P-2601HN(L)-F1 Series

ADSL2+ IAD with 802.11n Wireless

User's Guide

Firmware Version 3.10

Edition 1, 10/2010

Default Login Details

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

www.zyxel.com

ZyXEL

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the ZyXEL Device using the web configurator.

Related Documentation

- Quick Start Guide

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

- Support Disc

  Refer to the included CD for support documents.

Documentation Feedback

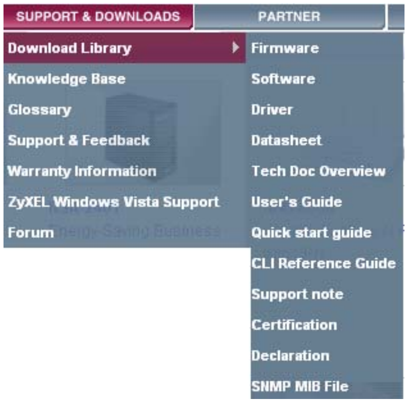
Send your comments, questions or suggestions to: techwriters@zyxel.com.tw

Thank you!

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

Need More Help?

More help is available at www.zyxel.com.



- Download Library

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

- Knowledge Base

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

- Forum

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

Customer Support

Should problems arise that cannot be solved by the methods listed above, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device.

See http://www.zyxel.com/web/contact_us.php for contact information. Please have the following information ready when you contact an office.

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

Document Conventions

Warnings and Notes

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

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

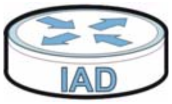
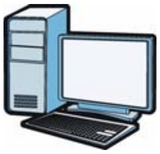
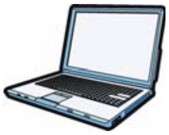
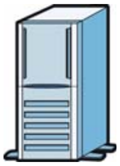
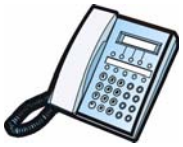
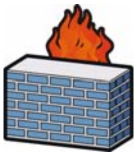
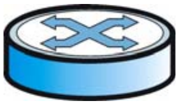
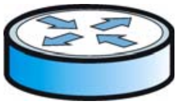
Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The P-2601HN(L)-F1 series may be referred to as the "ZyXEL Device", the "device", the "system" or the "product" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

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

ZyXEL Device  	Computer 	Notebook computer 
Server 	Telephone 	Firewall 
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).
- This CPE is indoor use only. (Utilisation intérieure exclusivement.)

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

Contents Overview

User's Guide 19

Introducing the ZyXEL Device 21
Introducing the Web Configurator 27
Tutorials 35

Technical Reference 59

Connection Status and System Info Screens 61
Broadband 67
Wireless 81
Home Networking 111
Routing 127
DNS Route 131
Quality of Service (QoS) 135
Network Address Translation (NAT) 149
Dynamic DNS 157
Firewall 159
MAC Filter 165
Certificates 167
VoIP 175
Logs 203
System Monitor 207
User Account 213
Remote MGMT 215
SNMP 217
System 221
Time Setting 223
Log Setting 225
Firmware Upgrade 227
Backup/Restore 229
Diagnostic 233
Troubleshooting 237
Product Specifications 243

Table of Contents

About This User's Guide 3

Document Conventions 5

Safety Warnings 7

Contents Overview 9

Table of Contents 11

Part I: User’s Guide 19

Chapter 1
Introducing the ZyXEL Device 21

1.1 Overview 21
1.2 Applications for the ZyXEL Device 22
1.2.1 Internet Access 22
1.2.2 Internet Calls (VoIP) 22
1.2.3 Wireless Connection 23
1.3 Ways to Manage the ZyXEL Device 23
1.4 Good Habits for Managing the ZyXEL Device 24
1.5 LEDs (Lights) 24
1.6 The RESET Button 25
1.7 The WIRELESS ON/OFF Button 26

Chapter 2
Introducing the Web Configurator 27

2.1 Overview 27
2.1.1 Accessing the Web Configurator 27
2.2 The Web Configurator Layout 30
2.2.1 Title Bar 31
2.2.2 Main Window 31
2.2.3 Navigation Panel 31
2.2.4 Status Bar 34

Chapter 3
Tutorials 35

3.1 Overview 35

3.2 Setting Up Your DSL Connection 35
3.3 How to Set up a Wireless Network 38
3.3.1 Example Parameters 38
3.3.2 Configuring the AP 38
3.3.3 Configuring the Wireless Client 40
3.4 Setting Up NAT Port Forwarding 45
3.5 How to Make a VoIP Call 47
3.5.1 VoIP Calls With a Registered SIP Account 47
3.6 Configuring the MAC Address Filter 50
3.7 Configuring Static Route for Routing to Another Network 51
3.8 Configuring QoS Queue and Class Setup 53
3.9 Access the ZyXEL Device Using DDNS 56
3.9.1 Registering a DDNS Account on www.dyndns.org 57
3.9.2 Configuring DDNS on Your ZyXEL Device 57
3.9.3 Testing the DDNS Setting 58

Part II: Technical Reference 59

Chapter 4
Connection Status and System Info Screens 61

4.1 Overview 61
4.2 The Connection Status Screen 61
4.3 The System Info Screen 63

Chapter 5
Broadband 67

5.1 Overview 67
5.1.1 What You Need to Know 67
5.1.2 Before You Begin 68
5.2 The Broadband Screen 69
5.2.1 Add/Edit Broadband 70
5.3 Technical Reference 76
5.3.1 Encapsulation 76
5.3.2 Multiplexing 77
5.3.3 VPI and VCI 77
5.3.4 IP Address Assignment 77
5.3.5 NAT 78
5.4 Traffic Shaping 78
5.4.1 ATM Traffic Classes 79

Chapter 6
Wireless 81

6.1 Overview 81
6.1.1 What You Can Do in this Chapter 81
6.1.2 Wireless Network Overview 81
6.1.3 Before You Begin 83
6.2 The Wireless General Screen 83
6.2.1 No Security 85
6.2.2 Basic (Static WEP/Shared WEP Encryption) 86
6.2.3 More Secure (WPA(2)-PSK) 88
6.2.4 WPA(2) Authentication 89
6.3 The More AP Screen 91
6.3.1 Edit More AP 92
6.4 The WPS Screen 93
6.5 The WMM Screen 95
6.6 Scheduling Screen 97
6.7 Technical Reference 97
6.7.1 Additional Wireless Terms 98
6.7.2 Wireless Security Overview 98
6.7.3 Signal Problems 101
6.7.4 BSS 101
6.7.5 MBSSID 102
6.7.6 WiFi Protected Setup (WPS) 103

Chapter 7
Home Networking 111

7.1 Overview 111
7.1.1 What You Can Do in this Chapter 111
7.1.2 What You Need To Know 111
7.2 The LAN Setup Screen 113
7.3 The Static DHCP Screen 114
7.3.1 Before You Begin 115
7.4 The UPnP Screen 116
7.5 Technical Reference 117
7.6 Installing UPnP in Windows Example 119
7.7 Using UPnP in Windows XP Example 122

Chapter 8
Routing 127

8.1 Overview 127
8.2 Configuring Static Route 128
8.2.1 Add/Edit Static Route 129

Chapter 9
DNS Route 131

9.1 Overview 131
9.2 The DNS Route Screen 132
9.2.1 Add/Edit DNS Route Edit 132

Chapter 10
Quality of Service (QoS)........ 135

10.1 Overview 135
10.1.1 What You Can Do in this Chapter 135
10.1.2 What You Need to Know 136
10.2 The QoS General Screen 136
10.3 The Queue Setup Screen 138
10.3.1 Add/Edit a QoS Queue 139
10.4 The Class Setup Screen 140
10.4.1 Add/Edit QoS Class 142
10.5 The QoS Monitor Screen 145
10.6 QoS Technical Reference 146
10.6.1 IEEE 802.1Q Tag 146
10.6.2 IP Precedence 147
10.6.3 DiffServ 147

Chapter 11
Network Address Translation (NAT)........ 149

11.1 Overview 149
11.1.1 What You Can Do in this Chapter 149
11.1.2 What You Need To Know 149
11.2 The Port Forwarding Screen 150
11.2.1 The Port Forwarding Screen 151
11.2.2 The Port Forwarding Edit Screen 152
11.3 The Sessions Screen 153
11.4 Technical Reference 154
11.4.1 NAT Definitions 154
11.4.2 What NAT Does 155
11.4.3 How NAT Works 155

Chapter 12
Dynamic DNS 157

12.1 Overview 157
12.1.1 What You Need To Know 157
12.2 The Dynamic DNS Screen 158

Chapter 13
Firewall........ 159

13.1 Overview 159

13.1.1 What You Can Do in this Chapter 159
13.1.2 What You Need to Know 160
13.2 The General Screen 161
13.3 The Services Screen 161
13.4 Firewall Technical Reference 163
13.4.1 Guidelines For Enhancing Security With Your Firewall 163
13.4.2 Security Considerations 163

Chapter 14
MAC Filter 165

14.1 Overview 165
14.1.1 What You Need to Know 165
14.2 The MAC Filter Screen 166

Chapter 15
Certificates 167

15.1 Overview 167
15.1.1 What You Can Do in this Chapter 167
15.1.2 What You Need to Know 167
15.1.3 Verifying a Certificate 169
15.2 Local Certificates 170
15.3 Trusted CA 172
15.4 Trusted CA Import 173
15.5 View Certificate 173

Chapter 16
VoIP 175

16.1 Overview 175
16.1.1 What You Can Do in this Chapter 175
16.1.2 What You Need to Know 176
16.1.3 Before You Begin 177
16.2 The SIP Service Provider Screen 177
16.3 The SIP Account Screen 181
16.3.1 Add/Edit SIP Account 183
16.4 The SIP Common Screen 186
16.5 The Phone Device Screen 187
16.5.1 Edit Phone Device 187
16.6 The Region Screen 188
16.7 The Call Rule Screen 189
16.8 The FXO Screen (“L” Models Only) 190
16.9 Technical Reference 191
16.9.1 VoIP 191
16.9.2 SIP 192

16.9.3 Quality of Service (QoS) 197
16.9.4 Phone Services Overview 198

Chapter 17
Logs 203

17.1 Overview 203
17.1.1 What You Can Do in this Chapter 203
17.2 The Phone Log Screen 203
17.3 The VoIP Call History Screen 204

Chapter 18
System Monitor 207

18.1 Overview 207
18.1.1 What You Can Do in this Chapter 207
18.2 The WAN Status Screen 207
18.3 The LAN Status Screen 208
18.4 The NAT Status Screen 209
18.5 The VoIP Status Screen 210

Chapter 19
User Account..... 213

19.1 Overview 213
19.2 The User Account Screen 213

Chapter 20
Remote MGMT..... 215

20.1 Overview 215
20.1.1 What You Need to Know 215
20.2 The Remote MGMT Screen 216

Chapter 21
SNMP..... 217

21.1 Overview 217
21.2 The SNMP Screen 217

Chapter 22
System 221

22.1 Overview 221
22.1.1 What You Need to Know 221
22.2 The System Screen 221

Chapter 23
Time Setting 223

23.1 Overview 223
23.2 The Time Setting Screen 223

Chapter 24
Log Setting 225

24.1 Overview 225
24.2 The Log Setting Screen 225

Chapter 25
Firmware Upgrade 227

25.1 Overview 227
25.2 The Firmware Upgrade Screen 227

Chapter 26
Backup/Restore 229

26.1 Overview 229
26.2 The Backup/Restore Screen 229
26.3 The Reboot Screen 231

Chapter 27
Diagnostic 233

27.1 Overview 233
27.1.1 What You Can Do in this Chapter 233
27.2 The Ping Screen 233
27.3 The DSL Line Screen 234

Chapter 28
Troubleshooting 237

28.1 Overview 237
28.2 Power, Hardware Connections, and LEDs 237
28.3 ZyXEL Device Access and Login 238
28.4 Internet Access 240
28.5 Phone Calls and VoIP 241
28.6 Wireless LAN Troubleshooting 242

Chapter 29
Product Specifications 243

Appendix A IP Addresses and Subnetting 253

Appendix B Setting Up Your Computer’s IP Address 265

Appendix C Pop-up Windows, JavaScript and Java Permissions 291

Appendix D Wireless LANs 299

Appendix E Common Services....................323

Appendix F Open Software Announcements....................327

Appendix G Legal Information....................333

Index....................337

PART I
User's Guide

1

Introducing the ZyXEL Device

1.1 Overview

The ZyXEL Device is an ADSL2+ Integrated Access Device (IAD) that combines an ADSL2+ router with Voice over IP (VoIP) communication capabilities to allow you to use a traditional analog telephone to make Internet calls. By integrating DSL and NAT, you are provided with ease of installation and high-speed, shared Internet access. The ZyXEL Device is also a complete security solution with a robust firewall and content filtering.

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).
- “N” denotes wireless functionality, including 802.11n mode. There is an embedded USB module for IEEE 802.11b/g/n wireless LAN connectivity.

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

- “L” denotes the PSTN (Public Switched Telephone Network) line feature. The PSTN line lets you have VoIP phone service and PSTN phone service at the same time. All PSTN line features documented in this user’s guide refer to the “L” models only.

When the ZyXEL Device does not have power, only the phone with lifeline connected to the FXO port can be used for making calls.

- Models ending in “1” denote a device that works over the analog telephone system, POTS (Plain Old Telephone Service).

See the chapter on product specifications for a full list of features.

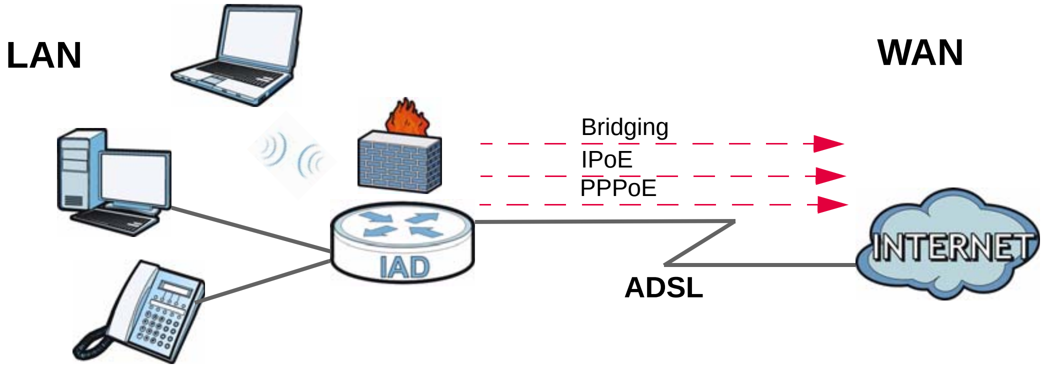
1.2 Applications for the ZyXEL Device

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

1.2.1 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 Internet Access Application



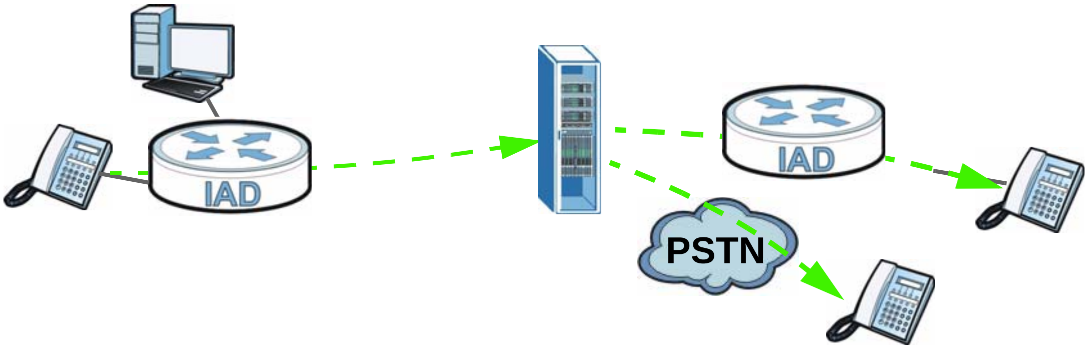
You can also configure firewall on the ZyXEL Device for secure Internet access. When the firewall is on, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely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

1.2.2 Internet Calls (VoIP)

You can register a SIP (Session Initiation Protocol) account and use the ZyXEL Device to make and receive VoIP telephone calls: You can register a SIP (Session

Initiation Protocol) account and use the ZyXEL Device to make and receive VoIP telephone calls:

Figure 2 ZyXEL Device's VoIP Application

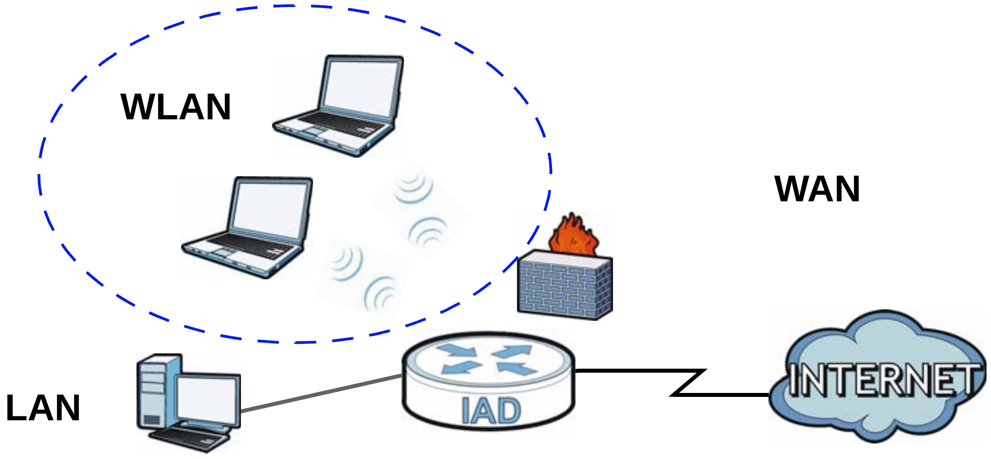


- Calls via a VoIP service provider - The ZyXEL Device sends your call to a VoIP service provider's SIP server which forwards your calls to either VoIP or PSTN phones.

1.2.3 Wireless Connection

By default, the wireless LAN (WLAN) is enabled on the ZyXEL Device. IEEE 802.11b/g/n compliant clients can wirelessly connect to the ZyXEL Device to access network resources. You can set up a wireless network with WPS (WiFi Protected Setup) or manually add a client to your wireless network.

Figure 3 Wireless Connection Application



1.3 Ways to Manage the ZyXEL Device

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

- Web Configurator. This is recommended for everyday management of the ZyXEL Device using a (supported) web browser.
- Command Line Interface (administrator account only). Line commands are mostly used for troubleshooting by service engineers.
- FTP for firmware upgrades and configuration backup/restore.

1.4 Good Habits for Managing the ZyXEL Device

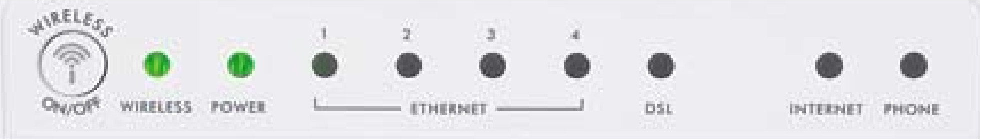
Do the following things regularly to make the ZyXEL Device more secure and to manage the ZyXEL Device more effectively.

- Change the password. Use a password that’s not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). 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.

1.5 LEDs (Lights)

The following graphic displays the labels of the LEDs.

Figure 4 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
WIRELESS	Green	On	The wireless network is activated and is operating in IEEE 802.11b/g/n 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.

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 performing Power On Self Test (POST).
	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.
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.
		Blinking	The ZyXEL Device is sending or receiving IP traffic.
	Red	On	The ZyXEL Device attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
	Off		The ZyXEL Device does not have an IP connection.
PHONE	Green	On	A SIP account is registered for the phone port.
		Blinking	A telephone connected to the phone port has its receiver off of the hook or there is an incoming call.
	Orange	On	A SIP account is registered for the phone port and there is a voice message in the corresponding SIP account.
		Blinking	A telephone connected to the phone port has its receiver off of the hook and there is a voice message in the corresponding SIP account.
	Off		The phone port does not have a SIP account registered.

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 passwords will be reset to the defaults.

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 5 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 WIRELESS ON/OFF Button

Use the **WIRELESS 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. Make sure the **POWER** LED is on (not blinking) before using the **WIRELESS ON/OFF** button.

- Press the **WIRELESS ON/OFF** button for one to five (1 - 5) second/s and release it. The **WIRELESS** LED should change from on to off or vice versa.
- Press the **WIRELESS ON/OFF** button for more than five seconds to turn on WPS. See Section 6.4 on page 93 for more on using WPS to configure your wireless clients.

2

Introducing the Web Configurator

2.1 Overview

The web configurator is an HTML-based management interface that allows easy device setup and management via Internet browser. Use Internet Explorer 6.0 and later versions, Mozilla Firefox 3 and later versions, or Safari 2.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

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

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

See Appendix C on page 291 if you need to make sure these functions are allowed in Internet Explorer.

2.1.1 Accessing the Web Configurator

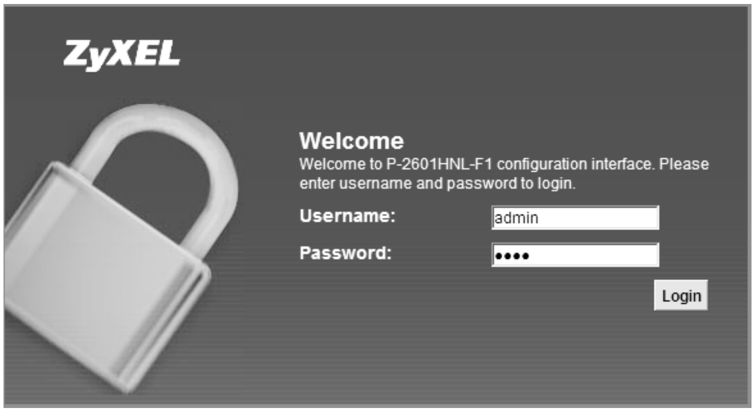
1 Make sure your ZyXEL Device hardware is properly connected (refer to the Quick Start Guide).

2 Launch your web browser.

3 Type "192.168.1.1" as the URL.

4 A password screen displays. Type “admin” (default) as the username and “1234” as the password, and click **Login**. If you have changed the password, enter your password and click **Login**.

Figure 5 Password Screen



Welcome

Welcome to P-2601HNL-F1 configuration interface. Please enter username and password to login.

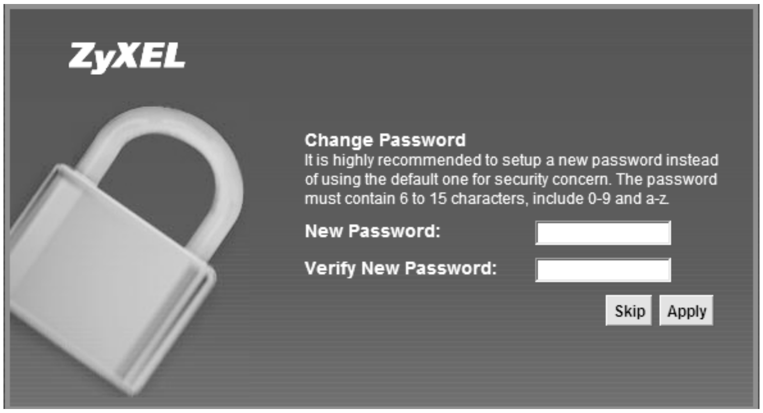
Username: admin

Password: ●●●●

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

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

Figure 6 Change Password Screen



Change Password

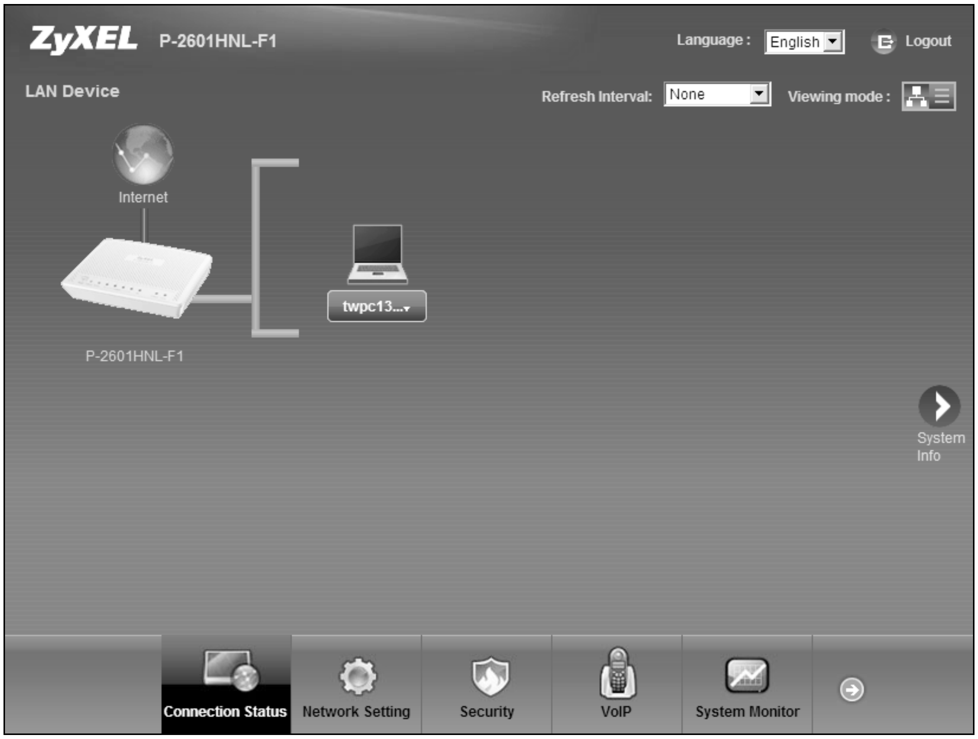
It is highly recommended to setup a new password instead of using the default one for security concern. The password must contain 6 to 15 characters, include 0-9 and a-z.

