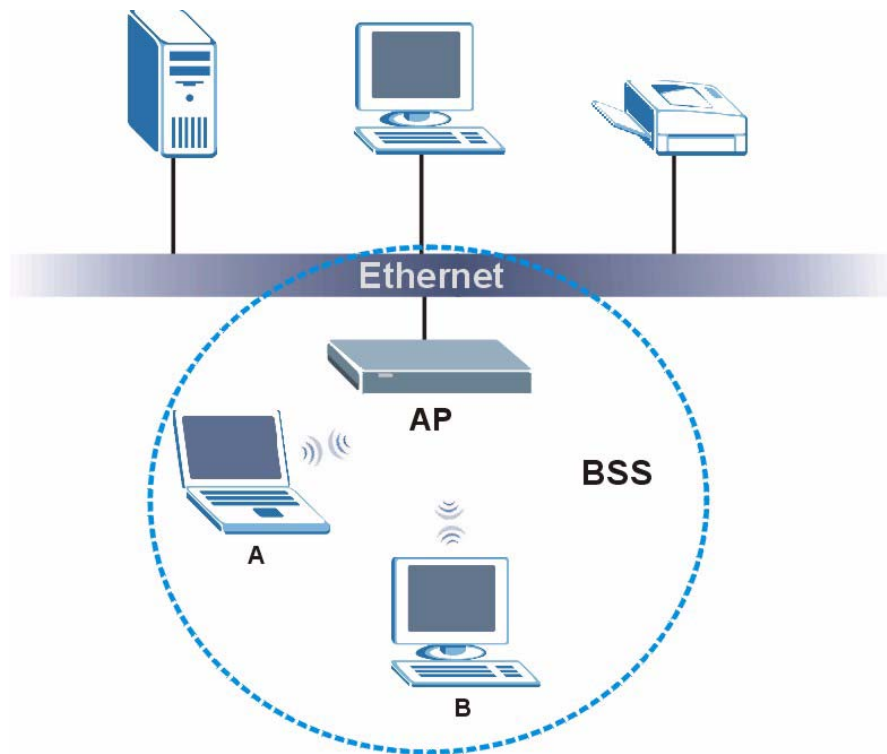
### BSS

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 157** Basic Service Set



## ESS

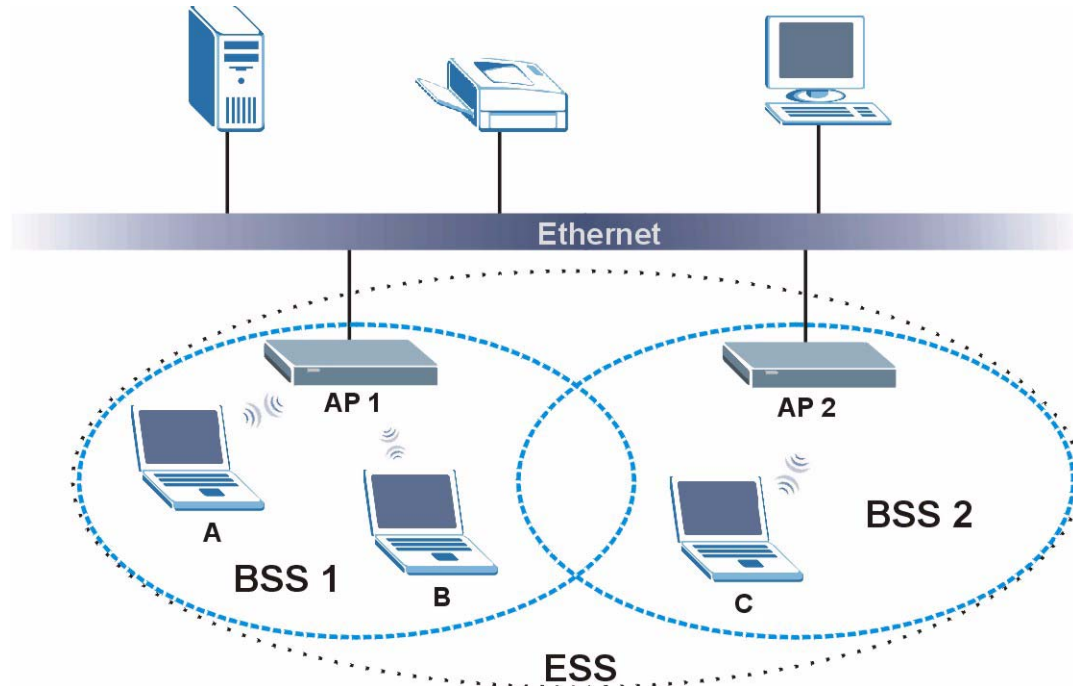
An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

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 158** 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.