New Password:

Verify New Password:

6 The **Connection Status** screen appears.

Figure 7 Connection Status

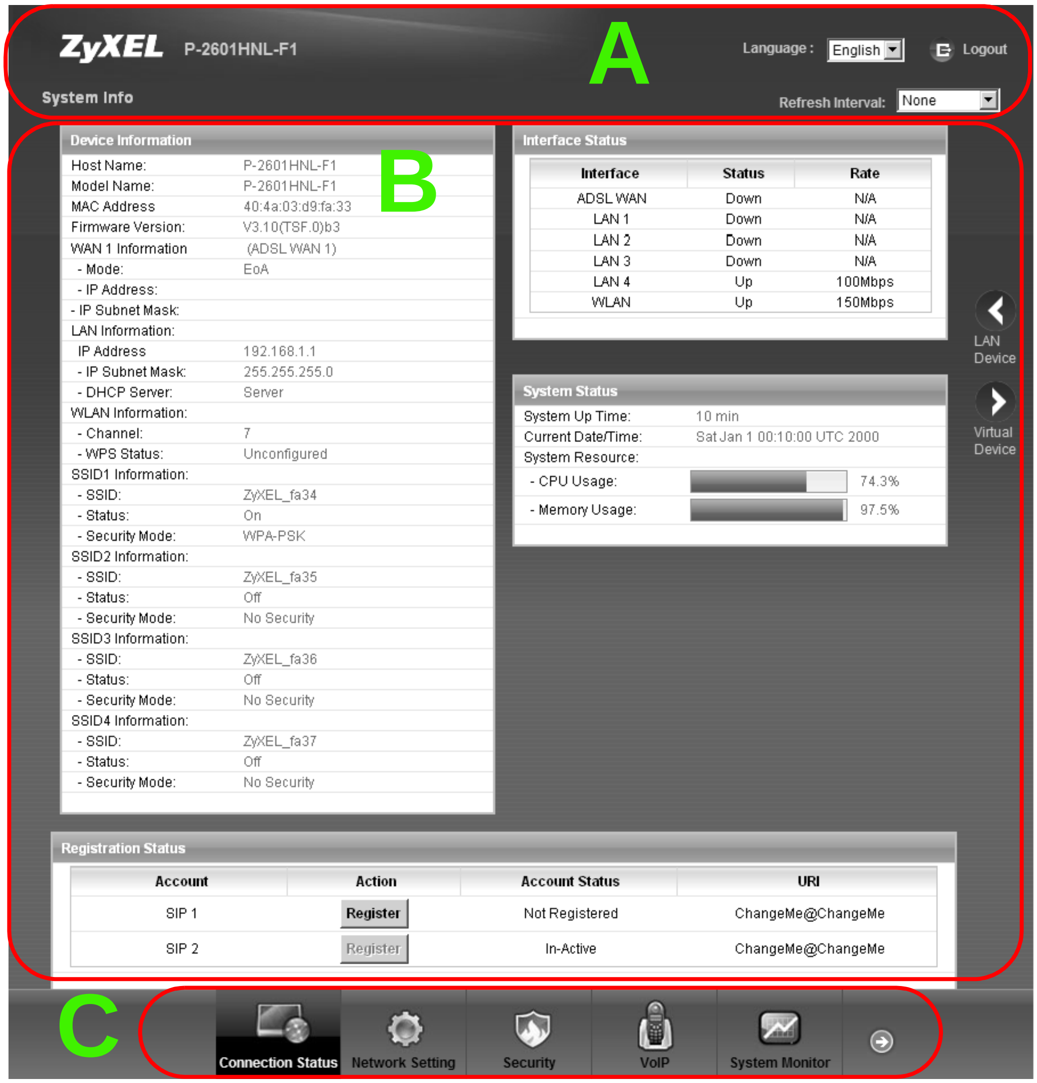


7 Click **System Info** to display the **System Info** screen, where you can view the ZyXEL Device’s interface and system information.

2.2 The Web Configurator Layout

Click **Connection Status > System Info** to show the following screen.

Figure 8 Web Configurator Layout



System Info

Refresh Interval: None

Device Information

Host Name:	P-2601HNL-F1
Model Name:	P-2601HNL-F1
MAC Address	40:4a:03:d9:fa:33
Firmware Version:	V3.10(TSF.0)b3
WAN 1 Information	(ADSL WAN 1)
- Mode:	EoA
- IP Address:	
- IP Subnet Mask:	
LAN Information:	
IP Address	192.168.1.1
- IP Subnet Mask:	255.255.255.0
- DHCP Server:	Server
WLAN Information:	
- Channel:	7
- WPS Status:	Unconfigured
SSID1 Information:	
- SSID:	ZyXEL_fa34
- Status:	On
- Security Mode:	WPA-PSK
SSID2 Information:	
- SSID:	ZyXEL_fa35
- Status:	Off
- Security Mode:	No Security
SSID3 Information:	
- SSID:	ZyXEL_fa36
- Status:	Off
- Security Mode:	No Security
SSID4 Information:	
- SSID:	ZyXEL_fa37
- Status:	Off
- Security Mode:	No Security

Interface Status

Interface	Status	Rate
ADSL WAN	Down	N/A
LAN 1	Down	N/A
LAN 2	Down	N/A
LAN 3	Down	N/A
LAN 4	Up	100Mbps
WLAN	Up	150Mbps

System Status

System Up Time:	10 min
Current Date/Time:	Sat Jan 1 00:10:00 UTC 2000
System Resource:	
- CPU Usage:	74.3%
- Memory Usage:	97.5%

Registration Status

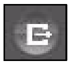
Account	Action	Account Status	URI
SIP 1	Register	Not Registered	ChangeMe@ChangeMe
SIP 2	Register	In-Active	ChangeMe@ChangeMe

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

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

2.2.1 Title Bar

The title bar shows the following icon in the upper right corner.



Click this icon to log out of the web configurator.

2.2.2 Main Window

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

After you click **System Info** on the **Connection Status** screen, the **System Info** screen is displayed. See Chapter 4 on page 63 for more information about the **System Info** screen.

If you click **LAN Device** on the **System Info** screen, the **Connection Status** screen appears. See Chapter 4 on page 61 for more information about the **Connection Status** screen.

If you click **Virtual Device** on the **System Info** screen, a visual graphic appears, showing the connection status of the ZyXEL Device’s ports. The connected ports are in color and disconnected ports are gray.

2.2.3 Navigation Panel

Use the menu items on the navigation panel to open screens to configure ZyXEL Device features. The following table describes each menu item.

Table 2 Navigation Panel Summary

LINK	TAB	FUNCTION
Connection Status		This screen shows the network status of the ZyXEL Device and computers/devices connected to it.
Network Setting		
Broadband	Broadband	Use this screen to configure Internet mode and encapsulation, IP address assignment, DNS servers and other advanced properties.

Table 2 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Wireless	General	Use this screen to turn the wireless connection on or off, specify the SSID(s) and configure the wireless LAN settings and WLAN authentication/security settings.
	More AP	Use this screen to configure multiple BSSs on the ZyXEL Device.
	WPS	Use this screen to use WPS (Wi-Fi Protected Setup) to establish a wireless connection.
	WMM	Use this screen to enable or disable Wi-Fi MultiMedia (WMM).
	Scheduling	Use this screen to configure when the ZyXEL Device enables or disables the wireless LAN.
Home Networking	LAN Setup	Use this screen to configure LAN TCP/IP settings, and other advanced properties.
	Static DHCP	Use this screen to assign specific IP addresses to individual MAC addresses.
	UPnP	Use this screen to enable the UPnP function.
Static Route	Static Route	Use this screen to view and set up static routes on the ZyXEL Device.
DNS Route	DNS Route	Use this screen to view and configure DNS routes.
QoS	General	Use this screen to enable QoS and decide allowable bandwidth using QoS.
	Queue Setup	Use this screen to configure QoS queue assignment.
	Class Setup	Use this screen to set up classifiers to sort traffic into different flows and assign priority and define actions to be performed for a classified traffic flow.
	Monitor	Use this screen to view each queue’s statistics.
NAT	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	Sessions	Use this screen to limit the number of NAT sessions a single client can establish.
Dynamic DNS	Dynamic DNS	Use this screen to allow a static hostname alias for a dynamic IP address.
Security		
Firewall	General	Use this screen to activate/deactivate the firewall.
	Services	Use this screen to set the default action to take on network traffic going in specific directions.
MAC Filter	MAC Filter	Use this screen to allow specific devices to access the ZyXEL Device.
Certificates	Local Certificates	Use this screen to generate and export self-signed certificates or certification requests and import the ZyXEL Device’s CA-signed certificates.
	Trusted CA	Use this screen to save CA certificates to the ZyXEL Device.
VoIP		

Table 2 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
SIP	SIP Service Provider	Use this screen to configure your ZyXEL Device's Voice over IP settings.
	SIP Account	Use this screen to set up information about your SIP account and configure audio settings such as volume levels for the phones connected to the ZyXEL Device.
	Common	Use this screen to configure RFC3262 support and bind interfaces on the ZyXEL Device.
Phone	Phone Device	Use this screen to set which phone ports use which SIP accounts.
	Region	Use this screen to select your location.
Call Rule	Call Rule	Use this screen to configure speed dial for SIP phone numbers that you call often.
FXO	FXO	Use this screen to set up the PSTN line you use to make regular phone calls.
System Monitor		
Log	Phone Log	Use this screen to view the ZyXEL Device's phone logs.
	VoIP Call History	Use this screen to view the ZyXEL Device's VoIP call history.
Traffic Status	WAN	Use this screen to view the status of all network traffic going through the WAN port of the ZyXEL Device.
	LAN	Use this screen to view the status of all network traffic going through the LAN ports of the ZyXEL Device.
	NAT	Use this screen to view the status of NAT sessions on the ZyXEL Device.
VoIP Status	VoIP Status	Use this screen to view the SIP, phone, and call status of the ZyXEL Device.
Maintenance		
Users Account	Users Account	Use this screen to configure the passwords your user accounts.
Remote MGMT	Remote MGMT	Use this screen to enable specific traffic directions for network services.
SNMP	SNMP	Use this screen to configure through which interface(s) and from which IP address(es) users can access the SNMP agent on the ZyXEL Device.
System	System	Use this screen to configure the ZyXEL Device's name, domain name, management inactivity time-out.
Time Setting	Time Setting	Use this screen to change your ZyXEL Device's time and date.
Log Setting	Log Setting	Use this screen to select which logs and/or immediate alerts your device is to record.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your device.

Table 2 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Backup/ Restore	Backup/ Restore	Use this screen to backup and restore your device’s configuration (settings) or reset the factory default settings.
Reboot	Reboot	Use this screen to reboot the ZyXEL Device without turning the power off.
Diagnostic	Ping	Use this screen to test the connections to other devices.
	DSL Line	Use this screen to identify problems with the DSL connection.

2.2.4 Status Bar

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

3

Tutorials

3.1 Overview

This chapter contains the following tutorials:

- Setting Up Your DSL Connection
- How to Set up a Wireless Network
- Setting Up NAT Port Forwarding
- How to Make a VoIP Call
- Configuring the MAC Address Filter
- Configuring Static Route for Routing to Another Network
- Configuring QoS Queue and Class Setup
- Access the ZyXEL Device Using DDNS

3.2 Setting Up Your DSL Connection

This tutorial shows you how to set up your Internet connection using the web configurator.

If you connect to the Internet through a DSL connection, use the information from your Internet Service Provider (ISP) to configure the ZyXEL Device. Do the following steps:

1. Connect the ZyXEL Device properly. Refer to the Quick Start Guide for details on the ZyXEL Device's hardware connection.

2. Check the back panel of your device where the Ethernet ports are located and make sure the **DSL/WAN** switch is pointing up to **DSL**.

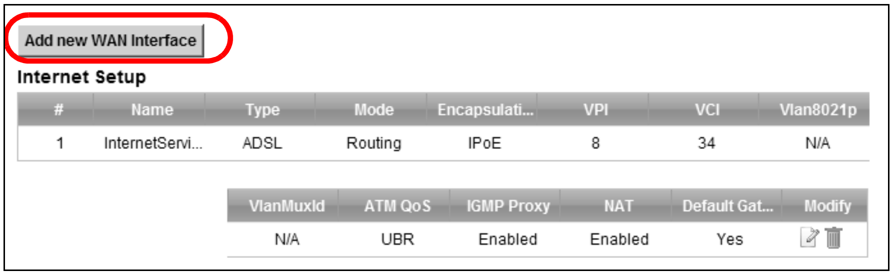
3. Connect one end of a DSL cable to the DSL port of your ZyXEL Device. The other end should be connected to the DSL port in your house or a DSL router/modem provided by your ISP.

4 Connect one end of Ethernet cable to an Ethernet port on the ZyXEL Device and the other end to a computer that you will use to access the web configurator.

5 Connect the ZyXEL Device to a power source, turn it on and wait for the **POWER** LED to become a steady green. Turn on the modem provided by your ISP as well as the computer.

Account Configuration

1 Click **Network Setting > Broadband** to open the following screen. Click **Add new WAN Interface**.



Internet Setup

#	Name	Type	Mode	Encapsulati...	VPI	VCI	Vlan8021p
1	InternetServi...	ADSL	Routing	IPoE	8	34	N/A

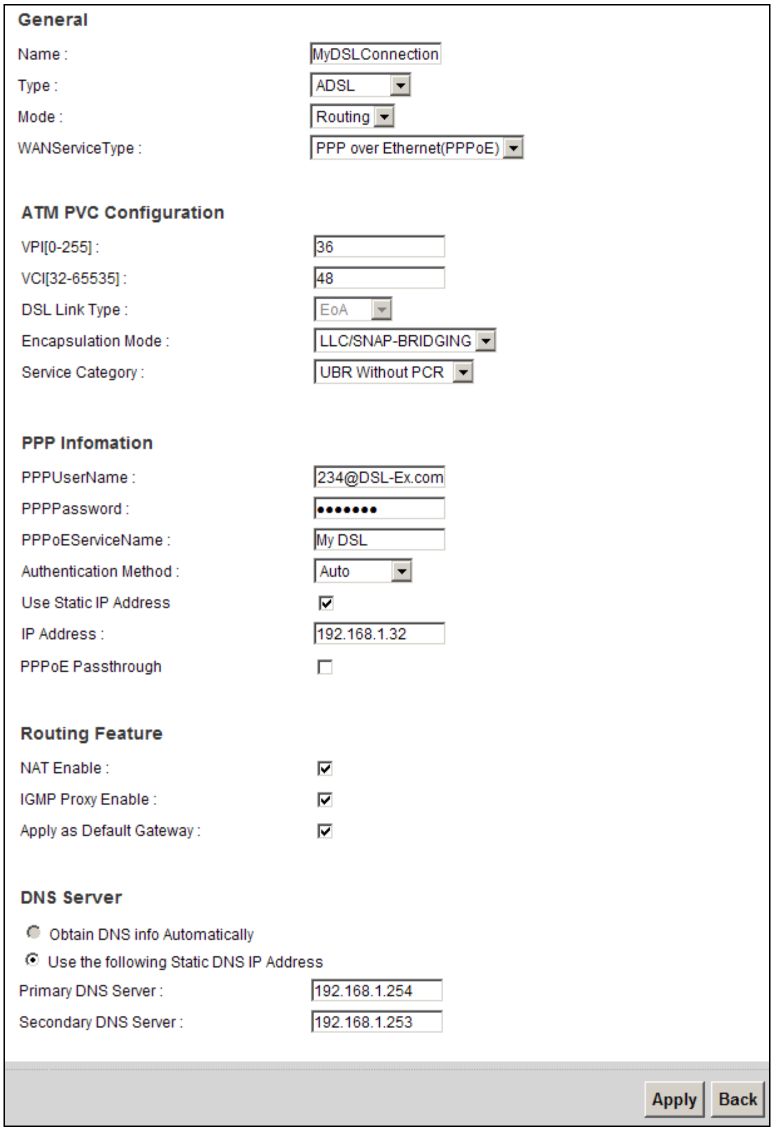
VlanMuxId	ATM QoS	IGMP Proxy	NAT	Default Gat...	Modify
N/A	UBR	Enabled	Enabled	Yes	✎🗑

2 For this example, the interface type is ADSL and the connection has the following information.

General	
Name	MyDSLConnection
Type	ADSL
Mode	Routing
WAN Service Type	PPPoE
ATM PVC Configuration	
VPI/VCI	36/48
Encapsulation Mode	LLC/SNAP-Bridging
Service Category	UBR without PCR
PPP Information	
PPP User Name	1234@DSL-Ex.com
PPP Password	ABCDEF!
PPPoE Service Name	My DSL
Authentication Method	Auto

Static IP Address	192.168.1.32
Others	PPPoE Passthrough: Disabled NAT: Enabled IGMP Multicast Proxy: Enabled Apply as Default Gateway: Enable DNS Server: Static DNS IP Address (Primary: 192.168.1.254 Secondary: 192.168.1.253)

Enter or select these values and click **Apply**.



General

Name :	MyDSLConnection
Type :	ADSL
Mode :	Routing
WANServiceType :	PPP over Ethernet(PPPoE)

ATM PVC Configuration

VPI[0-255] :	36
VCI[32-65535] :	48
DSL Link Type :	EoA
Encapsulation Mode :	LLC/SNAP-BRIDGING
Service Category :	UBR Without PCR

PPP Infomation

PPPUserName :	234@DSL-Ex.com
PPPPassword :	•••••••
PPPoEServiceName :	My DSL
Authentication Method :	Auto
Use Static IP Address	☑
IP Address :	192.168.1.32
PPPoE Passthrough	□

Routing Feature

NAT Enable :	☑
IGMP Proxy Enable :	☑
Apply as Default Gateway :	☑

DNS Server

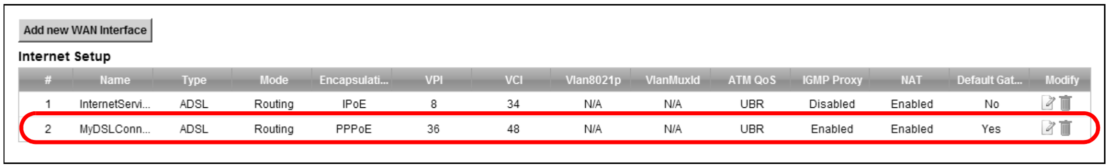
○ Obtain DNS info Automatically

● Use the following Static DNS IP Address

Primary DNS Server :	192.168.1.254
Secondary DNS Server :	192.168.1.253

This completes your DSL WAN connection setting.

3 You should see a summary of your new DSL connection setup in the **Broadband** screen as follows.



Internet Setup

#	Name	Type	Mode	Encapsulati...	VPI	VCI	Vlan8021p	VlanMuxId	ATM QoS	IGMP Proxy	NAT	Default Gat...	Modify
1	InternetServi...	ADSL	Routing	IPoE	8	34	N/A	N/A	UBR	Disabled	Enabled	No	✎ 🗑
2	MyDSLConn...	ADSL	Routing	PPPoE	36	48	N/A	N/A	UBR	Enabled	Enabled	Yes	✎ 🗑

Try to connect to a website, such as “www. zyxel.com” to see if you have correctly set up your Internet connection. Be sure to contact your service provider for any information you need to configure the WAN screens.

3.3 How to Set up a Wireless Network

This section 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 the ZyXEL Device wirelessly.

3.3.1 Example Parameters

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

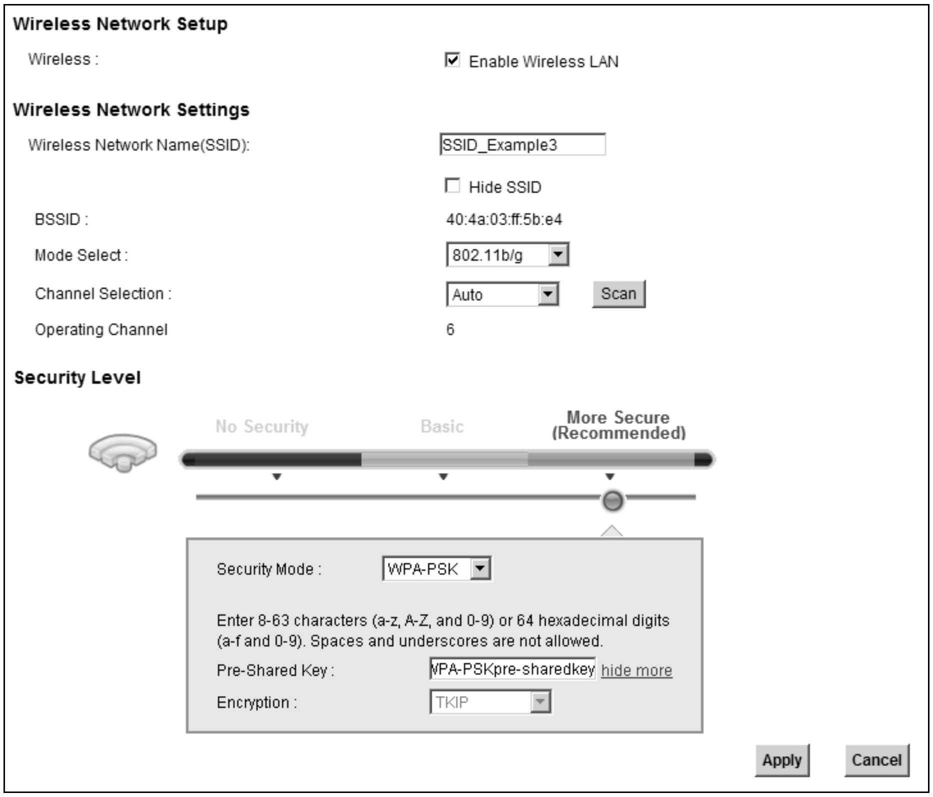
An access point (AP) or wireless router is referred to as the “AP” and a computer with a wireless network card or USB adapter is referred to as the “wireless client” here.

We use the [Model #] web screens and M-302 utility screens as an example. The screens may vary slightly for different models.

3.3.2 Configuring the AP

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

1 Open the **Network Setting > Wireless > General** screen in the AP's web configurator.



Wireless Network Setup

Wireless : ☑ Enable Wireless LAN

Wireless Network Settings

Wireless Network Name(SSID): SSID_Example3

□ Hide SSID

BSSID : 40:4a:03:ff:5b:e4

Mode Select : 802.11b/g

Channel Selection : Auto

Operating Channel 6

Security Level

Security Mode : WPA-PSK

Enter 8-63 characters (a-z, A-Z, and 0-9) or 64 hexadecimal digits (a-f and 0-9). Spaces and underscores are not allowed.

Pre-Shared Key : WPA-PSKpre-sharedkey

Encryption : TKIP

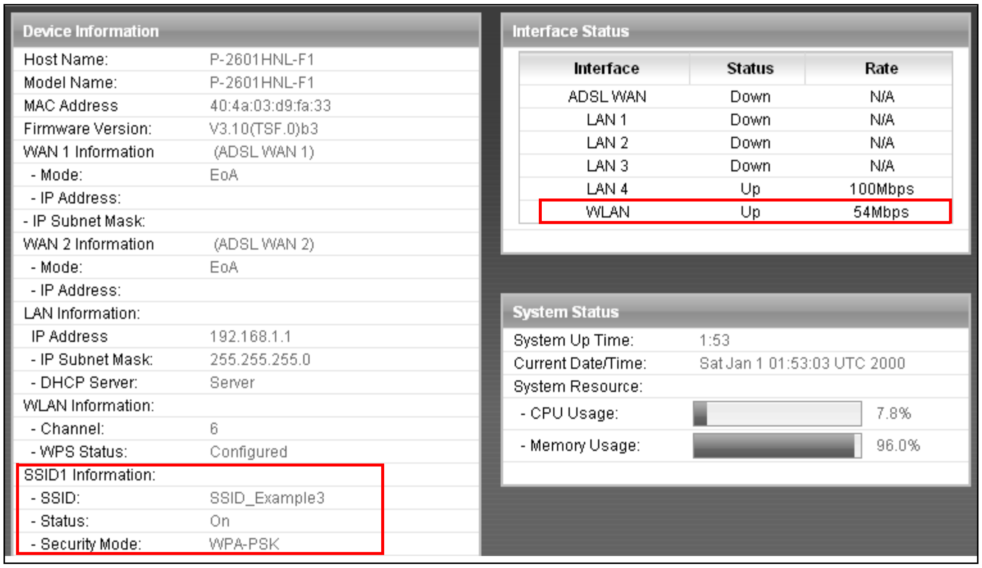
2 Make sure **Enable Wireless LAN** is selected.

3 Enter "SSID_Example3" as the SSID and select **Auto** in the **Channel Selection** field to have the device search for an available channel.

4 Select **802.11b/g** in the **Mode Select** field.

5 Select **More Secure** as your security level and set security mode to **WPA-PSK** and enter "ThisismyWPA-PSKpre-sharedkey" in the **Pre-Shared Key** field. Click **Apply**.

6 Click **Connection Status > System Info**.Verify your wireless and wireless security settings under **Device Information** and check if the WLAN connection is up under **Interface Status**.



Device Information

Host Name:	P-2601HNL-F1
Model Name:	P-2601HNL-F1
MAC Address	40:4a:03:d9:fa:33
Firmware Version:	V3.10(TSF.0)b3
WAN 1 Information	(ADSL WAN 1)
- Mode:	EoA
- IP Address:	
- IP Subnet Mask:	
WAN 2 Information	(ADSL WAN 2)
- Mode:	EoA
- IP Address:	
LAN Information:	
IP Address	192.168.1.1
- IP Subnet Mask:	255.255.255.0
- DHCP Server:	Server
WLAN Information:	
- Channel:	6
- WPS Status:	Configured
SSID1 Information:	
- SSID:	SSID_Example3
- Status:	On
- Security Mode:	WPA-PSK

Interface Status

Interface	Status	Rate
ADSL WAN	Down	N/A
LAN 1	Down	N/A
LAN 2	Down	N/A
LAN 3	Down	N/A
LAN 4	Up	100Mbps
WLAN	Up	54Mbps

System Status

System Up Time:	1:53
Current Date/Time:	Sat Jan 1 01:53:03 UTC 2000
System Resource:	
- CPU Usage:	7.8%
- Memory Usage:	96.0%

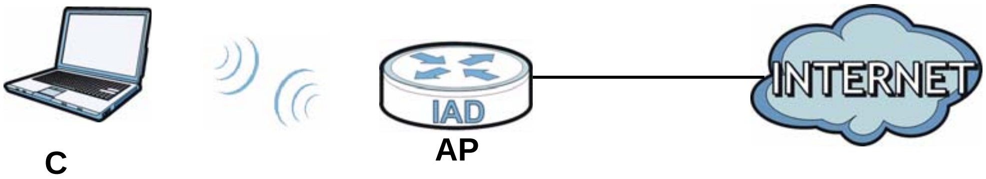
This finishes the configuration of the AP.

3.3.3 Configuring the Wireless Client

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

3.3.3.1 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**.



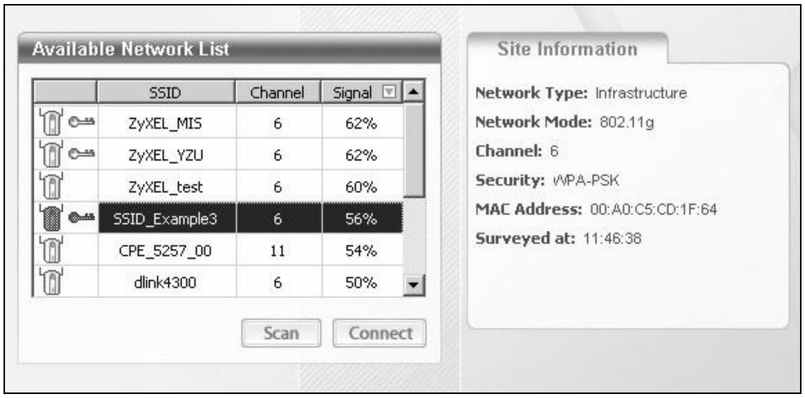
There are three ways to connect the client to an access point.

- 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.



Available Network List

	SSID	Channel	Signal
	ZyXEL_MIS	6	62%
	ZyXEL_YZU	6	62%
	ZyXEL_test	6	60%
	SSID_Example3	6	56%
	CPE_5257_00	11	54%
	dlink4300	6	50%

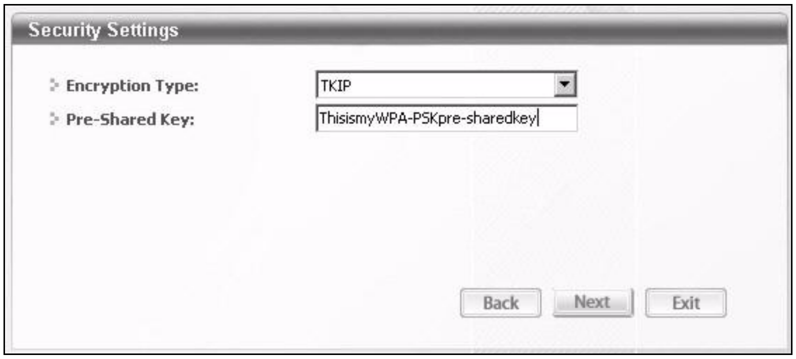
Site Information

Network Type: Infrastructure
Network Mode: 802.11g
Channel: 6
Security: WPA-PSK
MAC Address: 00:A0:C5:CD:1F:64
Surveyed at: 11:46:38

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.

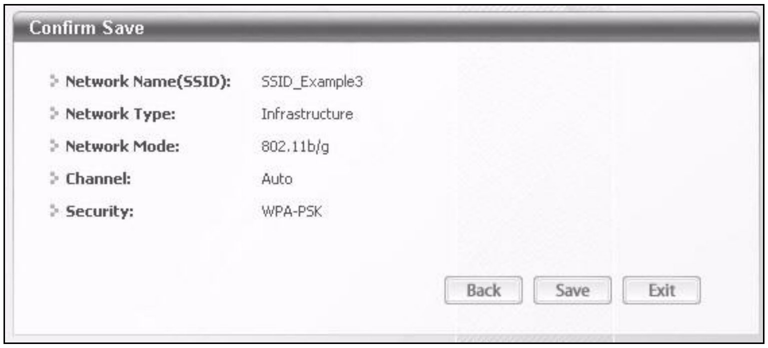
Use the **Next** button to move on to the next screen. You can use the **Back** button at any time to return to the previous screen, or the **Exit** button to return to the **Site Survey** screen.



Security Settings

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

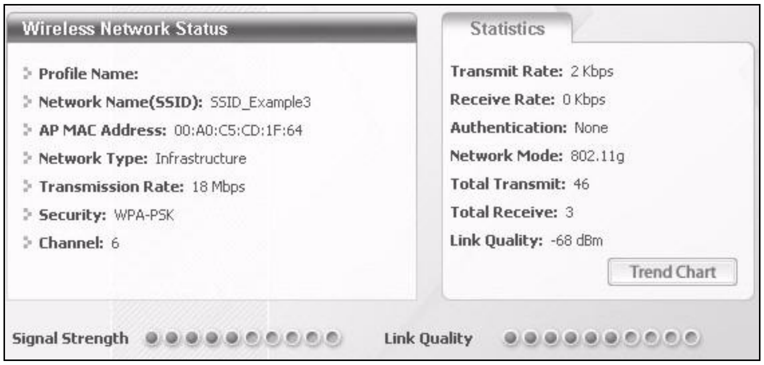
4 The **Confirm Save** window appears. Check your settings and click **Save** to continue.



Confirm Save

- 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.



Wireless Network Status

- Profile Name:
- Network Name(SSID): SSID_Example3
- AP MAC Address: 00:A0:C5:CD:1F:64
- Network Type: Infrastructure
- Transmission Rate: 18 Mbps
- Security: WPA-PSK
- Channel: 6

Statistics

Transmit Rate: 2 Kbps
Receive Rate: 0 Kbps
Authentication: None
Network Mode: 802.11g
Total Transmit: 46
Total Receive: 3
Link Quality: -68 dBm

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.

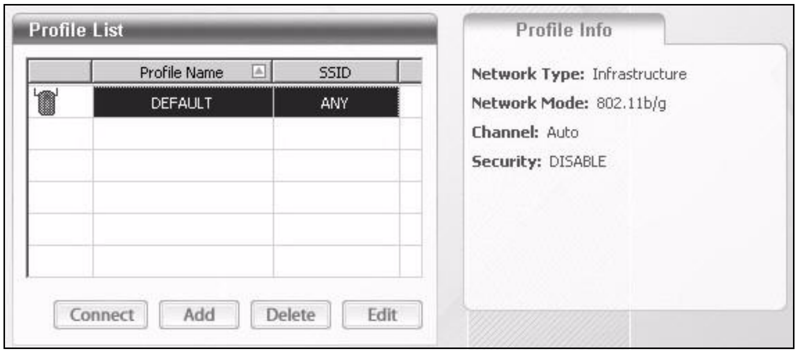
3.3.3.2 Creating and Using a Profile

A profile lets you easily connect to the same wireless network again later. 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 AP 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".

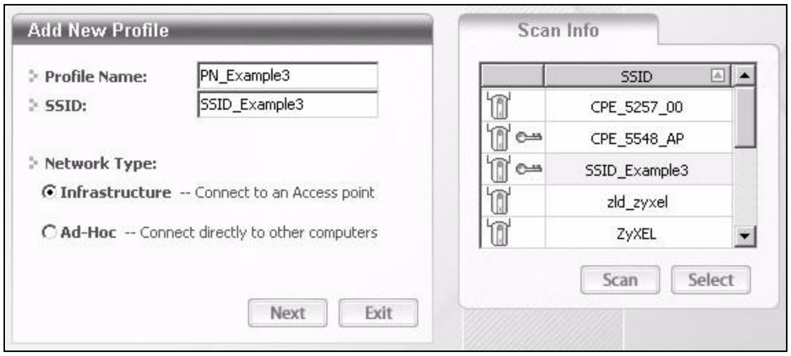
1 Open the ZyXEL utility and click the **Profile** tab to open the screen shown next. Click **Add** to configure a new profile.



Profile Name	SSID
DEFAULT	ANY

Network Type: Infrastructure
Network Mode: 802.11b/g
Channel: Auto
Security: DISABLE

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



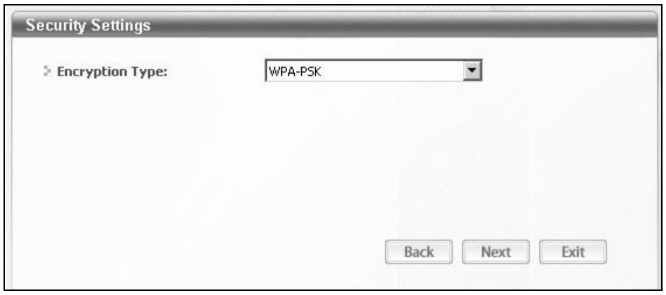
Profile Name: PN_Example3
SSID: SSID_Example3

Network Type:
● Infrastructure -- Connect to an Access point
○ Ad-Hoc -- Connect directly to other computers

SSID
CPE_5257_00
CPE_5548_AP
SSID_Example3
zld_zyxel
ZyXEL

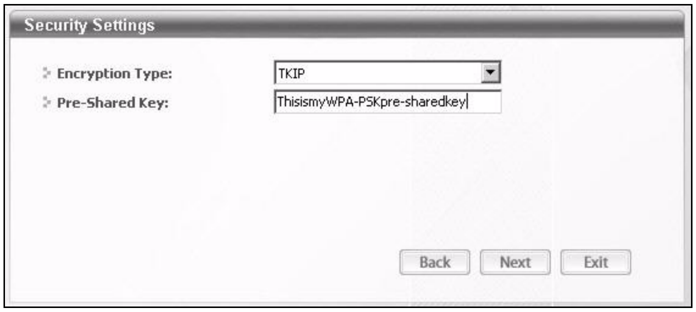
3 Give the profile a descriptive name (of up to 32 printable ASCII characters). Select **Infrastructure** and either manually enter or select the AP's SSID in the **Scan Info** table and click **Select**.

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



Encryption Type: WPA-PSK

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.

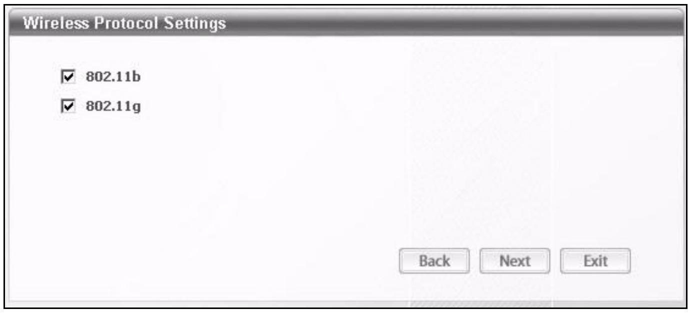


Security Settings

Encryption Type: TKIP

Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey

6 In the next screen, leave both boxes selected.

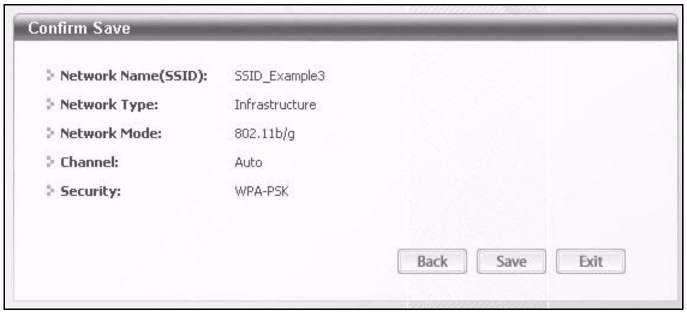


Wireless Protocol Settings

☑ 802.11b

☑ 802.11g

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



Confirm Save

Network Name(SSID): SSID_Example3

Network Type: Infrastructure

Network Mode: 802.11b/g

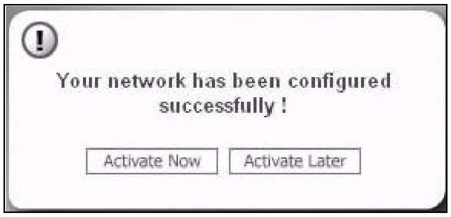
Channel: Auto

Security: WPA-PSK

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.


Your network has been configured successfully !

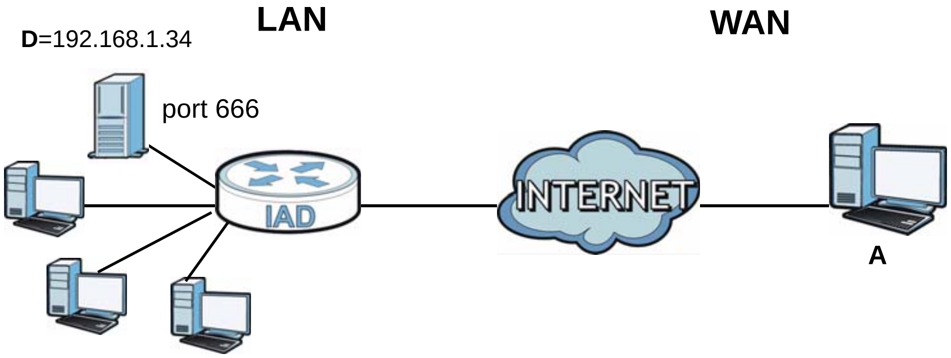
9 When you activate the new profile, the ZyXEL utility returns to the **Link Info** screen while it connects to the AP using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection.

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.

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.

3.4 Setting Up NAT Port Forwarding

In this tutorial, you manage the Doom server on a computer behind the ZyXEL Device. In order for players on the Internet (like **A** in the figure below) to communicate with the Doom server, you need to configure the port settings and IP address on the ZyXEL Device. Traffic should be forwarded to the port 666 of the Doom server computer which has an IP address of 192.168.1.34.

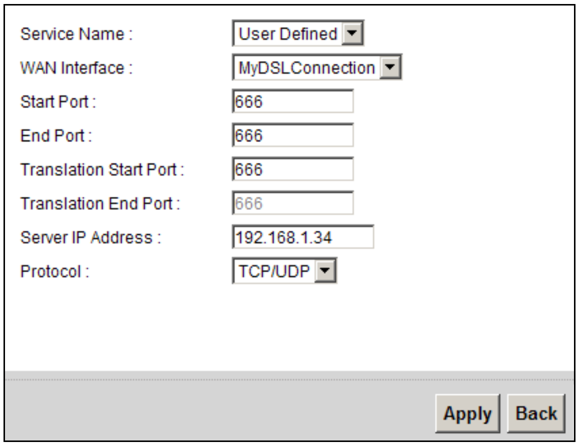


You may set up the port settings by configuring the port settings for the Doom server computer (see Chapter 11 on page 150 for more information).

1 Click **Network Setting** > **NAT** > **Port Forwarding**. Click **Add new rule**.

2 Enter the following values:

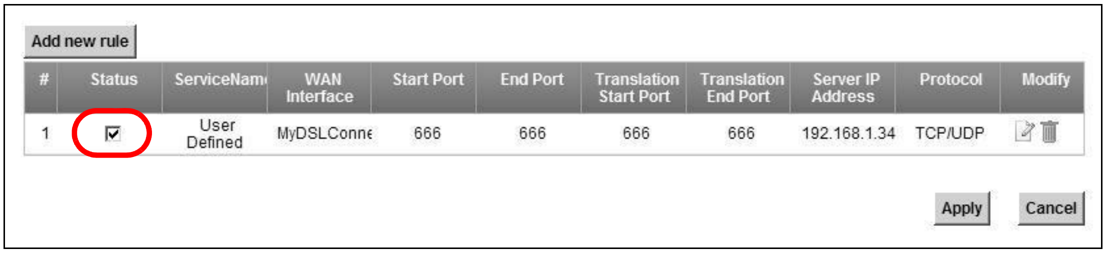
Service Name	Select **User Defined**.
WAN Interface	Select the WAN interface through which the Doom service is forwarded. This is the default interface for this example, which is **MyDSLConnection**.
Start/End Ports	**666**
Translation Start/End Ports	**666**
Server IP Address	Enter the IP address of the Doom server. This is **192.168.1.34** for this example.
Protocol	Select **TCP/UDP**. This should be the protocol supported by the Doom server.



Service Name :	User Defined
WAN Interface :	MyDSLConnection
Start Port :	666
End Port :	666
Translation Start Port :	666
Translation End Port :	666
Server IP Address :	192.168.1.34
Protocol :	TCP/UDP

3 Click **Apply**.

4 The port forwarding settings you configured should appear in the table. Make sure the **Status** check box for this rule is selected. Click **Apply** to have the ZyXEL Device start forwarding port 666 traffic to the computer with IP address 192.168.1.34.



#	Status	ServiceNam	WAN Interface	Start Port	End Port	Translation Start Port	Translation End Port	Server IP Address	Protocol	Modify
1	☑	User Defined	MyDSLConne	666	666	666	666	192.168.1.34	TCP/UDP	

Players on the Internet then can have access to your Doom server.

3.5 How to Make a VoIP Call

You can register a SIP account with the SIP server and make voice calls over the Internet to another VoIP device.

The following parameters are used in this example:

SIP Service Provider Name	ServiceProvider1
SIP Account Number	12345678
Username	ChangeMe
Password	ThisIsMySIP

3.5.1 VoIP Calls With a Registered SIP Account

To use a registered SIP account, you should configure the SIP service provider and applied for a SIP account.

3.5.1.1 SIP Service Provider Configuration

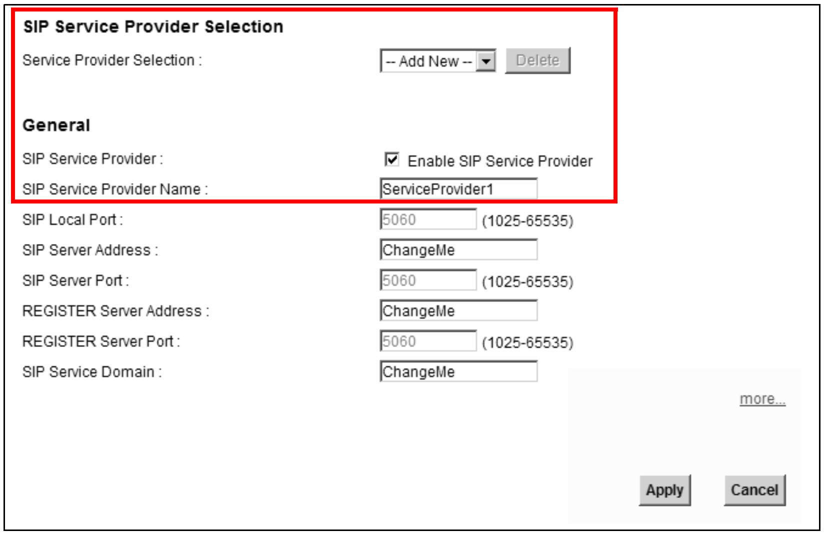
Follow the steps below to configure your SIP service provider.

1 Make sure your ZyXEL Device is connected to the Internet.

2 Open the web configurator.

3 Click **VoIP > SIP** to open the **SIP Service Provider** screen. Select **Add New** from the **Service Provider Selection** drop-down list box.

4 Select the **Enable** check box of **SIP Service Provider** and enter the **SIP Service Provider Name**.



SIP Service Provider Selection

Service Provider Selection : -- Add New -- Delete

General

SIP Service Provider : ☑ Enable SIP Service Provider

SIP Service Provider Name : ServiceProvider1

SIP Local Port : 5060 (1025-65535)

SIP Server Address : ChangeMe

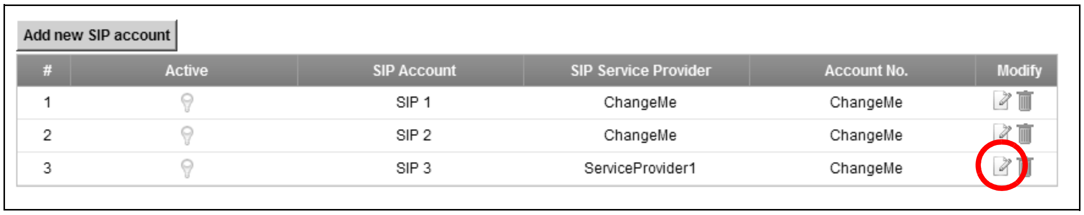
SIP Server Port : 5060 (1025-65535)

REGISTER Server Address : ChangeMe

REGISTER Server Port : 5060 (1025-65535)

SIP Service Domain : ChangeMe

5 Go to the **SIP Account** screen, click the **Edit** icon of **SIP 3**.

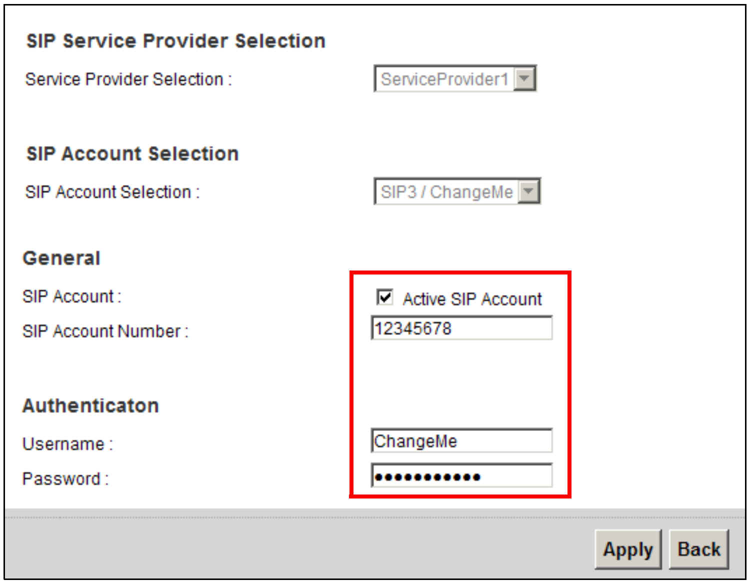


Add new SIP account

#	Active	SIP Account	SIP Service Provider	Account No.	Modify
1		SIP 1	ChangeMe	ChangeMe	
2		SIP 2	ChangeMe	ChangeMe	
3		SIP 3	ServiceProvider1	ChangeMe	

6 Select the **Active SIP Account** check box, then enter the **SIP Account Number**, **Username**, and **Password**. Leave other settings as default.

7 Click **Apply** to save your settings.



SIP Service Provider Selection

Service Provider Selection : ServiceProvider1

SIP Account Selection

SIP Account Selection : SIP3 / ChangeMe

General

SIP Account : ☑ Active SIP Account

SIP Account Number : 12345678

Authenticaton

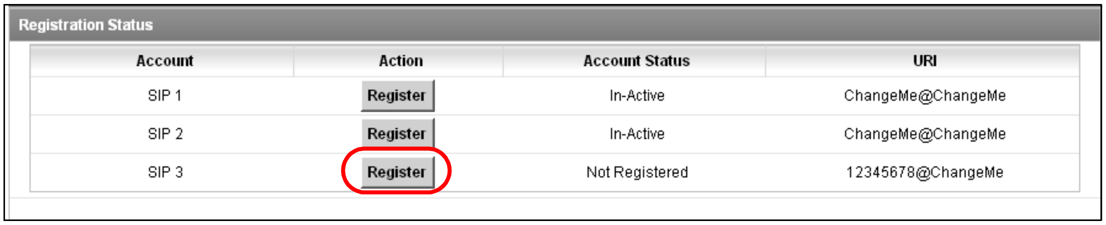
Username : ChangeMe

Password : ●●●●●●●●●●●

3.5.1.2 SIP Account Registration

Follow the steps below to register and activate your SIP account.

1 Click **Connection Status > System Info** to check if your SIP account has been registered successfully. If the status is **Not Registered**, check your Internet connection and click **Register** to register your SIP account.

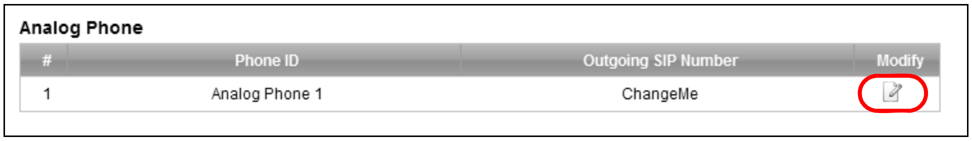


Registration Status

Account	Action	Account Status	URI
SIP 1	Register	In-Active	ChangeMe@ChangeMe
SIP 2	Register	In-Active	ChangeMe@ChangeMe
SIP 3	Register	Not Registered	12345678@ChangeMe

3.5.1.3 Analog Phone Configuration

1 Click **VoIP > Phone** to open the **Phone Device** screen. Click the **Edit** icon next to **Analog Phone 1** to configure the first phone port.



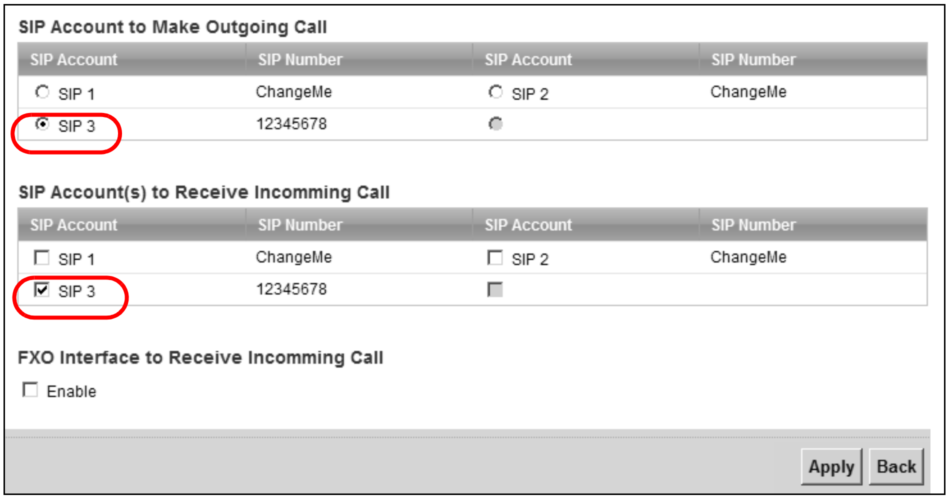
Analog Phone

#	Phone ID	Outgoing SIP Number	Modify
1	Analog Phone 1	ChangeMe	📝

2 Select **SIP 3** from the **SIP Account** in the **SIP Account to Make Outgoing Call** section to have the phone (connected to the first phone port) use the registered SIP 3 account to make outgoing calls.

3 Select the **SIP 3** check box in the **SIP Account(s) to Receive Incoming Call** section to have the phone (connected to the first phone port) receive phone calls for the SIP 3 account.

4 Click **Apply** to save your changes.



SIP Account to Make Outgoing Call

SIP Account	SIP Number	SIP Account	SIP Number
○ SIP 1	ChangeMe	○ SIP 2	ChangeMe
● SIP 3	12345678	○	

SIP Account(s) to Receive Incomming Call

SIP Account	SIP Number	SIP Account	SIP Number
□ SIP 1	ChangeMe	□ SIP 2	ChangeMe
☑ SIP 3	12345678	□	

FXO Interface to Receive Incomming Call

□ Enable

3.5.1.4 Making a VoIP Call

1 Make sure you connect a telephone to the first phone port on the ZyXEL Device.

2 Make sure the ZyXEL Device is on and connected to the Internet.

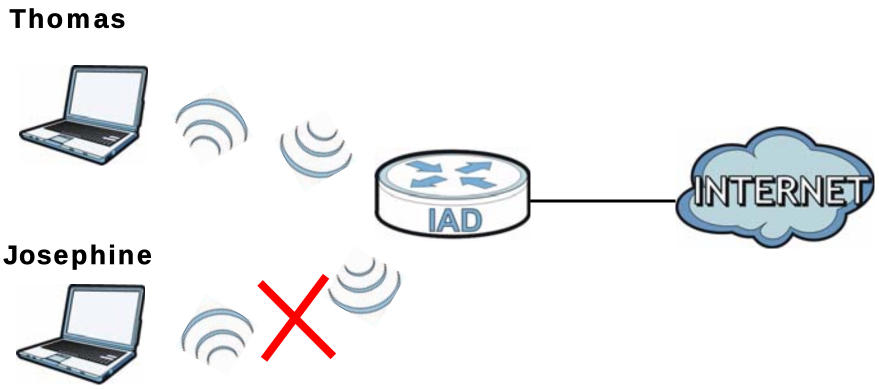
3 Pick up the phone receiver.