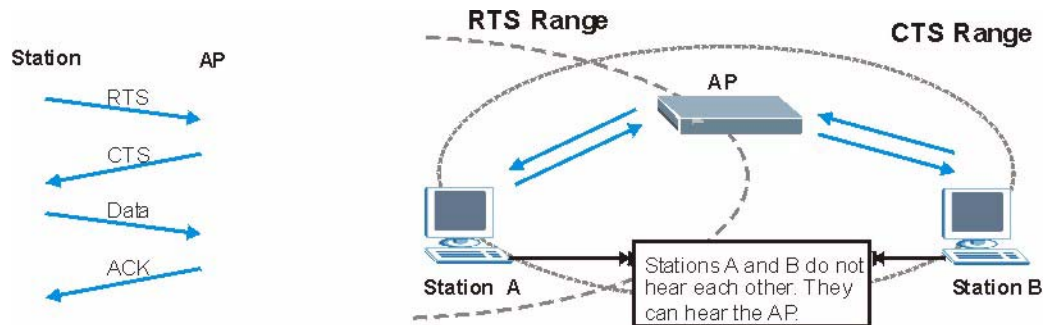
Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel 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 159** 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 70** 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 71** 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 72** 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.

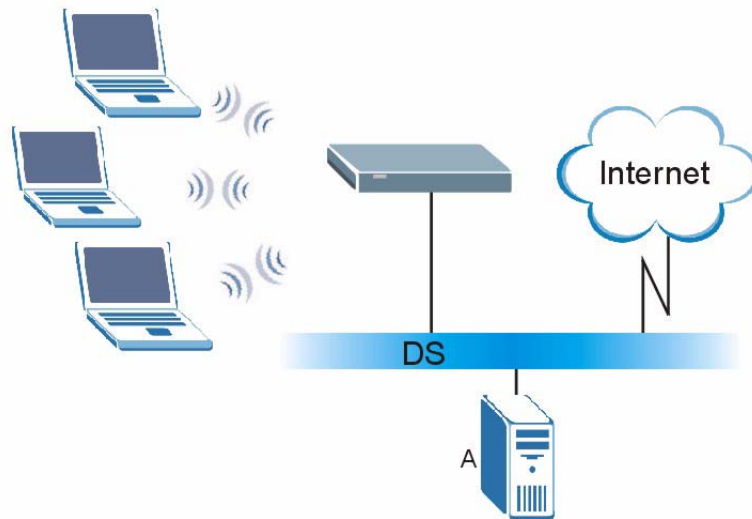
## WPA(2) with RADIUS Application Example

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 160** WPA(2) with RADIUS Application Example



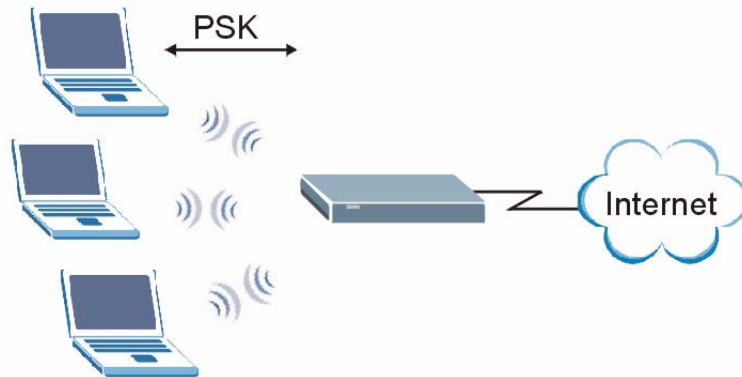
### WPA(2)-PSK Application Example

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 161** 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 73** 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 74** 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 <a href="http://www.zyxel.com">www.zyxel.com</a> ) to IP numbers.

**Table 74** 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 74** 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 74** 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.

# Legal Information

## Copyright

Copyright © 2009 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

### 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](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](http://www.zyxel.com).

# Index

## A

AAL5 [189](#)  
ACS [143](#)  
ADSL2 [189](#)  
Advanced Encryption Standard  
    See AES.  
AES [257](#)  
alternative subnet mask notation [238](#)  
antenna [187](#)  
    directional [262](#)  
    gain [261](#)  
    omni-directional [262](#)  
AP (access point) [249](#)  
applications  
    Internet access [20](#)  
ATM AAL5 [189](#)  
ATM Adaptation Layer 5 (AAL5) [189](#)  
Auto Configuration Server, see ACS [143](#)  
auto-negotiating rate adaptation [189](#)

## B

backup [176](#)  
Basic Service Set, See BSS [247](#)  
blinking LEDs [21](#)  
broadcast [67](#)  
BSS [247](#)