4 Dial the VoIP phone number you want to call.

3.6 Configuring the MAC Address Filter

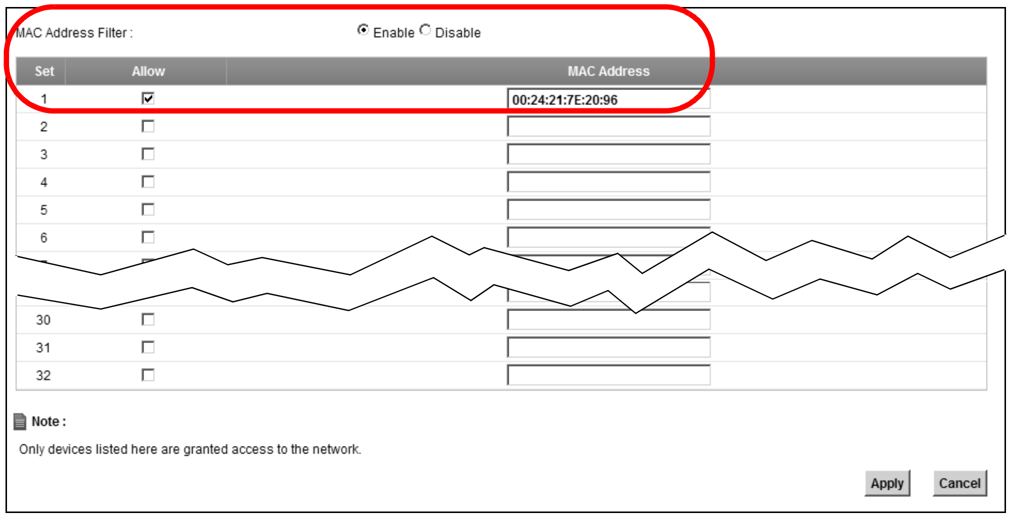
Thomas noticed that his daughter Josephine spends too much time surfing the web and downloading media files. He decided to prevent Josephine from accessing the Internet so that she can concentrate on preparing for her final exams.

Josephine's computer connects wirelessly to the Internet through the ZyXEL Device. Thomas decides to use the **Security > MAC Filter** screen to grant wireless network access to his computer but not to Josephine's computer.



1 Click **Security** > **MAC Filter** to open the **MAC Filter** screen. Select the **Enable** check box to activate MAC filter function.

2 Find the MAC address of Thomas' computer in this screen. Select **Allow**. Click **Apply**.



MAC Address Filter : ● Enable ○ Disable

Set	Allow	MAC Address
1	☑	00:24:21:7E:20:96
2	□	
3	□	
4	□	
5	□	
6	□	
30	□	
31	□	
32	□	

Note :

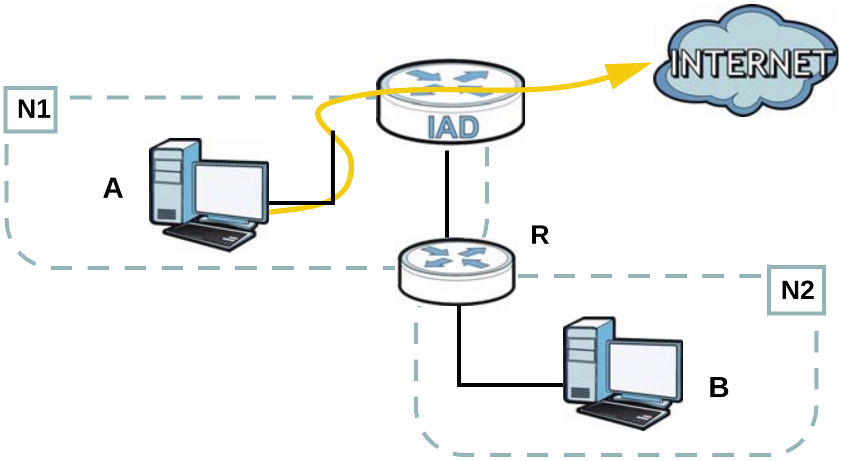
Only devices listed here are granted access to the network.

Thomas can also grant access to the computers of other members of his family and friends. However, Josephine and others not listed in this screen will no longer be able to access the Internet through the ZyXEL Device.

3.7 Configuring Static Route for Routing to Another Network

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

In the following figure, router **R** is connected to the ZyXEL Device's LAN. **R** connects to two networks, **N1** (192.168.1.x/24) and **N2** (192.168.10.x/24). If you want to send traffic from computer **A** (in **N1** network) to computer **B** (in **N2** network), the traffic is sent to the ZyXEL Device's WAN default gateway by default. In this case, **B** will never receive the traffic.



You need to specify a static routing rule on the ZyXEL Device to specify **R** as the router in charge of forwarding traffic to **N2**. In this case, the ZyXEL Device routes traffic from **A** to **R** and then **R** routes the traffic to **B**.This tutorial uses the following example IP settings:

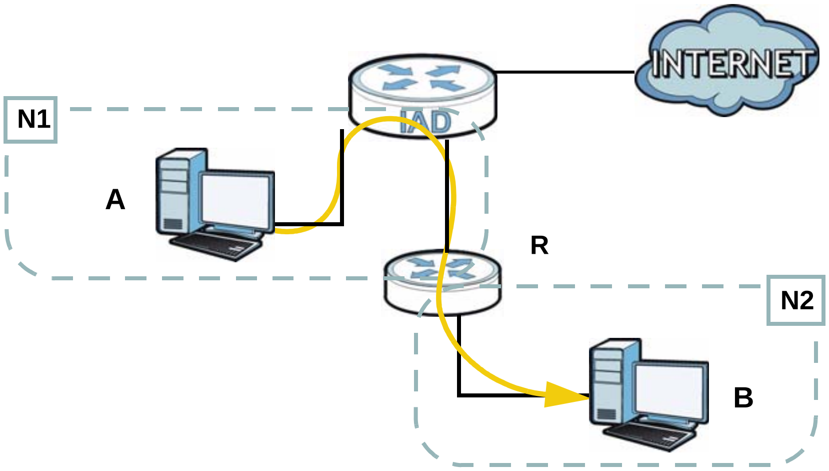
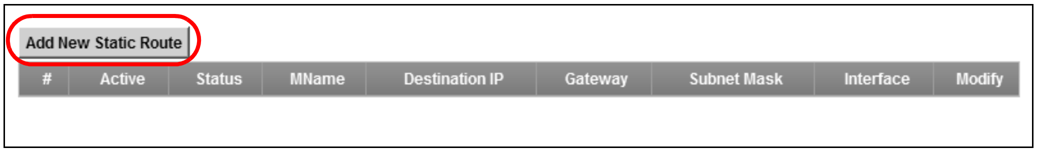


Table 3 IP Settings in this Tutorial

DEVICE / COMPUTER	IP ADDRESS
The ZyXEL Device's WAN	172.16.1.1
The ZyXEL Device's LAN	192.168.1.1
A	192.168.1.34
R's N1	192.168.1.253
R's N2	192.168.10.2
B	192.168.10.33

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

1 Click **Network Setting > Routing**. Click **Add New Static Route**.

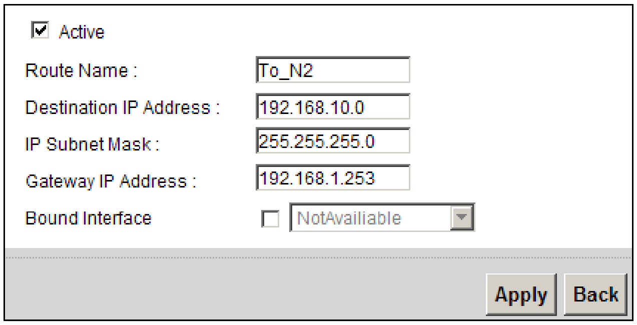


#	Active	Status	MName	Destination IP	Gateway	Subnet Mask	Interface	Modify

2 Configure the **Static Route Setup** screen using the following settings:

- Select **Active**.
- Specify a descriptive name for this routing rule.
- Type **192.168.10.0** and subnet mask **255.255.255.0** for the destination, **N2**.

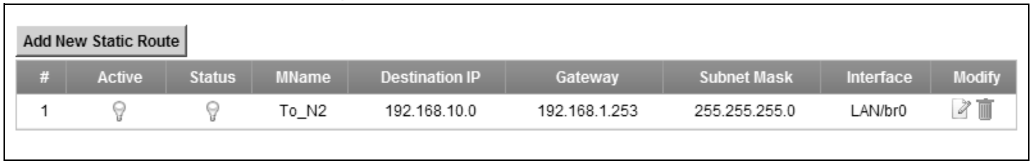
- Type **192.168.1.253** (**R**’s N1 address) in the **Gateway IP Address** field.



☑ Active

Route Name :	To_N2
Destination IP Address :	192.168.10.0
IP Subnet Mask :	255.255.255.0
Gateway IP Address :	192.168.1.253
Bound Interface	□ NotAvailiable

Click **Apply**. The **Routing** screen should display the route you just added.



#	Active	Status	MName	Destination IP	Gateway	Subnet Mask	Interface	Modify
1			To_N2	192.168.10.0	192.168.1.253	255.255.255.0	LAN/br0	

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

3.8 Configuring QoS Queue and Class Setup

This section contains tutorials on how you can configure the QoS screen.

Note: Voice traffic will not be affected by the user-defined QoS settings on the ZyXEL Device. It always gets the highest priority.

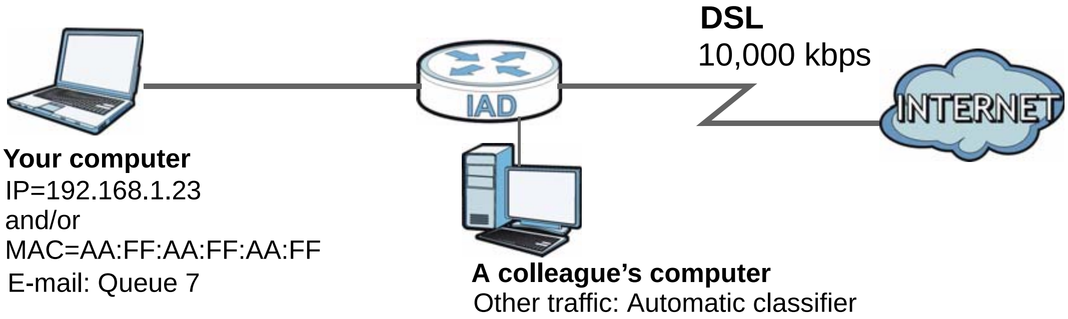
Let’s say you are a team leader of a small sales branch office. You want to prioritize e-mail traffic because your task includes sending urgent updates to clients at least twice every hour. You also upload data files (such as logs and e-mail archives) to the FTP server throughout the day. Your colleagues use the Internet for research, as well as chat applications for communicating with other branch offices.

In the following figure, your Internet connection has an upstream transmission bandwidth of 10,000 kbps. For this example, you want to configure QoS so that e-mail traffic gets the highest priority with at least 5,000 kbps. You can do the following:

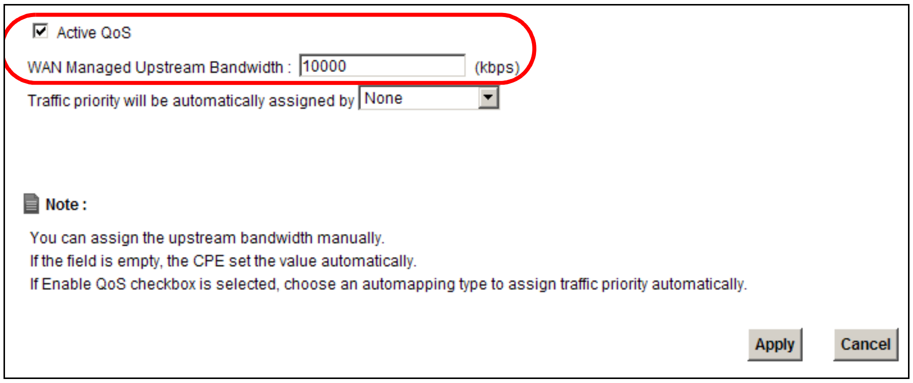
- Configure a queue to assign the highest priority queue (7) to e-mail traffic from the LAN interface, so that e-mail traffic would not get delayed when there is network congestion.
- Note the IP address (192.168.1.23 for example) and/or MAC address (AA:FF:AA:FF:AA:FF for example) of your computer and map it to queue 7.

Note: QoS is applied to traffic flowing out of the ZyXEL Device.

Traffic that does not match this class is assigned a priority queue based on the internal QoS mapping table on the ZyXEL Device.



1 Click **Network Setting > QoS > General** and check **Active**. Set your **WAN Managed Upstream Bandwidth** to 10,000 kbps (or leave this blank to have the ZyXEL Device automatically determine this figure). Click **Apply** to save your settings.



☑ Active QoS

WAN Managed Upstream Bandwidth : 10000 (kbps)

Traffic priority will be automatically assigned by None

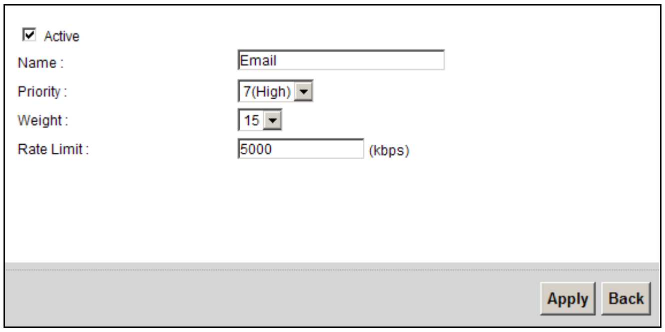
Note :

You can assign the upstream bandwidth manually.
If the field is empty, the CPE set the value automatically.
If Enable QoS checkbox is selected, choose an automapping type to assign traffic priority automatically.

2 Go to **Network Setting > QoS > Queue Setup**. Click **Add new Queue** to create a new queue. In the screen that opens, check **Active** and enter or select the following values, then click **Apply**.

- **Name**: Email
- **Priority**: 7 (High)
- **Weight**: 15

- **Rate Limit**: 5,000 (kbps)



☑ Active

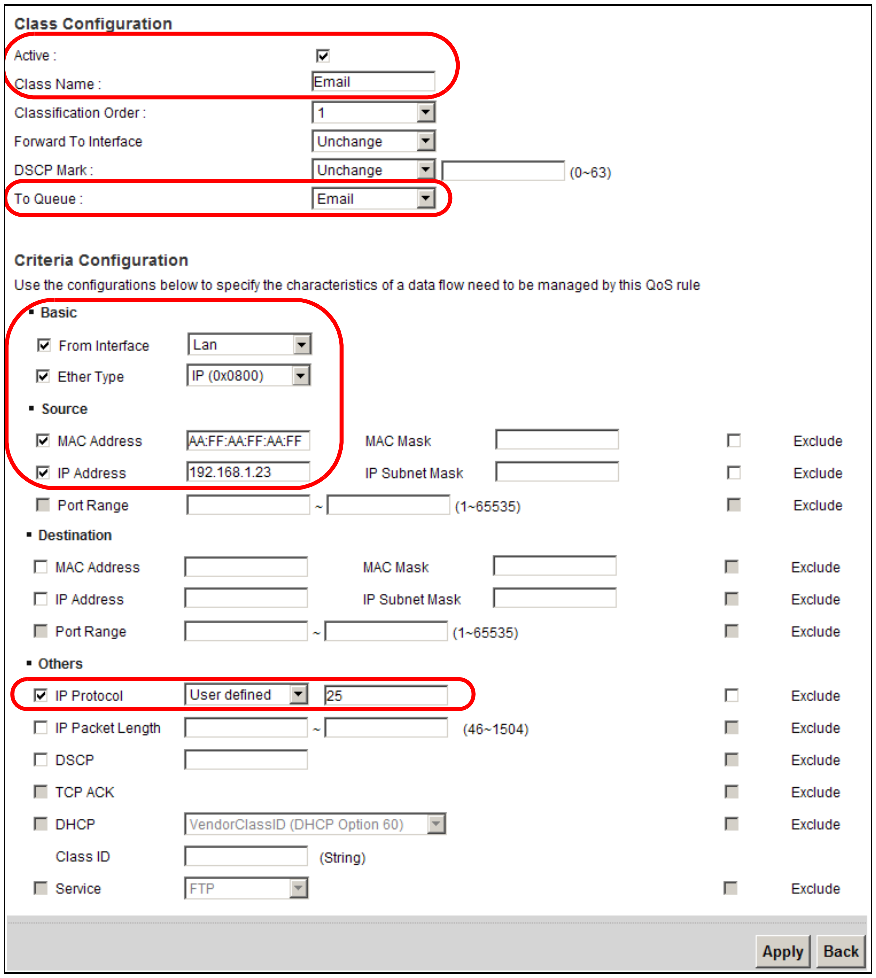
Name : Email

Priority : 7(High)

Weight : 15

Rate Limit : 5000 (kbps)

3 Go to **Network Setting > QoS > Class Setup**. Click **Add new Classifier** to create a new class. Check **Active** and follow the settings as shown in the screen below. Then click **Apply**.



Class Configuration

Active : ☑

Class Name : Email

Classification Order : 1

Forward To Interface : Unchange

DSCP Mark : Unchange (0~63)

To Queue : Email

Criteria Configuration

Use the configurations below to specify the characteristics of a data flow need to be managed by this QoS rule

- Basic

☑ From Interface: Lan

☑ Ether Type: IP (0x0800)

- Source

☑ MAC Address: AA:FF:AA:FF:AA:FF MAC Mask □ Exclude

☑ IP Address: 192.168.1.23 IP Subnet Mask □ Exclude

□ Port Range ~ (1~65535) □ Exclude

- Destination

□ MAC Address MAC Mask □ Exclude

□ IP Address IP Subnet Mask □ Exclude

□ Port Range ~ (1~65535) □ Exclude

- Others

☑ IP Protocol: User defined 25 □ Exclude

□ IP Packet Length ~ (46~1504) □ Exclude

□ DSCP □ Exclude

□ TCP ACK □ Exclude

□ DHCP VendorClassID (DHCP Option 60) □ Exclude

Class ID (String)

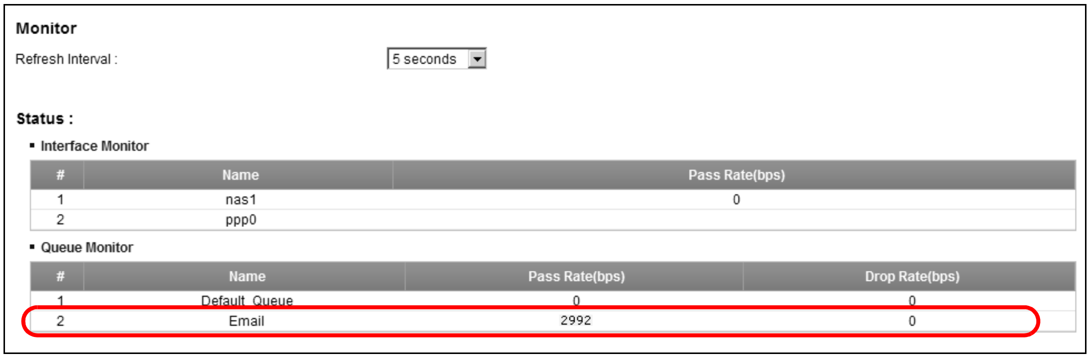
□ Service FTP □ Exclude

Class Name	Give a class name to this traffic, such as **Email** in this example.
To Queue	Link this to a queue created in the **QoS > Queue Setup** screen, which is the **Email** queue created in this example.

From Interface	This is the interface from which the traffic will be coming from. Select **Lan**.
Ether Type	Select **IP** to identify the traffic source by its IP address or MAC address.
MAC Address	Type the MAC address of your computer - **AA:FF:AA:FF:AA:FF**. Type the **MAC Mask** if you know it.
IP Address	Type the IP address of your computer - **192.168.1.23**. Type the **IP Subnet Mask** if you know it.

This maps e-mail traffic to queue 7 created in the previous screen (see the **IP Protocol** field). This also maps your computer's IP address and MAC address to queue 7 (see the **Source** fields).

4 Verify that the queue setup works by checking **Network Setting > QoS > Monitor**. This shows the bandwidth allotted to e-mail traffic compared to other network traffic.



Monitor

Refresh Interval : 5 seconds

Status :

▪ Interface Monitor

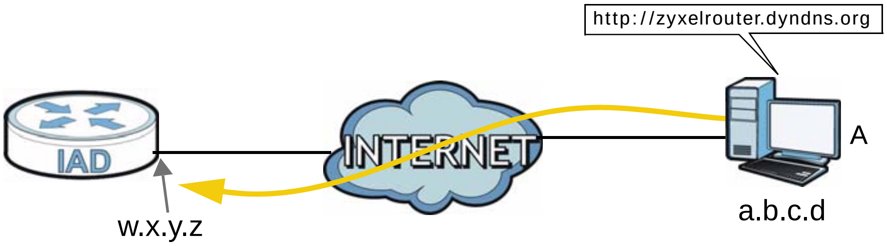
#	Name	Pass Rate(bps)
1	nas1	0
2	ppp0	

▪ Queue Monitor

#	Name	Pass Rate(bps)	Drop Rate(bps)
1	Default_Queue	0	0
2	Email	2992	0

3.9 Access the ZyXEL Device Using DDNS

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



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

This tutorial shows you how to:

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

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

3.9.1 Registering a DDNS Account on www.dyndns.org

1 Open a browser and type **http://www.dyndns.org**.

2 Apply for a user account. This tutorial uses **UserName1** and **12345** as the username and password.

3 Log into www.dyndns.org using your account.

4 Add a new DDNS host name. This tutorial uses the following settings as an example.

- Hostname: **zyxelrouter.dyndns.org**
- Service Type: **Host with IP address**
- IP Address: Enter the WAN IP address that your ZyXEL Device is currently using. You can find the IP address on the ZyXEL Device's web configurator **Status** page.

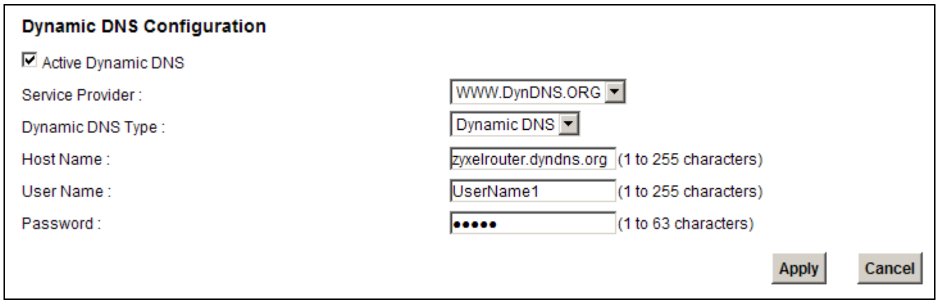
Then you will need to configure the same account and host name on the ZyXEL Device later.

3.9.2 Configuring DDNS on Your ZyXEL Device

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

- Select **Active Dynamic DNS**.
- Select **Dynamic DNS** for the DDNS type.
- Type **zyxelrouter.dyndns.org** in the **Host Name** field.

- Enter the user name (**UserName1**) and password (**12345**).



Dynamic DNS Configuration

☑ Active Dynamic DNS

Service Provider :	WWW.DynDNS.ORG
Dynamic DNS Type :	Dynamic DNS
Host Name :	zyxelrouter.dyndns.org (1 to 255 characters)
User Name :	UserName1 (1 to 255 characters)
Password :	●●●●● (1 to 63 characters)

Click **Apply**.

3.9.3 Testing the DDNS Setting

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

1 Open a web browser on the computer (using the IP address **a.b.c.d**) that is connected to the Internet.

2 Type **http://zyxelrouter.dyndns.org** and press [Enter].

3 The ZyXEL Device’s login page should appear. You can then log into the ZyXEL Device and manage it.

PART II

Technical Reference

4

Connection Status and System Info Screens

4.1 Overview

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

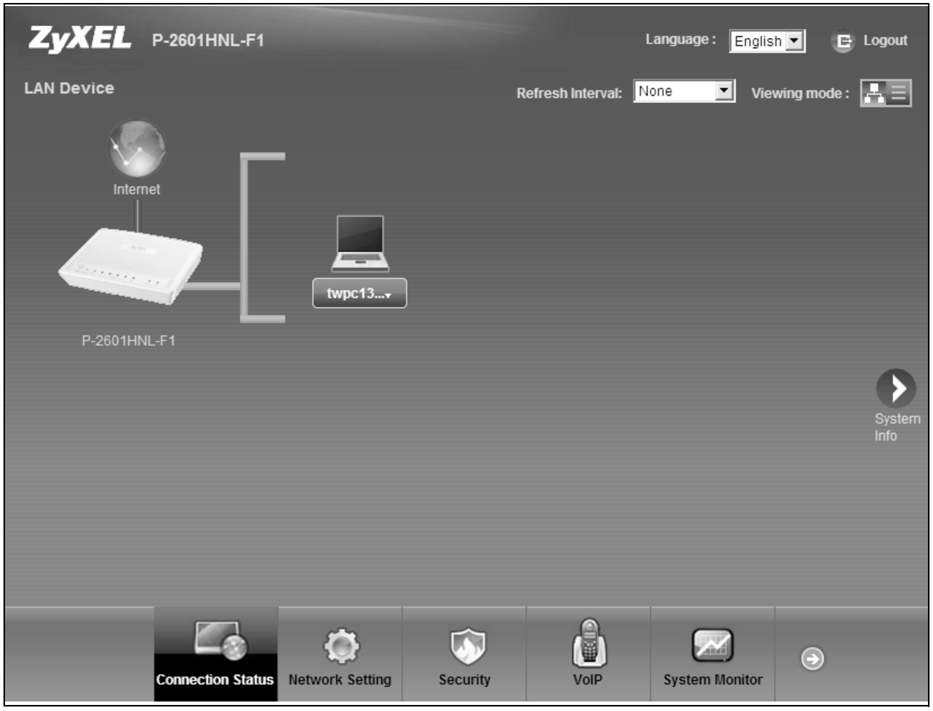
Use the **System Info** screen to look at the current status of the device, system resources, interfaces (LAN, WAN and WLAN), and SIP accounts. You can also register and unregister SIP accounts.

4.2 The Connection Status Screen

Use this screen to view the network connection status of the device and its clients. A warning message appears if there is a connection problem.

If you prefer to view the status in a list, click **List View** in the **Viewing mode** selection box. You can configure how often you want the ZyXEL Device to update this screen in **Refresh Interval**.

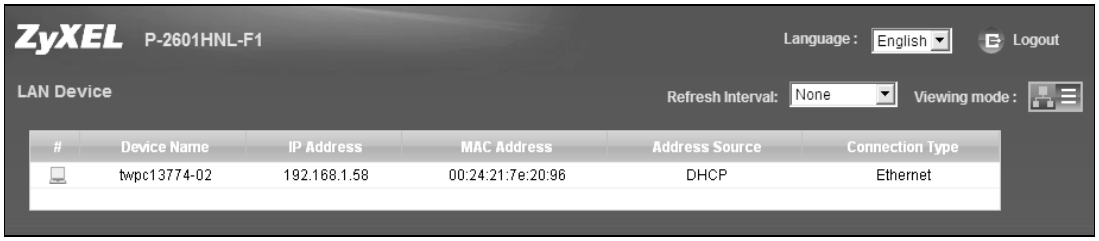
Figure 9 Connection Status: Icon View



Language : English

Refresh Interval: None

Figure 10 Connection Status: List View



Language : English

Refresh Interval: None

#	Device Name	IP Address	MAC Address	Address Source	Connection Type
💻	twpc13774-02	192.168.1.58	00:24:21:7e:20:96	DHCP	Ethernet

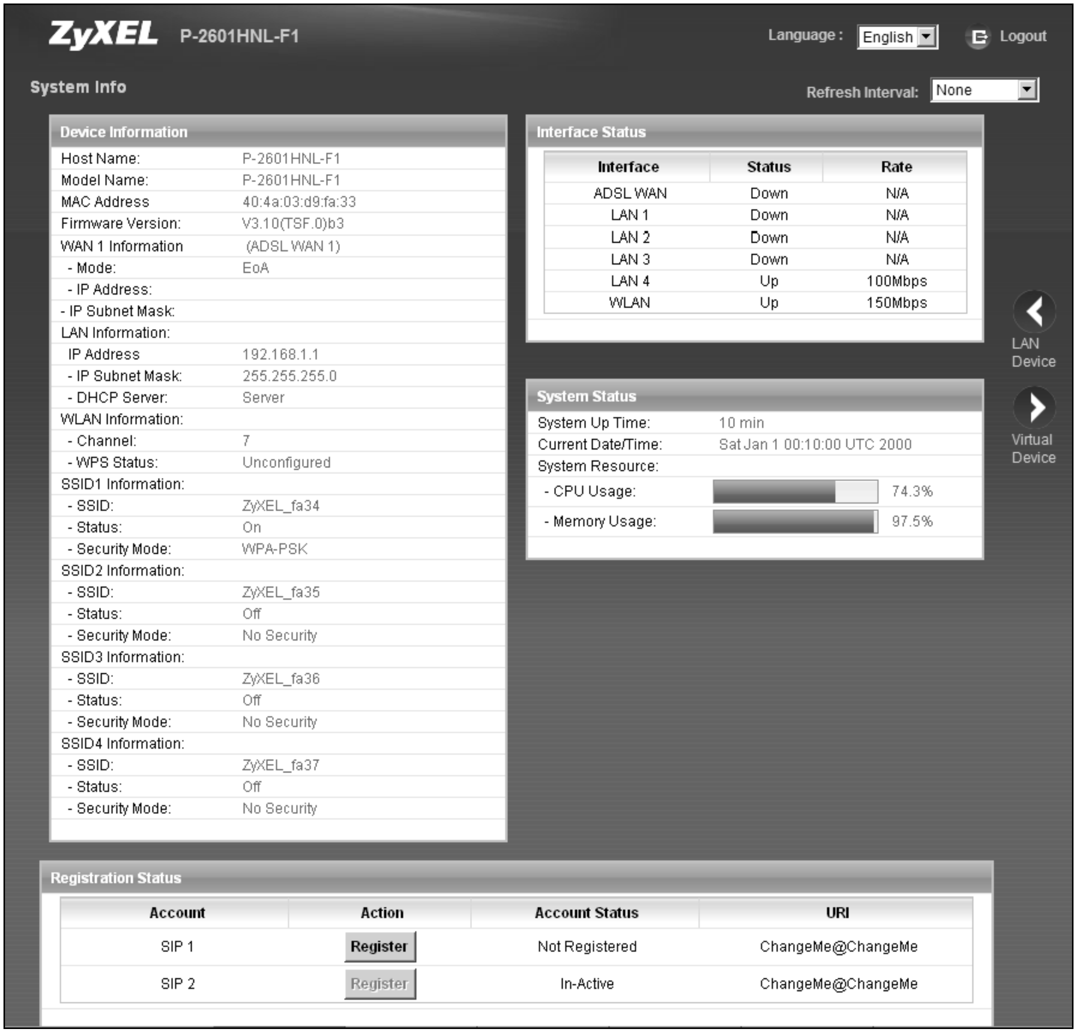
In **Icon View**, if you want to view information about a client, click the client's name and **Info**. Click the IP address if you want to change it. If you want to change the name or icon of the client, click **Change name/icon**.

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

4.3 The System Info Screen

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

Figure 11 System Info Screen



Device Information

Host Name:	P-2601HNL-F1
Model Name:	P-2601HNL-F1
MAC Address	40:4a:03:d9:fa:33
Firmware Version:	V3.10(TSF.0)b3
WAN 1 Information	(ADSL WAN 1)
- Mode:	EoA
- IP Address:	
- IP Subnet Mask:	
LAN Information:	
IP Address	192.168.1.1
- IP Subnet Mask:	255.255.255.0
- DHCP Server:	Server
WLAN Information:	
- Channel:	7
- WPS Status:	Unconfigured
SSID1 Information:	
- SSID:	ZyXEL_fa34
- Status:	On
- Security Mode:	WPA-PSK
SSID2 Information:	
- SSID:	ZyXEL_fa35
- Status:	Off
- Security Mode:	No Security
SSID3 Information:	
- SSID:	ZyXEL_fa36
- Status:	Off
- Security Mode:	No Security
SSID4 Information:	
- SSID:	ZyXEL_fa37
- Status:	Off
- Security Mode:	No Security

Interface Status

Interface	Status	Rate
ADSL WAN	Down	N/A
LAN 1	Down	N/A
LAN 2	Down	N/A
LAN 3	Down	N/A
LAN 4	Up	100Mbps
WLAN	Up	150Mbps

System Status

System Up Time:	10 min
Current Date/Time:	Sat Jan 1 00:10:00 UTC 2000
System Resource:	
- CPU Usage:	74.3%
- Memory Usage:	97.5%

Registration Status

Account	Action	Account Status	URI
SIP 1	Register	Not Registered	ChangeMe@ChangeMe
SIP 2	Register	In-Active	ChangeMe@ChangeMe

Each field is described in the following table.

Table 4 System Info Screen

LABEL	DESCRIPTION
Language	Select the web configurator language from the drop-down list box.
Refresh Interval	Select how often you want the ZyXEL Device to update this screen from the drop-down list box.
Device Information	
Host Name	This field displays the ZyXEL Device system name. It is used for identification. You can change this in the **Maintenance > System** screen's **Host Name** field.
Model Name	This is the model name of your device.

LABEL	DESCRIPTION
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your ZyXEL Device.
Firmware Version	This field displays the current version of the firmware inside the device. It also shows the date the firmware version was created. Go to the **Maintenance > Firmware Upgrade** screen to change it.
WAN Information	
Mode	This is the method of encapsulation used by your ISP.
IP Address	This field displays the current IP address of the ZyXEL Device in the WAN.
IP Subnet Mask	This field displays the current subnet mask in the WAN.
LAN Information	
IP Address	This field displays the current IP address of the ZyXEL Device in the LAN.
IP Subnet Mask	This field displays the current subnet mask in the LAN.
DHCP Server	This field displays what DHCP services the ZyXEL Device is providing to the LAN. Choices are: **Server** - The ZyXEL Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. **Relay** - The ZyXEL Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. **None** - The ZyXEL Device is not providing any DHCP services to the LAN.
WLAN Information	
Channel	This is the channel number used by the ZyXEL Device now.
WPS Status	**Configured** displays when a wireless client has connected to the ZyXEL Device or WPS is enabled and wireless or wireless security settings have been configured. **Unconfigured** displays if WPS is disabled or wireless security settings have not been configured.
SSID (1~4) Information	
SSID	This is the descriptive name used to identify the ZyXEL Device in the wireless LAN.
Status	This shows whether or not the SSID is enabled (on).
Security Mode	This displays the type of security the ZyXEL Device is using in the wireless LAN.
Interface Status	
Interface	This column displays each interface the ZyXEL Device has.

LABEL	DESCRIPTION
Status	This field indicates whether or not the ZyXEL Device is using the interface. For the DSL interface, this field displays **Down** (line is down), **Up** (line is up or connected) if you're using Ethernet encapsulation and **Down** (line is down), **Up** (line is up or connected), **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) and **Drop** (dropping a call) if you're using PPPoE encapsulation. For the WAN interface, this field displays **Up** when the ZyXEL Device is using the interface and **Down** when the ZyXEL Device is not using the interface. For the LAN interface, this field displays **Up** when the ZyXEL Device is using the interface and **Down** when the ZyXEL Device is not using the interface. For the WLAN interface, it displays **Up** when WLAN is enabled or **Down** when WLAN is disabled.
Rate	For the LAN interface, this displays the port speed. For the WAN interface, this displays the port speed. For the DSL interface, it displays the downstream and upstream transmission rate. For the WLAN interface, it displays the maximum transmission rate when WLAN is enabled or **N/A** when WLAN is disabled.
System Status	
System Up Time	This field displays how long the ZyXEL Device has been running since it last started up. The ZyXEL Device starts up when you plug it in, when you restart it (**Maintenance > Reboot**), or when you reset it (see Chapter 1 on page 25).
Current Date/Time	This field displays the current date and time in the ZyXEL Device. You can change this in **Maintenance > Time Setting**.
System Resource	
CPU Usage	This field displays what percentage of the ZyXEL Device's processing ability is currently used. When this percentage is close to 100%, the ZyXEL Device is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications.
Memory Usage	This field displays what percentage of the ZyXEL Device's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100%, the ZyXEL Device is probably becoming unstable, and you should restart the device. See Chapter 26 on page 231, or turn off the device (unplug the power) for a few seconds.
Registration Status	
Account	This column displays each SIP account in the ZyXEL Device.

LABEL	DESCRIPTION
Action	This field displays the current registration status of the SIP account. You have to register SIP accounts with a SIP server to use VoIP. If the SIP account is already registered with the SIP server, • Click **Unregister** to delete the SIP account's registration in the SIP server. This does not cancel your SIP account, but it deletes the mapping between your SIP identity and your IP address or domain name. • The second field displays **Registered**. If the SIP account is not registered with the SIP server, • Click **Register** to have the ZyXEL Device attempt to register the SIP account with the SIP server. • The second field displays the reason the account is not registered. **Inactive** - The SIP account is not active. You can activate it in **VoIP > SIP > SIP Settings**. **Register Fail** - The last time the ZyXEL Device tried to register the SIP account with the SIP server, the attempt failed. The ZyXEL Device automatically tries to register the SIP account when you turn on the ZyXEL Device or when you activate it.
Account Status	This shows **Active** when the SIP account has been registered and ready for use or **In-Active** when the SIP account is not yet registered.
URI	This field displays the account number and service domain of the SIP account. You can change these in **VoIP > SIP > SIP Settings**.

5

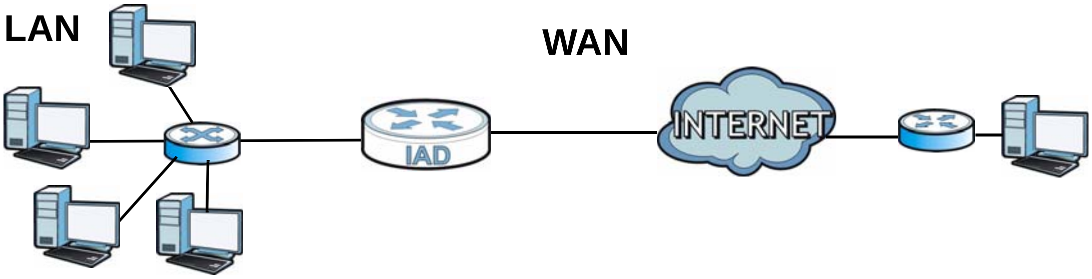
Broadband

5.1 Overview

This chapter describes how to configure WAN settings from the **Broadband** screen. Use this screen 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 12 LAN and WAN



5.1.1 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 encapsulation method).

Multicast

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

IGMP

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

Finding Out More

See Section 5.3 on page 76 for technical background information on WAN.

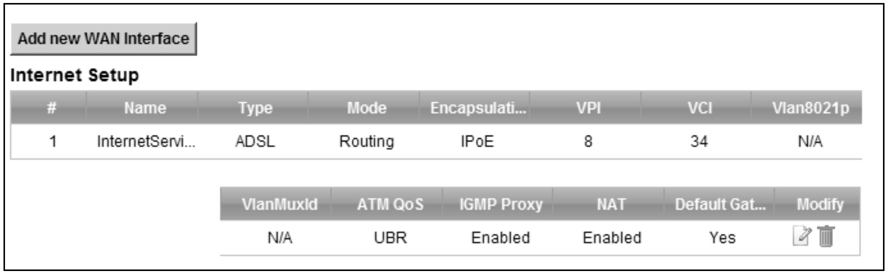
5.1.2 Before You Begin

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

5.2 The Broadband Screen

Use this screen to change your ZyXEL Device's Internet access settings. Click **Network Setting> Broadband** from the menu. The summary table shows you the configured WAN services (connections) on the ZyXEL Device.

Figure 13 Network Setting > Broadband



#	Name	Type	Mode	Encapsulati...	VPI	VCI	Vlan8021p
1	InternetServi...	ADSL	Routing	IPoE	8	34	N/A

VlanMuxId	ATM QoS	IGMP Proxy	NAT	Default Gat...	Modify
N/A	UBR	Enabled	Enabled	Yes	✎ 🗑

The following table describes the labels in this screen.

Table 5 Network Setting > Broadband

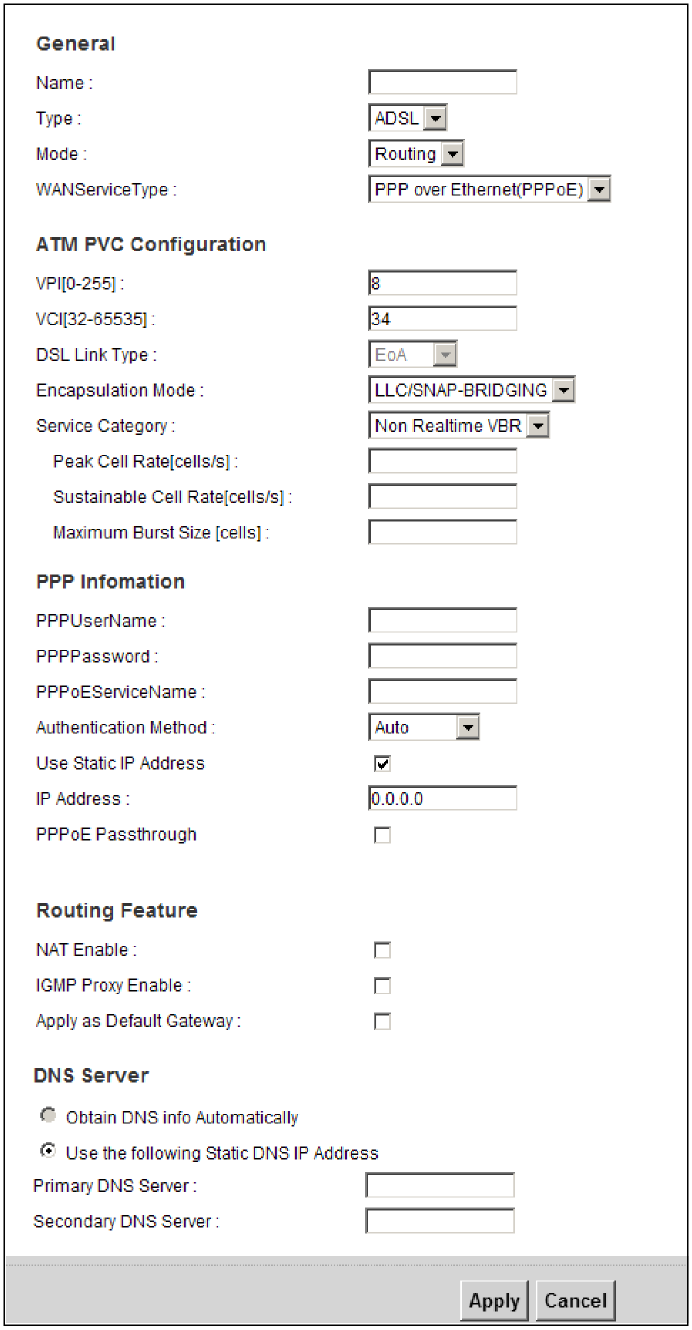
LABEL	DESCRIPTION
Add new WAN interface	Click this button to create a new connection.
#	This is the index number of the entry.
Status	This is the status of the connection.
Name	This is the service name of the connection.
Type	This shows the type of interface used by this connection.
Mode	This shows whether the connection is in routing mode or bridge mode.
Encapsulation	This is the method of encapsulation used by this connection.
VPI/VCI	This is the Virtual Path Identifier (VPI).
VCI	This is the Virtual Channel Identifier (VCI).
Vlan8021p	This indicates the 802.1P priority level assigned to traffic sent through this connection. This displays **N/A** when there is no priority level assigned.
VlanMuxId	This indicates the VLAN ID number assigned to traffic sent through this connection. This displays **N/A** when there is no VLAN ID number assigned.
ATM QoS	This is the type of ATM QoS of the connection.
IGMP Proxy	This shows whether the ZyXEL Device act as an IGMP proxy on this connection.
NAT	This shows whether NAT is activated or not for this connection.
Default Gateway	This shows whether the ZyXEL Device use the WAN interface of this connection as the system default gateway.
Modify	Click the **Edit** icon to configure the connection. Click the **Delete** icon to remove the connection.

5.2.1 Add/Edit Broadband

Click **Add new WAN interface** in the **Broadband** screen or the **Edit** icon next to an existing WAN interface to configure a WAN connection. The screen differs according to the mode and encapsulation you choose.

This screen displays when you select the **Routing** mode and **PPPoE** encapsulation. The fields in the screen may differ depending on the type of encapsulation you use.

Figure 14 Broadband: Add/Edit: Routing Mode



General

Name :	
Type :	ADSL
Mode :	Routing
WANServiceType :	PPP over Ethernet(PPPoE)

ATM PVC Configuration

VPI[0-255] :	8
VCI[32-65535] :	34
DSL Link Type :	EoA
Encapsulation Mode :	LLC/SNAP-BRIDGING
Service Category :	Non Realtime VBR
Peak Cell Rate[cells/s] :	
Sustainable Cell Rate[cells/s] :	
Maximum Burst Size [cells] :	

PPP Infomation

PPPUserName :	
PPPPassword :	
PPPoEServiceName :	
Authentication Method :	Auto
Use Static IP Address	☑
IP Address :	0.0.0.0
PPPoE Passthrough	☐

Routing Feature

NAT Enable :	☐
IGMP Proxy Enable :	☐
Apply as Default Gateway :	☐

DNS Server

○ Obtain DNS info Automatically

● Use the following Static DNS IP Address

Primary DNS Server :	
Secondary DNS Server :	

The following table describes the labels in this screen.

Table 6 Broadband: Add/Edit: Routing Mode

LABEL	DESCRIPTION
General	
Name	Enter a service name of the connection.
Type	The interface type used by the ZyXEL Device is **ADSL**. The ZyXEL Device uses the ADSL technology for data transmission over the DSL port.
Mode	Select **Routing** (default) from the drop-down list box if your ISP give you one IP address only and you want multiple computers to share an Internet account.
WAN Service Type	Select the method of encapsulation used by your ISP from the drop-down list box. This option is available only when you select **Routing** in the **Mode** field. The choices are **PPPoE**, **PPPoA**, and **IPoE**.
ATM PVC Configuration	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
DSL Link Type	If your **WAN Service Type** is **PPPoE** or **IPoE**, the DSL link type is set to **EoA** (Ethernet over ATM) to have an Ethernet header in the packet, so that you can have multiple services/connections over one PVC. You can set each connection to have its own MAC address or all connections share one MAC address but use different VLAN IDs for different services. **EoA** supports IPoE, PPPoE and RFC1483/2684 bridging encapsulation methods. If your **WAN Service Type** is **PPPoA**, the DSL link type is set to **PPPoA** (PPP over ATM) to allow just one PPPoA connection over a PVC.
Encapsulation Mode	Select the method of multiplexing used by your ISP from the drop-down list box. Choices are: • **LLC/SNAP-BRIDGING:** In LCC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header. • **VC/MUX:** In VC multiplexing, each protocol is carried on a single ATM virtual circuit (VC). To transport multiple protocols, the ZyXEL Device needs separate VCs. There is a binding between a VC and the type of the network protocol carried on the VC. This reduces payload overhead since there is no need to carry protocol information in each Protocol Data Unit (PDU) payload.

Table 6 Broadband: Add/Edit: Routing Mode (continued)

LABEL	DESCRIPTION
Service Category	Select **UBR Without PCR** for applications that are non-time sensitive, such as e-mail. Select **CBR** (Constant Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **Non Realtime VBR** (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation. Select **Realtime VBR** (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here. This field is not available when you select **UBR Without PCR**.
Sustainable Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec. This field is available only when you select **Non Realtime VBR** or **Realtime VBR**.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535. This field is available only when you select **Non Realtime VBR** or **Realtime VBR**.
PPP Information	This section is available only when you select **Routing** in the **Mode** field and **PPPoE** or **PPPoA** in the **WAN Service Type** field.
PPP User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
PPP Password	Enter the password associated with the user name above.
PPPoE Service Name	Type the name of your PPPoE service here. This field is available only when you select **PPPoE** in the **WAN Service Type** field.
Authentication Mode	The ZyXEL Device supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms. Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **AUTO**: Your ZyXEL Device accepts either CHAP or PAP when requested by this remote node. **PAP**: Your ZyXEL Device accepts PAP only. **CHAP**: Your ZyXEL Device accepts CHAP only. **MS-CHAP**: Your ZyXEL Device accepts MSCHAP only. MS-CHAP is the Microsoft version of the CHAP.

Table 6 Broadband: Add/Edit: Routing Mode (continued)

LABEL	DESCRIPTION
Use Static IP Address	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you want to get a dynamic IP address from the ISP.
IP Address	Enter the static IP address provided by your ISP.
PPPoE Passthrough	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. PPPoE pass through is an alternative to NAT for application where NAT is not appropriate. 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. This field is available only when you select **PPPoE** in the **WAN Service Type** field.
IP Address	This section is available only when you select **Routing** in the **Mode** field and **IPoE** in the **WAN Service Type** field.
Obtain an IP Address Automatically	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you have a dynamic IP address.
Enable DHCP Option 60	Select this to identify the vendor and functionality of the ZyXEL Device in DHCP requests that the ZyXEL Device sends to a DHCP server when getting a WAN IP address.
Vendor Class Identifier	Enter the Vendor Class Identifier (Option 60), such as the type of the hardware or firmware.
Static IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter the static IP address provided by your ISP.
Subnet Mask	Enter the subnet mask provided by your ISP.
Gateway IP Address	Enter the gateway IP address provided by your ISP.
Routing Feature	
NAT Enable	Select this option to activate NAT on this connection.
IGMP Proxy Enable	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. Select this option to have the ZyXEL Device act as an IGMP proxy on this connection. This allows the ZyXEL Device to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Apply as Default Gateway	Select this option to have the ZyXEL Device use the WAN interface of this connection as the system default gateway.
DNS Server	The section is not available when you select **Bridge** in the **WAN Service Type** field.

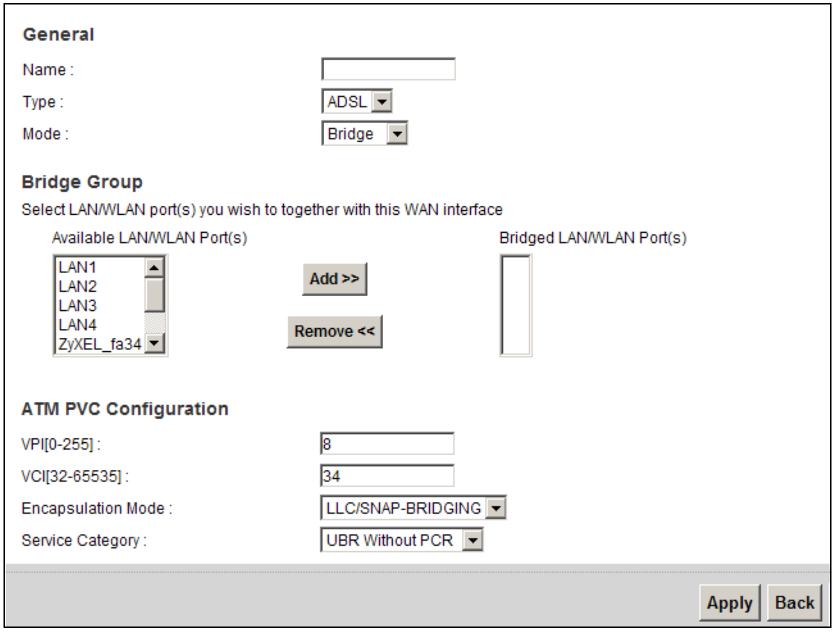
Table 6 Broadband: Add/Edit: Routing Mode (continued)

LABEL	DESCRIPTION
Obtain DNS info Automatically	Select this to have the ZyXEL Device get the DNS server addresses from the ISP automatically.
Use the following Static DNS IP Address	Select this to have the ZyXEL Device use the DNS server addresses you configure manually.
Primary DNS Server	Enter the first DNS server address assigned by the ISP.
Secondary DNS Server	Enter the second DNS server address assigned by the ISP.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen.

5.2.1.1 Bridge

This screen displays when you select the **Bridge** mode.

Figure 15 Broadband: Add/Edit: Bridge Mode



General

Name :

Type : ADSL

Mode : Bridge

Bridge Group

Select LAN/WLAN port(s) you wish to together with this WAN interface

Available LAN/WLAN Port(s): LAN1, LAN2, LAN3, LAN4, ZyXEL_fa34

Bridged LAN/WLAN Port(s)

ATM PVC Configuration

VPI[0-255] : 8

VCI[32-65535] : 34

Encapsulation Mode : LLC/SNAP-BRIDGING

Service Category : UBR Without PCR

The following table describes the labels in this screen.

Table 7 Broadband: Add/Edit: Bridge Mode

LABEL	DESCRIPTION
General	
Name	Specify a descriptive name of up to 15 alphanumeric characters for this connection.
Type	The interface type used by the ZyXEL Device is **ADSL**. The ZyXEL Device uses the ADSL technology for data transmission over the DSL port.