## C

CA [255](#)  
Canonical Format Indicator See CFI  
Certificate Authority  
    See CA.  
certifications [267](#)  
    notices [269](#)

    viewing [269](#)  
CFI [67](#)  
channel [249](#)  
    interference [249](#)  
channel ID [83](#)  
configuration [70](#), [75](#)  
copyright [267](#)  
CoS [138](#)  
CoS technologies [130](#)  
CPU usage [41](#)  
CTS (Clear to Send) [250](#)

## D

date and time [41](#)  
default [178](#)  
default LAN IP address [35](#)  
DHCP [47](#), [70](#), [75](#), [141](#)  
DHCP client [47](#)  
DHCP client list [47](#)  
DHCP relay [188](#)  
DHCP server [188](#)  
Differentiated Services, see DiffServ [138](#)  
DiffServ [138](#)  
    marking rule [139](#)  
disclaimer [267](#)  
DNS [70](#)  
DNS server address assignment [67](#)  
Domain Name [112](#)  
domain name system  
    see DNS  
Domain Name System. See DNS.  
DS field [139](#)  
DS, dee differentiated services  
DSCP [138](#)  
DSL interface [52](#)  
dynamic DNS [141](#)

Dynamic Host Configuration Protocol. See DHCP.  
dynamic WEP key exchange [256](#)  
DYNDNS wildcard [141](#)

## E

EAP Authentication [254](#)  
EAP-MD5 [191](#)  
ECHO [112](#)  
encapsulated routing link protocol (ENET ENCAP) [64](#)  
Encapsulation [64](#)  
    PPP over Ethernet [64](#)  
encapsulation  
    ENET ENCAP [64](#)  
encryption [257](#)  
    WEP [86](#)  
ESS [248](#)  
ESSID [40](#)  
Extended Service Set IDentification [83](#)  
Extended Service Set, See ESS [248](#)  
external antenna [190](#)  
external RADIUS [191](#)

## F

F4/F5 OAM [189](#)  
FCC interference statement [267](#)  
Finger [112](#)  
firmware  
    upload [174](#)  
    upload error [175](#)  
firmware version [40](#)  
fragmentation threshold [251](#)  
frequency range [191](#)  
FTP [108](#), [112](#)

## G

G.992.1 [189](#)

G.992.3 [189](#)  
G.992.4 [189](#)  
G.992.5 [189](#)

## H

hidden node [249](#)  
host [166](#)  
host name [40](#)  
HTTP [112](#), [117](#), [118](#)  
HTTP (Hypertext Transfer Protocol) [174](#)  
humidity [187](#)

## I

IANA [76](#), [244](#)  
IBSS [247](#)  
IEEE 802.11g [251](#)  
IEEE 802.11g wireless LAN [190](#)  
IEEE 802.11i [190](#)  
IEEE 802.1Q [66](#)  
IGMP [67](#), [70](#), [77](#)  
    version [67](#)  
IGMP proxy [190](#)  
IGMP v1 [190](#)  
IGMP v2 [190](#)  
Independent Basic Service Set  
    See IBSS [247](#)  
initialization vector (IV) [257](#)  
install UPnP [151](#)  
    Windows Me [151](#)  
    Windows XP [153](#)  
internal routing table [43](#)  
Internet access [20](#)  
Internet Assigned Numbers Authority  
    See IANA [244](#)  
IP Address [111](#)  
IP address [76](#)  
IP Address Assignment [64](#)  
IP alias [189](#)  
IP filter  
    basics [117](#)



- creating or editing rules [120](#)
- introduction [117](#)
- policies [118](#)
- IP multicasting [190](#)
- IP pool [72](#)
- IP pool setup [75](#)

## L

- LAN statistics [46](#)
- LAN TCP/IP [75](#)
- logs [169](#)
  - overview [169](#)
  - settings [170](#)

## M

- MAC [40](#)
- MAC address [40](#)
- MAC address filter action [92](#)
- MAC filter [91](#)
- managing the device
  - good habits [20](#)
- memory usage [41](#)
- Message Integrity Check (MIC) [257](#)
- MTU (Multi-Tenant Unit) [66](#)
- multicast [67](#), [70](#), [77](#)
- multiple PVC support [189](#)

## N

- NAT [76](#), [107](#), [243](#)
  - default server [111](#)
  - DMZ host [111](#)
  - external port [109](#)
  - internal port [109](#)
  - port forwarding [108](#)
  - port number [108](#), [112](#)
  - services [112](#)
  - Symmetric [65](#)
- NAT example [113](#)
- NAT traversal [149](#)

- Network Address Translation, see NAT
- NNTP [112](#)

## O

- OAM [189](#)
- operation humidity [187](#)
- operation temperature [187](#)