Table 7 Broadband: Add/Edit: Bridge Mode (continued)

LABEL	DESCRIPTION
Mode	Select **Bridge** when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. If you select **Bridge**, you cannot use routing functions, such as Firewall, DHCP server and NAT on traffic from the selected LAN port(s).
Encapsulation	This field is not available if you select **Bridge** mode.
Bridge Group	Select the LAN/WLAN port(s) from which traffic will be forwarded to the WAN interface directly. Select a port from the **Available LAN/WLAN Port(s)** list and click **Add >>** to add it to the **Bridged LAN/WLAN Port(s)** list. If you want to remove a port from the **Bridged LAN/WLAN Port(s)** list, select it and click **Remove <<**. You cannot configure a QoS class for traffic from the LAN port which is selected here.
ATM PVC Configuration	
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
Encapsulation Mode	Select the method of multiplexing used by your ISP from the drop-down list box. Choices are: • **LLC/SNAP-BRIDGING:** In LCC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header. • **VC/MUX:** In VC multiplexing, each protocol is carried on a single ATM virtual circuit (VC). To transport multiple protocols, the ZyXEL Device needs separate VCs. There is a binding between a VC and the type of the network protocol carried on the VC. This reduces payload overhead since there is no need to carry protocol information in each Protocol Data Unit (PDU) payload.
Service Category	Select **UBR Without PCR** or **UBR With PCR** for applications that are non-time sensitive, such as e-mail. Select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **Non Realtime VBR** (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation. Select **Realtime VBR** (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.This field is not available when you select **UBR Without PCR**.

Table 7 Broadband: Add/Edit: Bridge Mode (continued)

LABEL	DESCRIPTION
Sustain Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec. This field is available only when you select **Non Realtime VBR** or **Realtime VBR**.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535. This field is available only when you select **Non Realtime VBR** or **Realtime VBR**.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Back	Click **Back** to exit this screen without saving.

5.3 Technical Reference

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

5.3.1 Encapsulation

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

5.3.1.1 PPP over Ethernet

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

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

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

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

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

5.3.1.2 PPPoA

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

5.3.2 Multiplexing

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

VC-based Multiplexing

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

LLC-based Multiplexing

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

5.3.3 VPI and VCI

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

5.3.4 IP Address Assignment

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

IP Assignment with PPPoA or PPPoE Encapsulation

If you have a dynamic IP, then the **IP Address** and **Gateway IP Address** fields are not applicable (N/A). If you have a static IP, then you only need to fill in the **IP Address** field and not the **Gateway IP Address** field.

5.3.5 NAT

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

5.4 Traffic Shaping

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

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

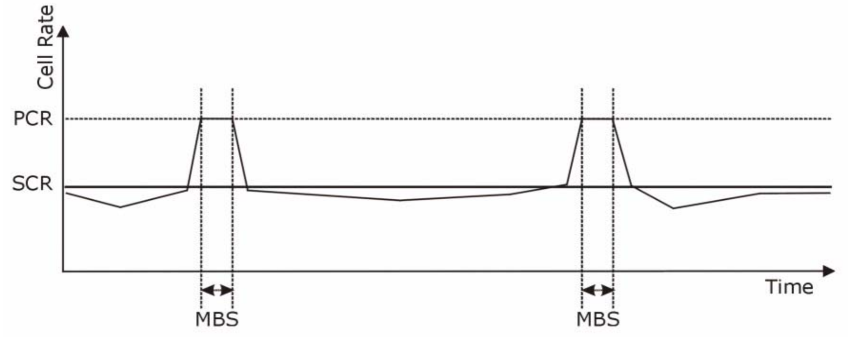
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

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

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

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

Figure 16 Example of Traffic Shaping



5.4.1 ATM Traffic Classes

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

Constant Bit Rate (CBR)

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

Variable Bit Rate (VBR)

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

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

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

Unspecified Bit Rate (UBR)

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

6

Wireless

6.1 Overview

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

6.1.1 What You Can Do in this Chapter

- Use the **General** screen to enable the Wireless LAN, enter the SSID and select the wireless security mode (Section 6.2 on page 83).
- Use the **More AP** screen to set up multiple wireless networks on your ZyXEL Device (Section 6.3 on page 91).
- Use the **WPS** screen to enable or disable WPS, view or generate a security PIN (Personal Identification Number) (Section 6.4 on page 93).
- Use the **WMM** screen to enable Wi-Fi MultiMedia (WMM) to ensure quality of service in wireless networks for multimedia applications (Section 6.5 on page 95).
- Use the **Scheduling** screen to schedule a time period for the wireless LAN to operate each day (Section 6.6 on page 97).

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.

6.1.2 Wireless Network Overview

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

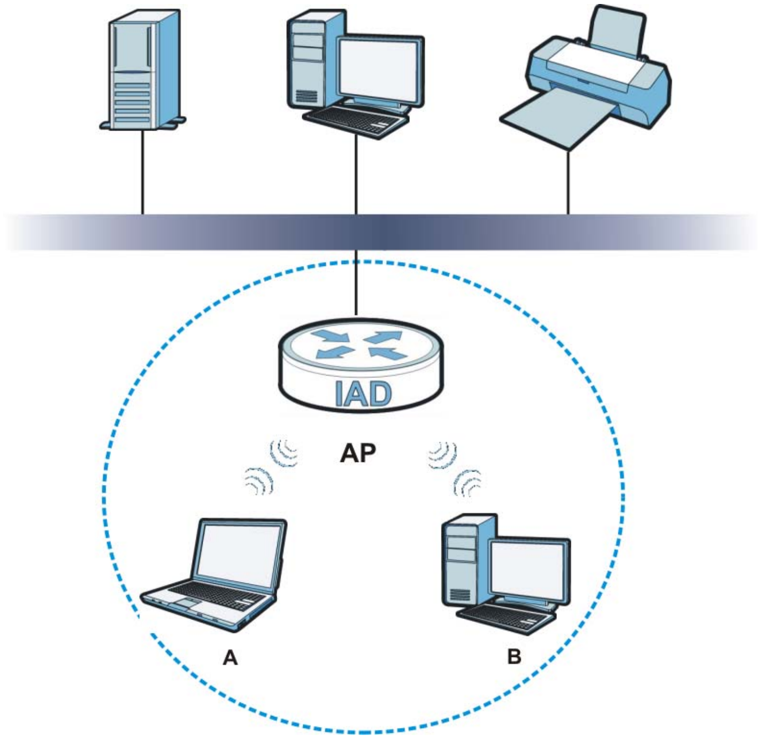
- A wireless client is a radio connected to a user's computer.
- An access point is a radio with a wired connection to a network, which can connect with numerous wireless clients and let them access the network.
- A bridge is a radio that relays communications between access points and wireless clients,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

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

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

The following figure provides an example of a wireless network.

Figure 17 Example of a Wireless Network



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

Every wireless network must follow these basic guidelines.

- Every device in the same wireless network must use the same SSID.

  The SSID is the name of the wireless network. It stands for Service Set IDentifier.
- If two wireless networks overlap, they should use a different channel.

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

Radio Channels

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

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

6.1.3 Before You Begin

Before you start using these screens, ask yourself the following questions. See Section 6.7 on page 97 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.

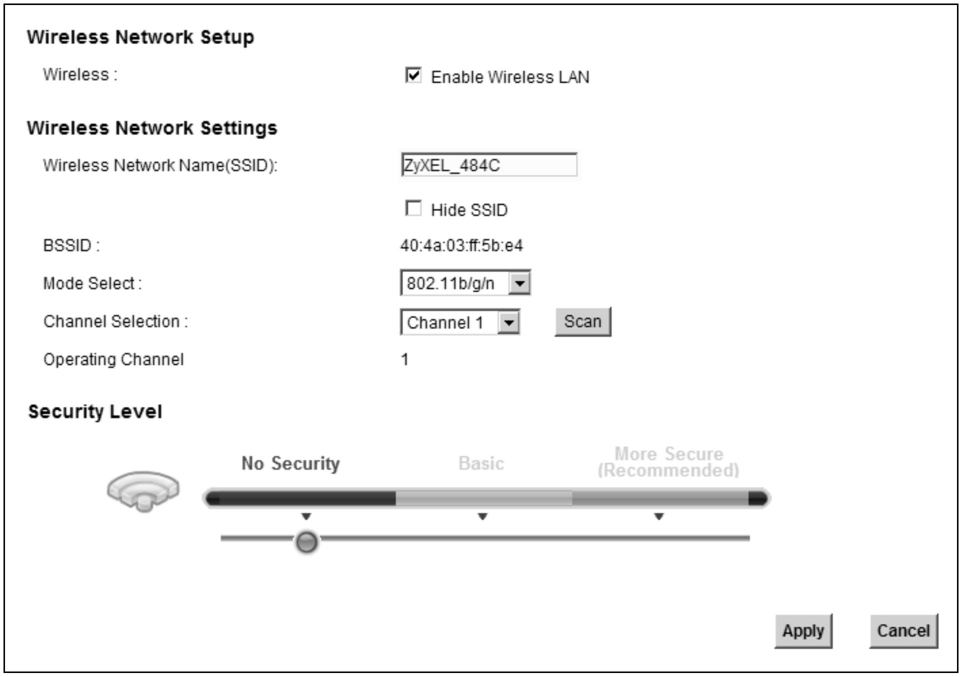
6.2 The Wireless General Screen

Use this screen to enable the Wireless LAN, enter the SSID and select the wireless security mode.

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

Figure 18 Network Setting > Wireless > General



Wireless Network Setup

Wireless : ☑ Enable Wireless LAN

Wireless Network Settings

Wireless Network Name(SSID): ZyXEL_484C

☐ Hide SSID

BSSID : 40:4a:03:ff:5b:e4

Mode Select : 802.11b/g/n

Channel Selection : Channel 1

Operating Channel 1

Security Level

The following table describes the labels in this screen.

Table 8 Network > Wireless LAN > General

LABEL	DESCRIPTION
Wireless Network Setup	
Wireless	Select the **Enable Wireless LAN** check box to activate the wireless LAN.
Wireless Network Settings	
Wireless Network Name (SSID)	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
BSSID	This shows the MAC address of the wireless interface on the ZyXEL Device when wireless LAN is enabled.

Table 8 Network > Wireless LAN > General (continued)

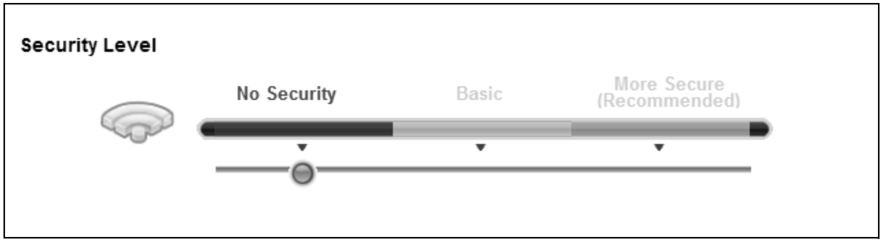
LABEL	DESCRIPTION
Mode Select	This makes sure that only compliant WLAN devices can associate with the ZyXEL Device. Select **802.11b/g/n** to allow IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced. Select **802.11b/g** to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced. Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device.
Channel Selection	Set the channel depending on your particular region. Select a channel or use **Auto** to have the ZyXEL Device automatically determine a channel to use. If you are having problems with wireless interference, changing the channel may help. Try to use a channel that is as many channels away from any channels used by neighboring APs as possible. The channel number which the ZyXEL Device is currently using then displays in the **Operating Channel** field.
Scan	Click this button to have the ZyXEL Device immediately scan for and select a channel (which is not used by another device) whenever the device reboots or the wireless setting is changed.
Operating Channel	This is the channel currently being used by your AP.
Security Level	
Security Mode	Select **Basic** or **More Secure** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the ZyXEL Device. When you select to use a security, additional options appears in this screen. Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication. See the following sections for more details about wireless security modes.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to restore your previously saved settings.

6.2.1 No Security

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

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

Figure 19 Wireless > General: No Security



The following table describes the labels in this screen.

Table 9 Wireless > General: No Security

LABEL	DESCRIPTION
Security Level	Choose **No Security** from the sliding bar.

6.2.2 Basic (Static WEP/Shared WEP Encryption)

WEP encryption scrambles the data transmitted between the wireless stations and the access points (AP) to keep network communications private. Both the wireless stations and the access points must use the same WEP key.

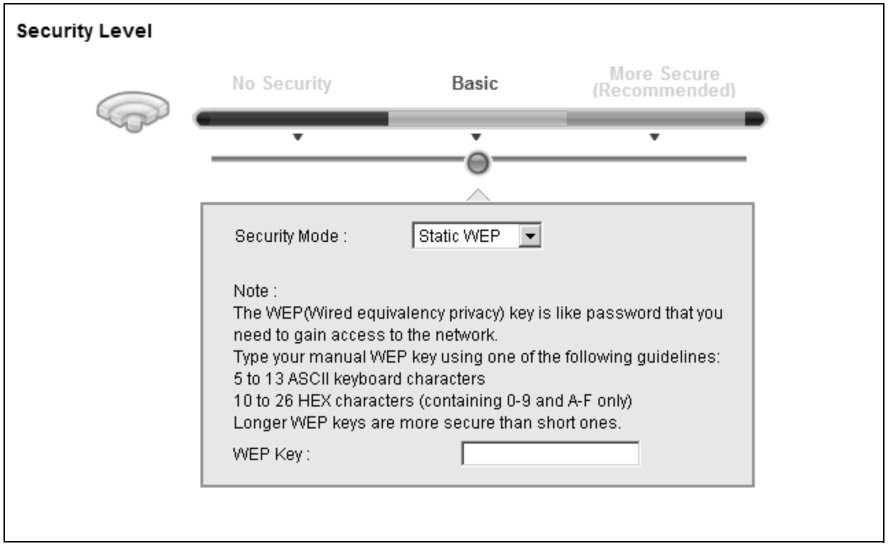
There are two types of WEP authentication namely, Open System (**Static WEP**) and Shared Key (**Shared WEP**).

Open system is implemented for ease-of-use and when security is not an issue. The wireless station and the AP or peer computer do not share a secret key. Thus the wireless stations can associate with any AP or peer computer and listen to any transmitted data that is not encrypted.

Shared key mode involves a shared secret key to authenticate the wireless station to the AP or peer computer. This requires you to enable the wireless LAN security and use same settings on both the wireless station and the AP or peer computer.

In order to configure and enable WEP encryption, click **Network Settings > Wireless** to display the **General** screen. Select **Basic** as the security level. Then select **Static WEP** or **Shared WEP** from the **Security Mode** list.

Figure 20 Wireless > General: Basic (Static WEP/Shared WEP)



Security Level

Security Mode : Static WEP

Note :
The WEP(Wired equivalency privacy) key is like password that you need to gain access to the network.
Type your manual WEP key using one of the following guidelines:
5 to 13 ASCII keyboard characters
10 to 26 HEX characters (containing 0-9 and A-F only)
Longer WEP keys are more secure than short ones.

WEP Key :

The following table describes the labels in this screen.

Table 10 Wireless > General: Basic (Static WEP/Shared WEP)

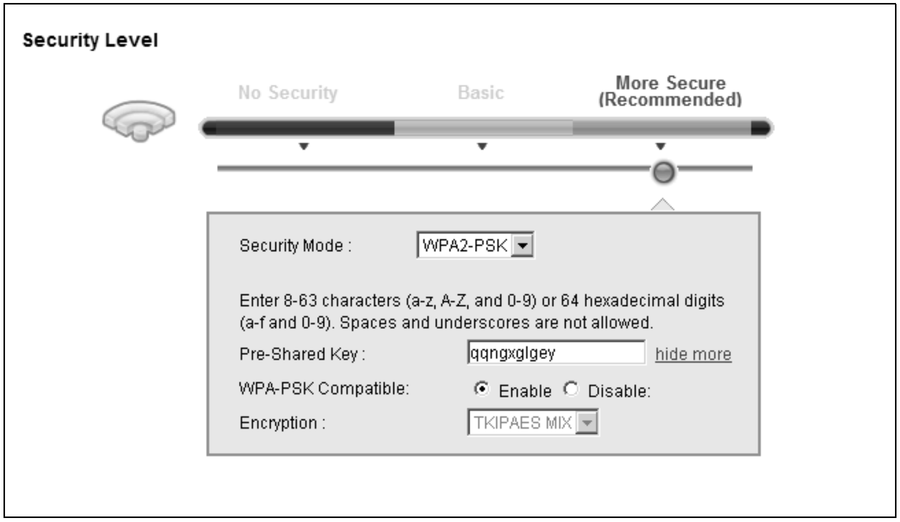
LABEL	DESCRIPTION
Security Mode	Choose **Static WEP** or **Shared WEP** from the drop-down list box. • Select **Static WEP** to have the ZyXEL Device allow association with wireless clients that use Open System mode. Data transfer is encrypted as long as the wireless client has the correct WEP key for encryption. The ZyXEL Device authenticates wireless clients using Shared Key mode that have the correct WEP key. • Select **Shared WEP** to have the ZyXEL Device authenticate only those wireless clients that use Shared Key mode and have the correct WEP key.
WEP Key	Enter a WEP key that will be used to encrypt data. Both the ZyXEL Device and the wireless stations must use the same WEP key for data transmission. If you want to manually set the WEP key, enter any 5 or 13 characters (ASCII string) or 10 or 26 hexadecimal characters ("0-9", "A-F") for a 64-bit or 128-bit WEP key respectively.

6.2.3 More Secure (WPA(2)-PSK)

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

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

Figure 21 Wireless > General: More Secure: WPA(2)-PSK



Security Mode : WPA2-PSK

Enter 8-63 characters (a-z, A-Z, and 0-9) or 64 hexadecimal digits (a-f and 0-9). Spaces and underscores are not allowed.

Pre-Shared Key : qqngxglgey

WPA-PSK Compatible: ● Enable ○ Disable:

Encryption : TKIPAES MIX

The following table describes the labels in this screen.

Table 11 Wireless > General: WPA(2)-PSK

LABEL	DESCRIPTION
Security Level	Select **More Secure** to enable WPA(2)-PSK data encryption.
Security Mode	Select **WPA-PSK** or **WPA2-PSK** from the drop-down list box.
Pre-Shared Key	The encryption mechanisms used for **WPA/WPA2** and **WPA-PSK/WPA2-PSK** are the same. The only difference between the two is that **WPA-PSK/WPA2-PSK** uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters or 64 hexidecimal digits.
more.../hide more	Click **more...** to show more fields in this section. Click **hide more** to hide them.

Table 11 Wireless > General: WPA(2)-PSK (continued)

LABEL	DESCRIPTION
WPA-PSK Compatible	This field appears when you choose **WPA-PSK2** as the **Security Mode**. Check this field to allow wireless devices using **WPA-PSK** security mode to connect to your ZyXEL Device. The ZyXEL Device supports WPA-PSK and WPA2-PSK simultaneously.
Encryption	If the security mode is **WPA-PSK**, the encryption mode is set to **TKIP** to enable Temporal Key Integrity Protocol (TKIP) security on your wireless network. If the security mode is **WPA-PSK2** and **WPA-PSK Compatible** is disabled, the encryption mode is set to **AES** to enable Advanced Encryption System (AES) security on your wireless network. AES provides superior security to TKIP. If the security mode is **WPA-PSK2** and **WPA-PSK Compatible** is enabled, the encryption mode is set to **TKIPAES MIX** to allow both TKIP and AES types of security in your wireless network.

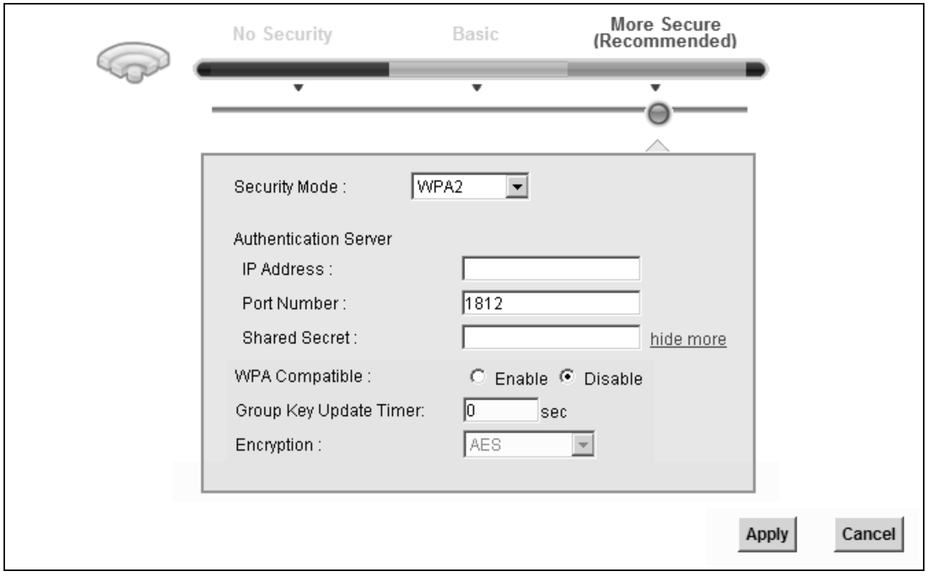
6.2.4 WPA(2) Authentication

The WPA2 security mode is currently the most robust form of encryption for wireless networks. It requires a RADIUS server to authenticate user credentials and is a full implementation the security protocol. Use this security option for maximum protection of your network. However, it is the least backwards compatible with older devices.

The WPA security mode is a security subset of WPA2. It requires the presence of a RADIUS server on your network in order to validate user credentials. This encryption standard is slightly older than WPA2 and therefore is more compatible with older devices.

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

Figure 22 Wireless > General: More Secure: WPA(2)



Security Mode : WPA2

Authentication Server

IP Address :

Port Number : 1812

Shared Secret :

WPA Compatible : ○ Enable ● Disable

Group Key Update Timer: 0 sec

Encryption : AES

The following table describes the labels in this screen.

Table 12 Wireless > General: More Secure: WPA(2)

LABEL	DESCRIPTION
Security Level	Select **More Secure** to enable WPA(2)-PSK data encryption.
Security Mode	Choose **WPA** or **WPA2** from the drop-down list box.
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the ZyXEL Device. The key must be the same on the external authentication server and your ZyXEL Device. The key is not sent over the network.
more.../hide more	Click **more...** to show more fields in this section. Click **hide more** to hide them.
WPA Compatible	This field is only available for WPA2. Select this if you want the ZyXEL Device to support WPA and WPA2 simultaneously.

Table 12 Wireless > General: More Secure: WPA(2) (continued)

LABEL	DESCRIPTION
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the RADIUS server sends a new group key out to all clients.
Encryption	If the security mode is **WPA**, the encryption mode is set to **TKIP** to enable Temporal Key Integrity Protocol (TKIP) security on your wireless network. If the security mode is **WPA2** and **WPA Compatible** is disabled, the encryption mode is set to **AES** to enable Advanced Encryption System (AES) security on your wireless network. AES provides superior security to TKIP. If the security mode is **WPA2** and **WPA Compatible** is enabled, the encryption mode is set to **TKIPAES MIX** to allow the wireless clients to use either TKIP or AES.

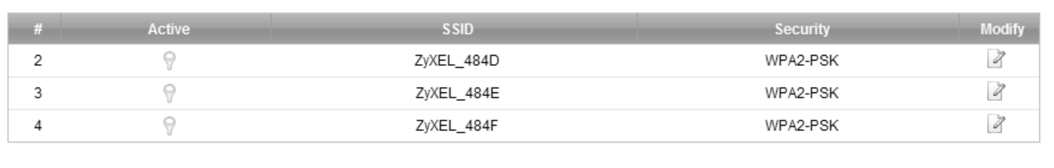
6.3 The More AP Screen

The ZyXEL Device can broadcast up to four wireless network names at the same time. This means that users can connect to the ZyXEL Device using different SSIDs. You can secure the connection on each SSID profile so that wireless clients connecting to the ZyXEL Device using different SSIDs cannot communicate with each other.

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

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

Figure 23 Network Settings > Wireless > More AP



#	Active	SSID	Security	Modify
2	💡	ZyXEL_484D	WPA2-PSK	✎
3	💡	ZyXEL_484E	WPA2-PSK	✎
4	💡	ZyXEL_484F	WPA2-PSK	✎

The following table describes the labels in this screen.

Table 13 Network Settings > Wireless > More AP

LABEL	DESCRIPTION
#	This is the index number of the entry.
Active	This field indicates whether this SSID is active. A yellow bulb signifies that this SSID is active. A gray bulb signifies that this SSID is not active.

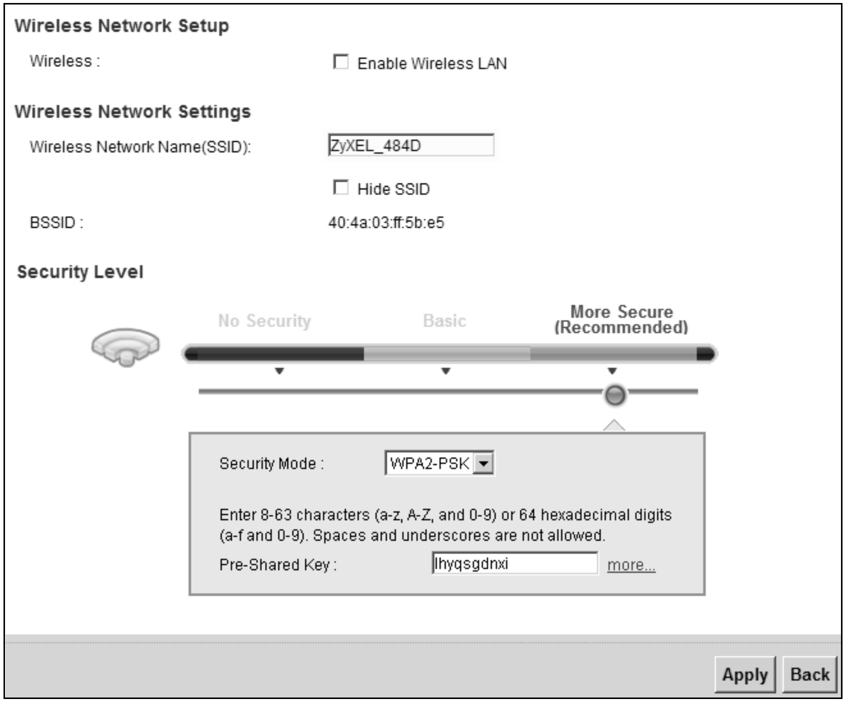
Table 13 Network Settings > Wireless > More AP (continued)

LABEL	DESCRIPTION
SSID	An SSID profile is the set of parameters relating to one of the ZyXEL Device's BSSs. The SSID (Service Set IDentifier) identifies the Service Set with which a wireless device is associated. This field displays the name of the wireless profile on the network. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
Security	This field indicates the security mode of the SSID profile.
Modify	Click the **Edit** icon to configure the SSID profile.

6.3.1 Edit More AP

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

Figure 24 Wireless > More AP: Edit



Wireless Network Setup

Wireless : □ Enable Wireless LAN

Wireless Network Settings

Wireless Network Name(SSID): ZyXEL_484D

□ Hide SSID

BSSID : 40:4a:03:ff:5b:e5

Security Level

Security Mode : WPA2-PSK

Enter 8-63 characters (a-z, A-Z, and 0-9) or 64 hexadecimal digits (a-f and 0-9). Spaces and underscores are not allowed.

Pre-Shared Key : lhyqsgdnxi

The following table describes the fields in this screen.

Table 14 Wireless > More AP: Edit

LABEL	DESCRIPTION
Wireless Network Setup	
Wireless	Select the **Enable Wireless LAN** check box to activate the wireless LAN.
Wireless Network Settings	

Table 14 Wireless > More AP: Edit (continued)

LABEL	DESCRIPTION
Wireless Network Name (SSID)	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
BSSID	This shows the MAC address of the wireless interface on the ZyXEL Device when wireless LAN is enabled.
Security Level	
Security Mode	Select **Basic (WEP)** or **More Secure (WPA(2)-PSK, WPA(2))** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the ZyXEL Device. After you select to use a security, additional options appears in this screen. Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication. See Section 6.2.1 on page 85 for more details about this field.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to exit this screen without saving.

6.4 The WPS Screen

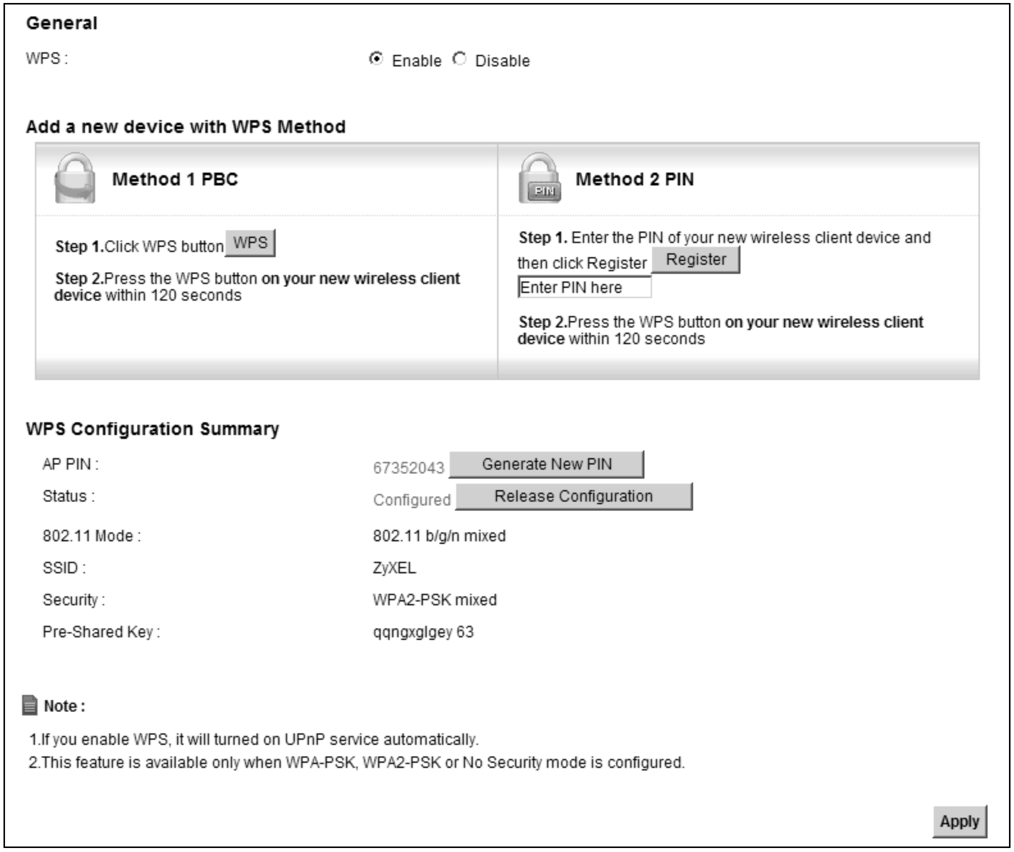
Use this screen to configure WiFi Protected Setup (WPS) on your ZyXEL Device.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Set up each WPS connection between two devices. Both devices must support WPS. See Section 6.7.6.3 on page 105 for more information about WPS.

Note: The ZyXEL Device applies the security settings of the **SSID1** profile (see Section 6.2 on page 83). If you want to use the WPS feature, make sure you have set the security mode of **SSID1** to **WPA-PSK**, **WPA2-PSK** or **No Security**.

Click **Network Setting > Wireless > WPS**. The following screen displays. Select **Enable** and click **Apply** to activate the WPS function. You can configure the WPS settings in this screen.

Figure 25 Network Setting > Wireless > WPS



General

WPS : ● Enable ○ Disable

Add a new device with WPS Method

Step 1.Click WPS button WPS

Step 2.Press the WPS button on your new wireless client device within 120 seconds

Step 1. Enter the PIN of your new wireless client device and then click Register Register

Enter PIN here

Step 2.Press the WPS button on your new wireless client device within 120 seconds

WPS Configuration Summary

AP PIN : 67352043 Generate New PIN

Status : Configured Release Configuration

802.11 Mode : 802.11 b/g/n mixed

SSID : ZyXEL

Security : WPA2-PSK mixed

Pre-Shared Key : qqngxglgey 63

Note :

1.If you enable WPS, it will turned on UPnP service automatically.

2.This feature is available only when WPA-PSK, WPA2-PSK or No Security mode is configured.

The following table describes the labels in this screen.

Table 15 Network Setting > Wireless > WPS

LABEL	DESCRIPTION
Enable WPS	Select **Enable** to activate WPS on the ZyXEL Device.
Add a new device with WPS Method	
Method 1PBC	Use this section to set up a WPS wireless network using Push Button Configuration (PBC).
WPS	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 **WPS** button on this screen. Note: You must press the other wireless device's WPS button within two minutes of pressing this button.
Method 2 PIN	Use this section to set up a WPS wireless network by entering the PIN (Personal Identification Number) of the client into the ZyXEL Device.

Table 15 Network Setting > Wireless > WPS (continued)

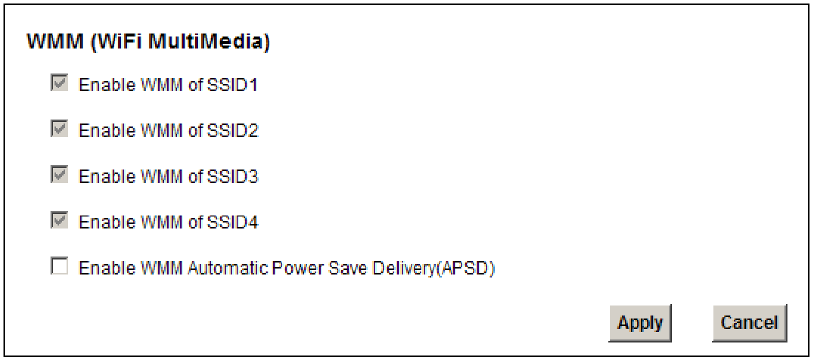
LABEL	DESCRIPTION
Register	Enter the PIN of the device that you are setting up a WPS connection with and click **Register** to authenticate and add the wireless device to your wireless network. You can find the PIN either on the outside of the device, or by checking the device's settings. Note: You must also activate WPS on that device within two minutes to have it present its PIN to the ZyXEL Device.
WPS Configuration Summary	
AP PIN	The PIN of the ZyXEL Device is shown here. Enter this PIN in the configuration utility of the device you want to connect to using WPS. The PIN is not necessary when you use WPS push-button method. Click the **Generate New PIN** button to have the ZyXEL Device create a new PIN.
Status	This displays **Configured** when the ZyXEL Device has connected to a wireless network using WPS or **Enable WPS** is selected and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the screen. This displays **Not Configured** when there is no wireless or wireless security changes on the ZyXEL Device or you click **Release Configuration** to remove the configured wireless and wireless security settings.
Release Configuration	This button is available when the WPS status is **Configured.** Click this button to remove all configured wireless and wireless security settings for WPS connections on the ZyXEL Device.
802.11 Mode	This is the 802.11 mode used. Only compliant WLAN devices can associate with the ZyXEL Device.
SSID	This is the name of the wireless network.
Security	This is the type of wireless security employed by the network.
Apply	Click **Apply** to save your changes.

6.5 The WMM Screen

Use this screen to enable or disable Wi-Fi MultiMedia (WMM) wireless networks for multimedia applications.

Click **Network Setting > Wireless > WMM**. The following screen displays.

Figure 26 Network Setting > Wireless > WMM



WMM (WiFi MultiMedia)

☑ Enable WMM of SSID1

☑ Enable WMM of SSID2

☑ Enable WMM of SSID3

☑ Enable WMM of SSID4

☐ Enable WMM Automatic Power Save Delivery(APSD)

The following table describes the labels in this screen.

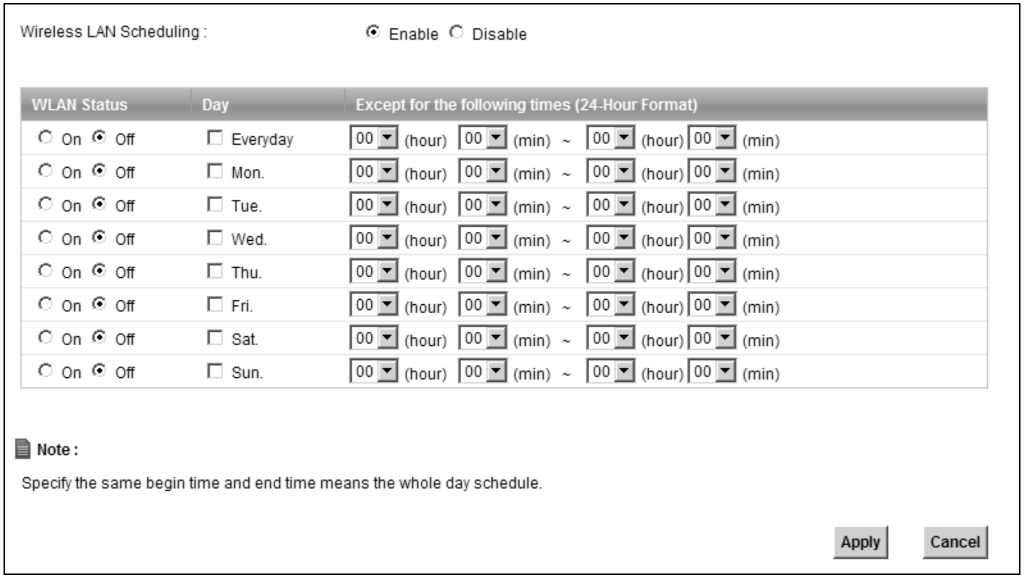
Table 16 Network Setting > Wireless > WMM

LABEL	DESCRIPTION
Enable WMM of SSID1~4	This enables the ZyXEL Device to automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly.
Enable WMM Automatic Power Save Deliver (APSD)	Click this to increase battery life for battery-powered wireless clients. APSD uses a longer beacon interval when transmitting traffic that does not require a short packet exchange interval.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

6.6 Scheduling Screen

Click **Network Setting > Wireless > Scheduling** to open the **Wireless LAN Scheduling** screen. Use this screen to configure when the ZyXEL Device enables or disables the wireless LAN.

Figure 27 Network Setting > Wireless > Scheduling



Wireless LAN Scheduling : ● Enable ○ Disable

WLAN Status	Day	Except for the following times (24-Hour Format)
○ On ● Off	□ Everyday	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
○ On ● Off	□ Mon.	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
○ On ● Off	□ Tue.	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
○ On ● Off	□ Wed.	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
○ On ● Off	□ Thu.	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
○ On ● Off	□ Fri.	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
○ On ● Off	□ Sat.	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
○ On ● Off	□ Sun.	00 (hour) 00 (min) ~ 00 (hour) 00 (min)

Note :

Specify the same begin time and end time means the whole day schedule.

The following table describes the labels in this screen.

Table 17 Network Setting > Wireless > Scheduling

LABEL	DESCRIPTION
Wireless LAN Scheduling	Select **Enable** to activate wireless LAN scheduling on your ZyXEL Device.
WLAN status	Select **On** or **Off** to enable or disable the wireless LAN.
Day	Select the day(s) you want to turn the wireless LAN on or off.
Except for the following times	Specify the time period during which to apply the schedule. For example, you want the wireless network to be only available during work hours. Check Mon ~ Fri in the day column, and specify 8:00 ~ 18:00 in the time table.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

6.7 Technical Reference

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

6.7.1 Additional Wireless Terms

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

Table 18 Additional Wireless Terms

TERM	DESCRIPTION
RTS/CTS Threshold	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. 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. 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.
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.

6.7.2 Wireless Security Overview

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

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

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

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

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

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

6.7.2.1 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.

6.7.2.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; 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.

[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.

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.

6.7.2.3 User Authentication

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

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

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

6.7.2.4 Encryption

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

The types of encryption you can choose depend on the type of authentication. (See Section 6.7.2.3 on page 100 for information about this.)

Table 19 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.

6.7.3 Signal Problems

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

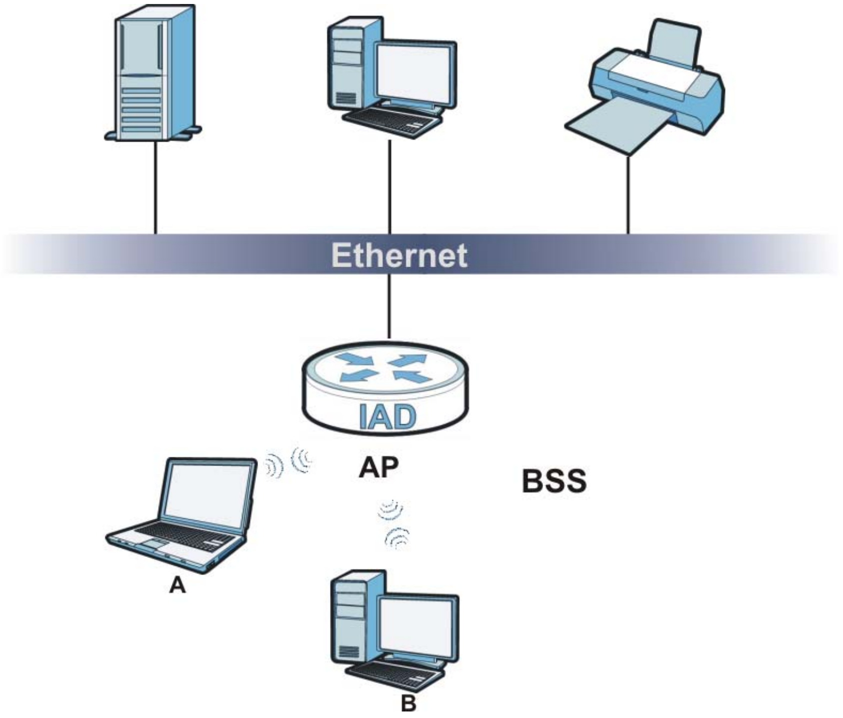
Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters 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.

6.7.4 BSS

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

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

Figure 28 Basic Service set



6.7.5 MBSSID

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

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

6.7.5.1 Notes on Multiple BSSs

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

6.7.6 WiFi Protected Setup (WPS)

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

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

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

6.7.6.1 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 6.4 on page 93).

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.

6.7.6.2 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.

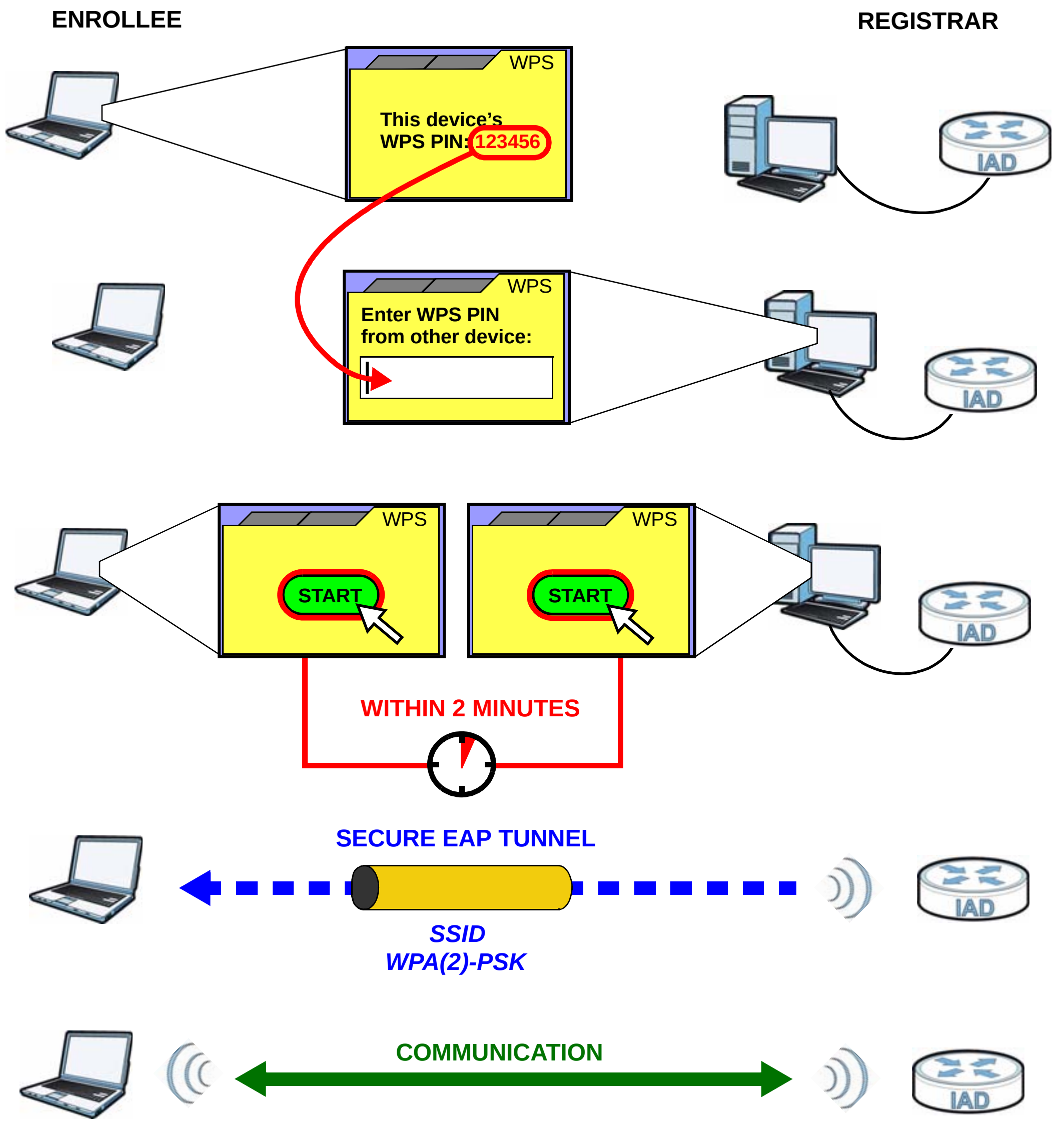
Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

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 6.4 on page 93).
4. Enter the client's PIN in the AP's configuration interface.
5. If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client - it does not matter which.
6. Start WPS on both devices within two minutes.
7. Use the configuration utility to activate WPS, not the push-button on the device itself.
8. On a computer connected to the wireless client, try to connect to the Internet. If you can connect, WPS was successful.

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

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

Figure 29 Example WPS Process: PIN Method

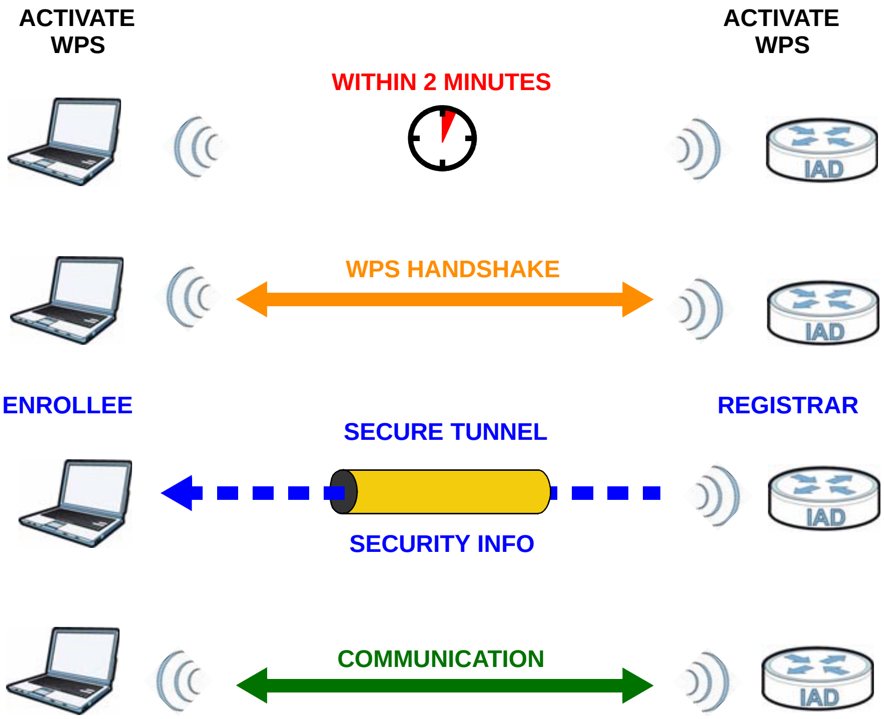


6.7.6.3 How WPS Works

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 30 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.

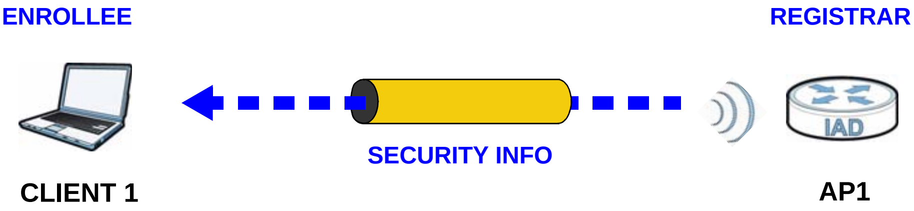
By default, a WPS devices is “unconfigured”. This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled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

6.7.6.4 Example WPS Network Setup

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

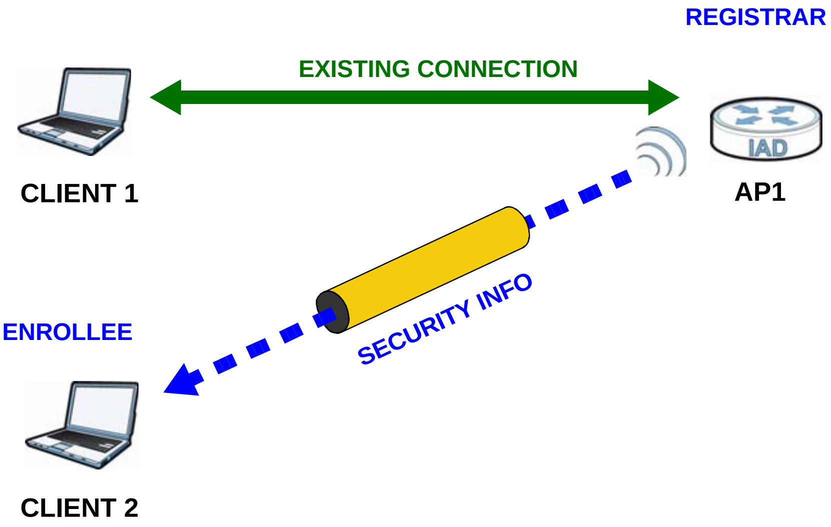
The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information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

Figure 31 WPS: Example Network Step 1



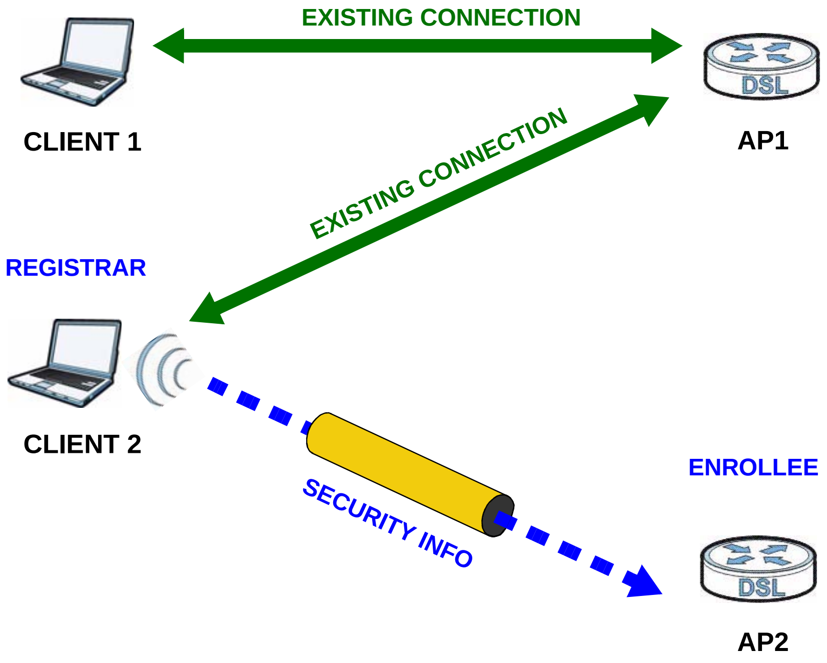
In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the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

Figure 32 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 33 WPS: Example Network Step 3



6.7.6.5 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.

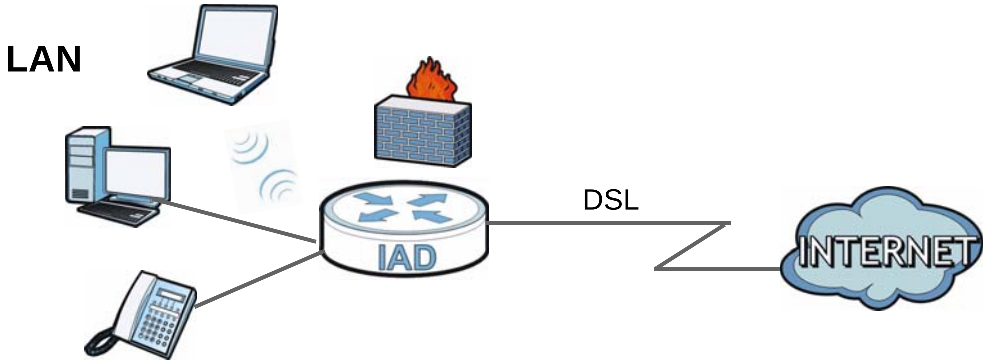
7

Home Networking

7.1 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.