## P

- Packet Transfer Mode [52](#)
- Pairwise Master Key (PMK) [257](#), [259](#)
- Per-Hop Behavior, see PHB [139](#)
- Permanent Virtual Circuits [189](#)
- PHB [139](#)
- Point-to-Point Tunneling Protocol [112](#)
- POP3 [112](#), [117](#), [118](#)
- ports [21](#)
- power adaptor [191](#)
- power specifications [187](#)
- PPP (Point-to-Point Protocol) Link Layer Protocol [190](#)
- PPP over ATM AAL5 [189](#)
- PPP over Ethernet [189](#)
- PPPoE [64](#)
  - Benefits [64](#)
- PPPoE (Point-to-Point Protocol over Ethernet) [189](#)
- PPTP [112](#)
- preamble mode [251](#)
- product registration [270](#)
- PSK [257](#)
- PTM [52](#)
- PVCs [189](#)

## Q

- QoS [129](#), [138](#)
  - marking [130](#)
  - setup [129](#)

- tagging [130](#)
- versus CoS [130](#)
- Quality of Service, see QoS
- Quick Start Guide [35](#)

## R

- RADIUS [191](#), [253](#)
  - message types [253](#)
  - messages [253](#)
  - shared secret key [254](#)
- Reach-Extended ADSL [189](#)
- registration
  - product [270](#)
- related documentation [3](#)
- remote management
  - TR-069 [143](#)
- Remote Procedure Calls, see RPCs [143](#)
- resetting your device [22](#)
- restore [177](#)
- RFC 1483 [189](#)
- RFC 1631 [107](#)
- RFC 2131. See DHCP.
- RFC 2132. See DHCP
- RFC 2364 [189](#)
- RFC 2516 [189](#)
- RFC 2684 [189](#)
- RIP [70](#)
  - Routing Information Protocol
  - see RIP
- route status [44](#)
- router features [20](#)
- routing information [43](#)
- RPPCs [143](#)
- RTS (Request To Send) [250](#)
  - threshold [249](#), [250](#)

## S

- safety warnings [7](#)
- seamless rate adaptation [189](#)
- service access control [145](#)

- Service Set [83](#)
- Services [112](#)
- SMTP [112](#)
- SNMP [112](#), [190](#)
- SNMP trap [112](#)
- SRA [189](#)
- static route [125](#)
- static VLAN
- status indicators [21](#)
- storage humidity [187](#)
- storage temperature [187](#)
- subnet [235](#)
- subnet mask [76](#), [236](#)
- subnetting [238](#)
- Symmetric NAT [65](#)
- Symmetric NAT, Outgoing [66](#)
- syntax conventions [5](#)
- system name [40](#)

## T

- Tag Control Information See TCI
- Tag Protocol Identifier See TPID
- TCI
- TCP/IP [117](#)
- temperature [187](#)
- Temporal Key Integrity Protocol (TKIP) [257](#)
- TLS [191](#)
- TPID [66](#)
- TR-069 [143](#)
  - ACS setup [143](#)
  - authentication [144](#)
- trademarks [267](#)
- transparent bridging [190](#)
- TTLS [191](#)

## U

- unicast [67](#)
- Universal Plug and Play [149](#)
  - application [150](#)

UPnP [149](#)

forum [150](#)

security issues [150](#)

## V

VID

Virtual Local Area Network See VLAN

VLAN [66](#)

Introduction [66](#)

number of possible VIDs

priority frame

static

VLAN ID [66](#)

VLAN Identifier See VID

VLAN tag [66](#)

## W

WAN (Wide Area Network) [51](#)

WAN interface [42](#)

WAN statistics [42](#)

warranty [269](#)

note [269](#)

Web Configurator [35](#)

WEP (Wired Equivalent Privacy) [190](#)

WEP encryption [87](#)

Wi-Fi Protected Access [256](#)

Wi-Fi Protected Access (WPA) [190](#)

wireless client WPA supplicants [258](#)

wireless LAN MAC address filtering [190](#)

wireless security [252](#)

wireless station list [45](#)

Wireless tutorial [25](#)

WLAN

interference [249](#)

security parameters [260](#)

WLAN button [23](#)

WPA [256](#)

key caching [258](#)

pre-authentication [258](#)

user authentication [258](#)

vs WPA-PSK [257](#)

wireless client supplicant [258](#)

with RADIUS application example [258](#)

WPA2 [256](#)

user authentication [258](#)

vs WPA2-PSK [257](#)

wireless client supplicant [258](#)

with RADIUS application example [258](#)

WPA2-Pre-Shared Key [256](#)

WPA2-PSK [256](#), [257](#)

application example [259](#)

WPA-PSK [257](#)

application example [259](#)

WPS

status [40](#)