7.1.1 What You Can Do in this Chapter

- Use the **LAN IP** screen to set the LAN IP address, subnet mask, and DHCP settings (Section 7.2 on page 113).
- Use the **DHCP Server** screen to configure the DNS server information that the ZyXEL Device sends to the DHCP client devices on the LAN (Section 7.3 on page 114).
- Use the **UPnP** screen to enable UPnP (Section 7.4 on page 116).

7.1.2 What You Need To Know

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

7.1.2.1 About LAN

IP Address

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

Subnet Mask

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

DHCP

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

DNS

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

7.1.2.2 About UPnP

How do I know if I'm using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows 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.

Cautions with UPnP

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

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

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

UPnP and ZyXEL

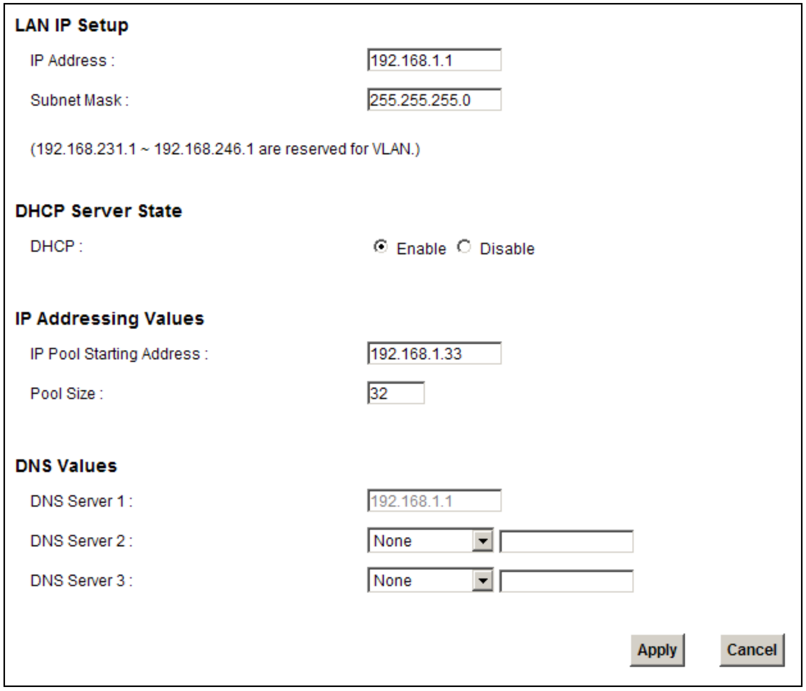
ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports Internet Gateway Device (IGD) 1.0.

See Section 7.6 on page 119 for examples of installing and using UPnP.

7.2 The LAN Setup Screen

Click **Network Setting > Home Networking** to open the **LAN Setup** screen. Use this screen to set the Local Area Network IP address and subnet mask of your ZyXEL Device and configure the DNS server information that the ZyXEL Device sends to the DHCP client devices on the LAN.

Figure 34 Network Setting > Home Networking > LAN Setup



LAN IP Setup

IP Address : 192.168.1.1

Subnet Mask : 255.255.255.0

(192.168.231.1 ~ 192.168.246.1 are reserved for VLAN.)

DHCP Server State

DHCP : ● Enable ○ Disable

IP Addressing Values

IP Pool Starting Address : 192.168.1.33

Pool Size : 32

DNS Values

DNS Server 1 : 192.168.1.1

DNS Server 2 : None

DNS Server 3 : None

The following table describes the fields in this screen.

Table 20 Network Setting > Home Networking > LAN Setup

LABEL	DESCRIPTION
LAN IP Setup	
IP Address	Enter the LAN IP address you want to assign to your ZyXEL Device in dotted decimal notation, for example, 192.168.1.1 (factory default).
IP Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your ZyXEL Device automatically computes the subnet mask based on the IP address you enter, so do not change this field unless you are instructed to do so.
DHCP Server State	
DHCP	Select **Enable** to have your ZyXEL Device assign IP addresses, an IP default gateway and DNS servers to LAN computers and other devices that are DHCP clients. If you select **Disable**, you need to manually configure the IP addresses of the computers and other devices on your LAN. When DHCP is used, the following fields need to be set.
IP Addressing Values	
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.
DNS Values	
DNS Server 1-3	Select **From ISP** if your ISP dynamically assigns DNS server information (and the ZyXEL Device's WAN IP address). Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. You must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

7.3 The Static DHCP Screen

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

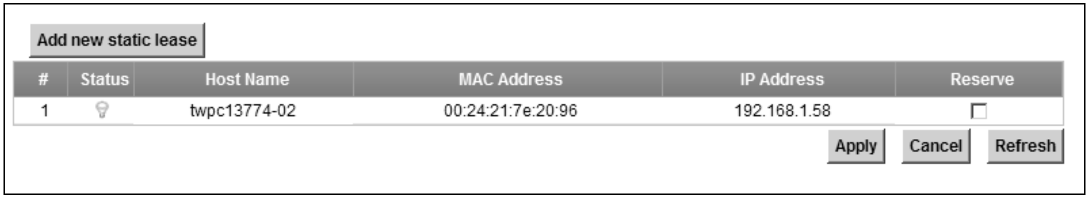
Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

7.3.1 Before You Begin

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

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

Figure 35 Network Setting > Home Networking > Static DHCP



#	Status	Host Name	MAC Address	IP Address	Reserve
1	💡	twpc13774-02	00:24:21:7e:20:96	192.168.1.58	□

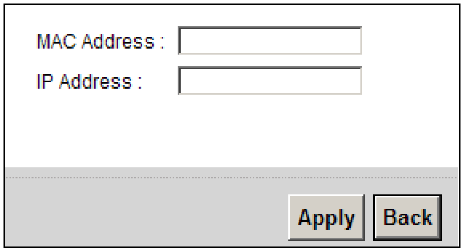
The following table describes the labels in this screen.

Table 21 Network Setting > Home Networking > Static DHCP

LABEL	DESCRIPTION
Add new static lease	Click this to add a new static DHCP entry.
#	This is the index number of the entry.
Status	This field displays whether the client is connected to the ZyXEL Device.
Host Name	This field displays the client host name.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
IP Address	This field displays the IP address relative to the # field listed above.
Reserve	Select the check box in the heading row to automatically select all check boxes or select the check box(es) in each entry to have the ZyXEL Device always assign the selected entry(ies)’s IP address(es) to the corresponding MAC address(es) (and host name(s)). You can select up to 128 entries in this table.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.
Refresh	Click **Refresh** to reload the DHCP table.

If you click **Add new static lease** in the **Static DHCP** screen, the following screen displays.

Figure 36 Static DHCP: Add



The following table describes the labels in this screen.

Table 22 Static DHCP: Add

LABEL	DESCRIPTION
MAC Address	Enter the MAC address of a computer on your LAN.
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.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to exit this screen without saving.

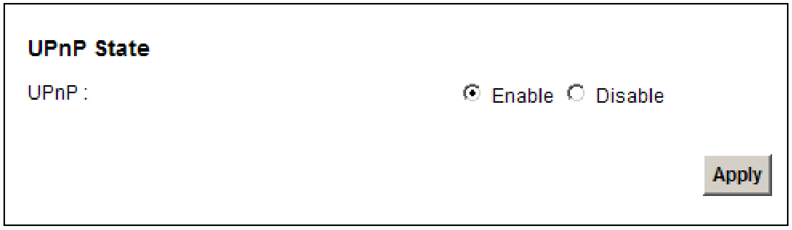
7.4 The UPnP Screen

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between 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.

See page 119 for more information on UPnP.

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

Figure 37 Network Setting > Home Networking > UPnP



UPnP : ● Enable ○ Disable

The following table describes the labels in this screen.

Table 23 Network Settings > Home Networking > UPnP

LABEL	DESCRIPTION
UPnP	Select **Enable** to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the ZyXEL Device's IP address (although you must still enter the password to access the web configurator).
Apply	Click **Apply** to save your changes.

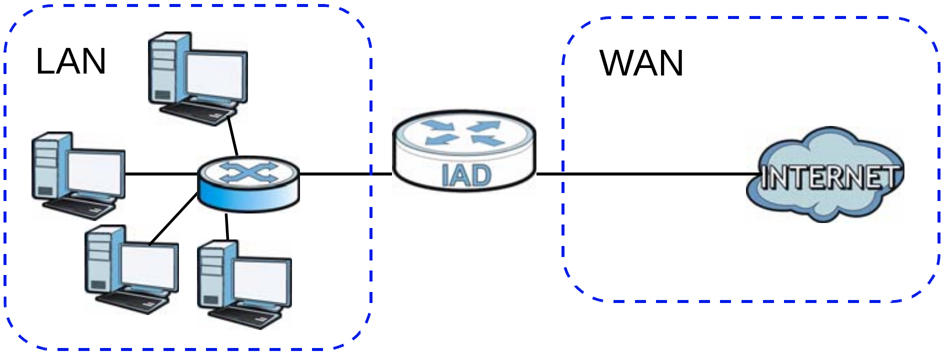
7.5 Technical Reference

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

LANs, WANs and the ZyXEL Device

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

Figure 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”.

7.6 Installing UPnP in Windows Example

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

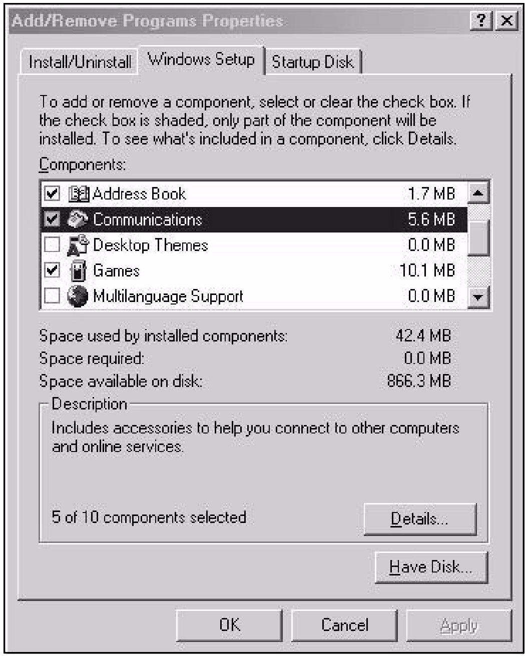
Installing UPnP in Windows Me

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

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

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

Figure 39 Add/Remove Programs: Windows Setup: Communication



To add or remove a component, select or clear the check box. If the check box is shaded, only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑ Address Book	1.7 MB
☑ Communications	5.6 MB
□ Desktop Themes	0.0 MB
☑ Games	10.1 MB
□ Multilanguage Support	0.0 MB

Space used by installed components:	42.4 MB
Space required:	0.0 MB
Space available on disk:	866.3 MB

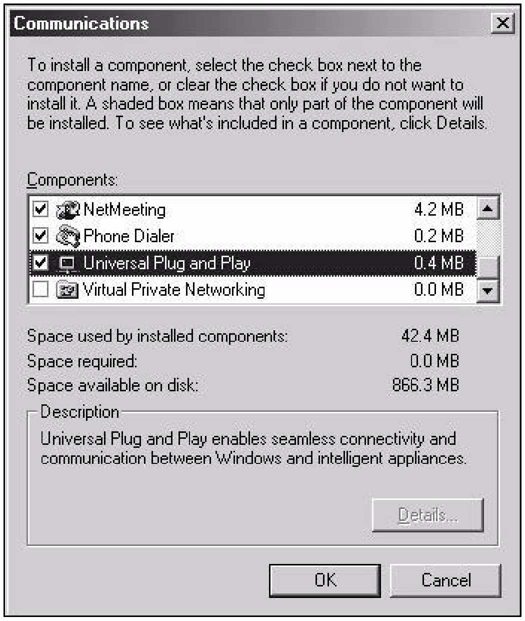
Description

Includes accessories to help you connect to other computers and online services.

5 of 10 components selected

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

Figure 40 Add/Remove Programs: Windows Setup: Communication: Components



To install a component, select the check box next to the component name, or clear the check box if you do not want to install it. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑ NetMeeting	4.2 MB
☑ Phone Dialer	0.2 MB
☑ Universal Plug and Play	0.4 MB
□ Virtual Private Networking	0.0 MB

Space used by installed components:	42.4 MB
Space required:	0.0 MB
Space available on disk:	866.3 MB

Description

Universal Plug and Play enables seamless connectivity and communication between Windows and intelligent appliances.

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

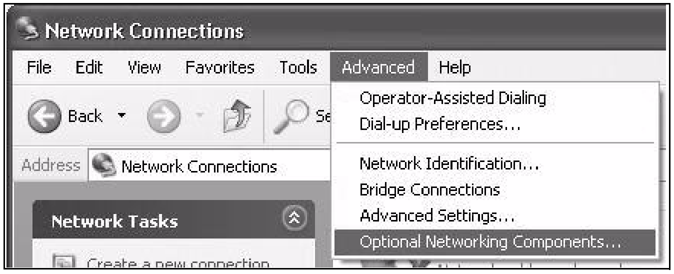
Follow the steps below to install the UPnP in Windows XP.

1 Click **Start** and **Control Panel**.

2 Double-click **Network Connections**.

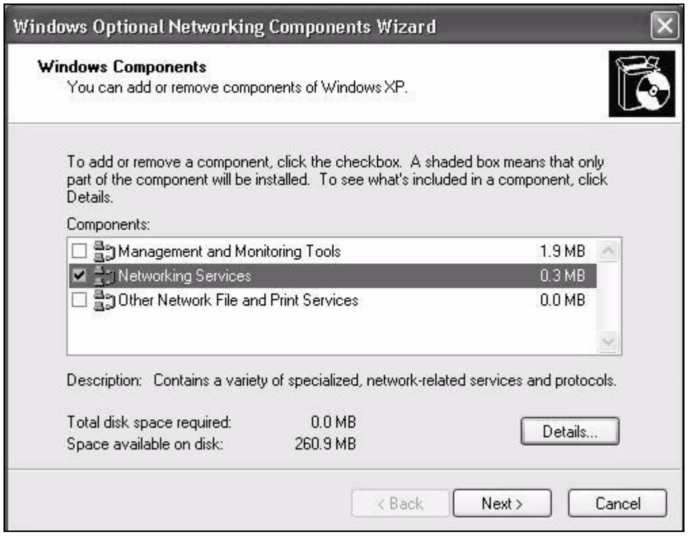
3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ...**.

Figure 41 Network Connections



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

Figure 42 Windows Optional Networking Components Wizard



Windows Components

You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☐	Management and Monitoring Tools	1.9 MB
☑	Networking Services	0.3 MB
☐	Other Network File and Print Services	0.0 MB

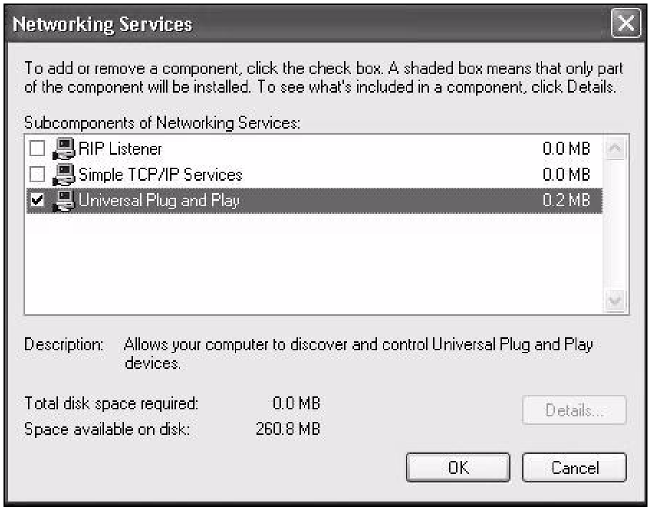
Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 0.0 MB

Space available on disk: 260.9 MB

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

Figure 43 Networking Services



Networking Services

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

☐	RIP Listener	0.0 MB
☐	Simple TCP/IP Services	0.0 MB
☑	Universal Plug and Play	0.2 MB

Description: Allows your computer to discover and control Universal Plug and Play devices.

Total disk space required: 0.0 MB

Space available on disk: 260.8 MB

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

7.7 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.

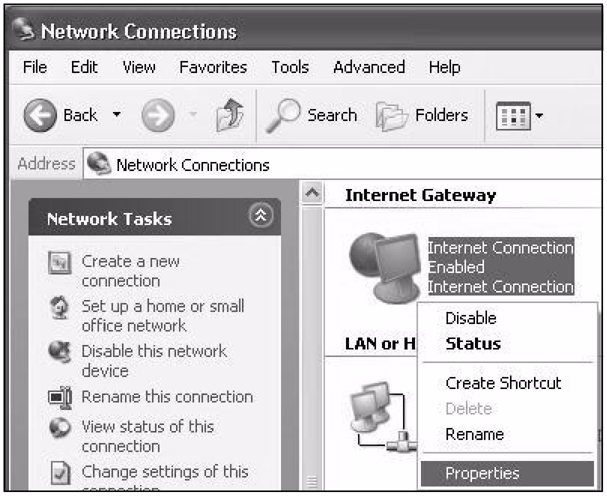
Make sure the computer is connected to a LAN port of the ZyXEL Device. Turn on your computer and the ZyXEL Device.

Auto-discover Your UPnP-enabled Network Device

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

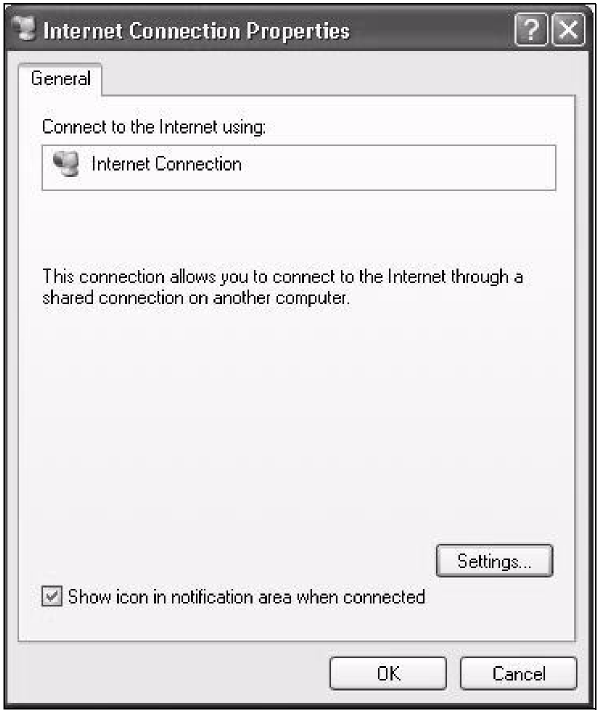
2 Right-click the icon and select **Properties**.

Figure 44 Network Connections



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

Figure 45 Internet Connection Properties



Connect to the Internet using:

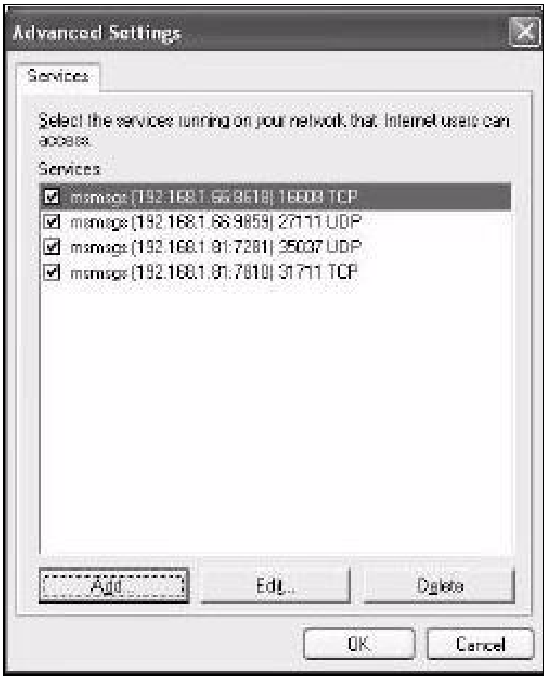
Internet Connection

This connection allows you to connect to the Internet through a shared connection on another computer.

☑ Show icon in notification area when connected

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

Figure 46 Internet Connection Properties: Advanced Settings

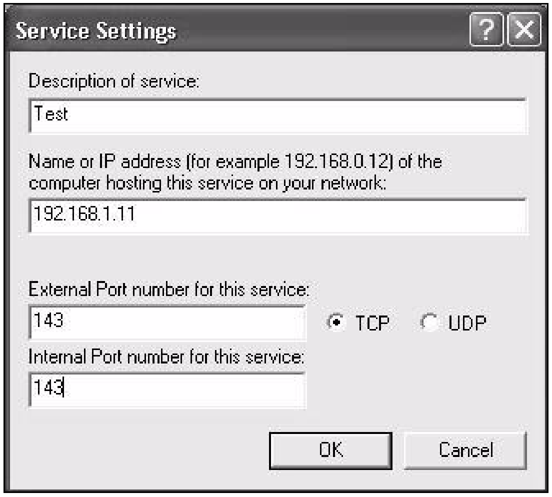


Select the services running on your network that Internet users can access.

Services

☑ msmsgs (192.168.1.66:9618) 16608 TCP
☑ msmsgs (192.168.1.66:9859) 27111 UDP
☑ msmsgs (192.168.1.81:7281) 35037 UDP
☑ msmsgs (192.168.1.81:7810) 31711 TCP

Figure 47 Internet Connection Properties: Advanced Settings: Add



Description of service:
Test

Name or IP address (for example 192.168.0.12) of the computer hosting this service on your network:
192.168.1.11

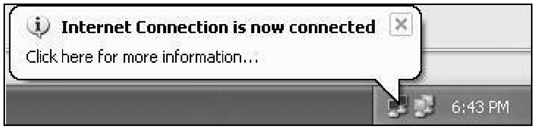
External Port number for this service:
143 ● TCP ○ UDP

Internal Port number for this service:
143

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.

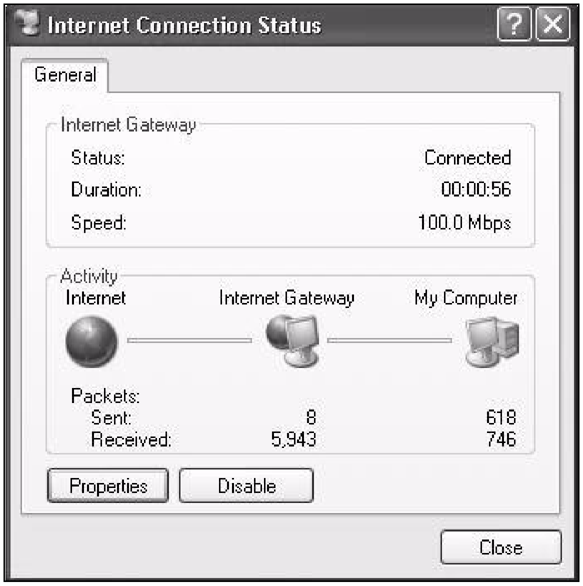
Figure 48 System Tray Icon



Internet Connection is now connected
Click here for more information...

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

Figure 49 Internet Connection Status



Internet Gateway

Status: Connected
Duration: 00:00:56
Speed: 100.0 Mbps

Packets:	Internet Gateway	My Computer
Sent:	8	618
Received:	5,943	746

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.

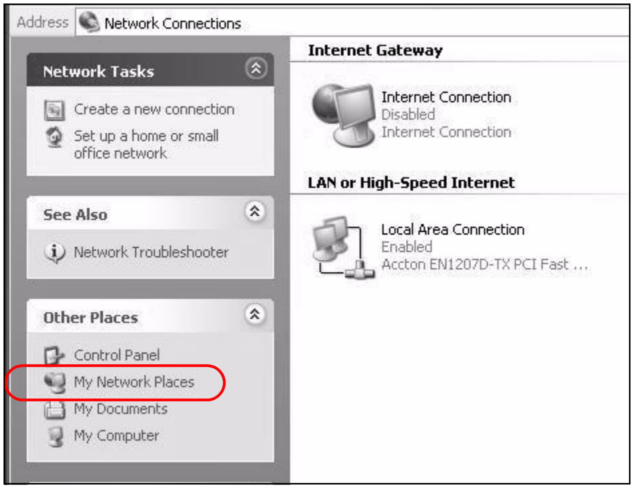
Follow the steps below to access the web configurator.

1 Click **Start** and then **Control Panel**.

2 Double-click **Network Connections**.

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

Figure 50 Network Connections



Internet Gateway

Internet Connection
Disabled
Internet Connection

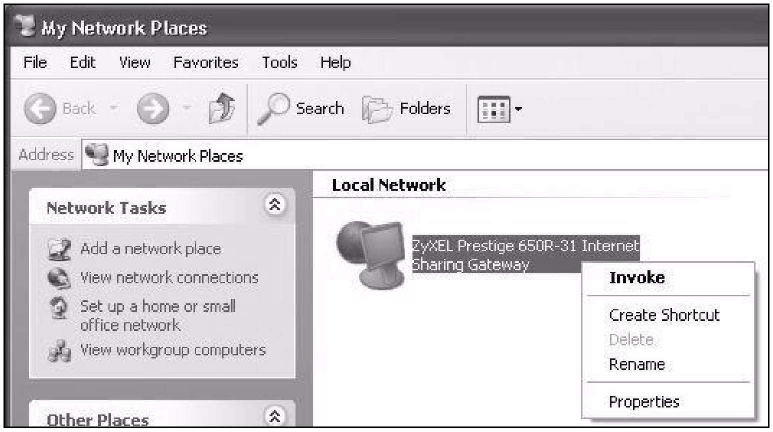
LAN or High-Speed Internet

Local Area Connection
Enabled
Accton EN1207D-TX PCI Fast ...

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

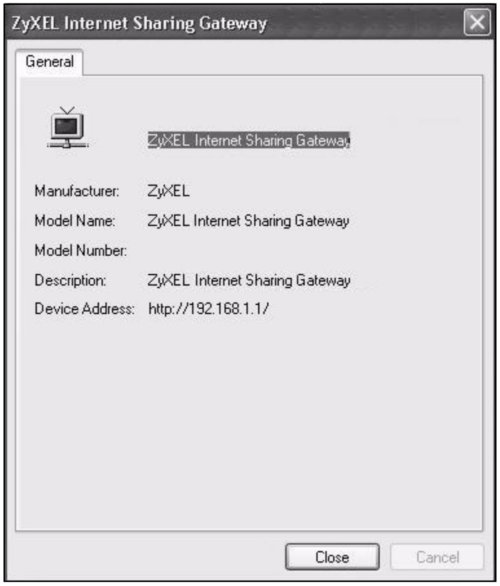
5 Right-click on the icon for your ZyXEL Device and select **Invoke**. The web configurator login screen displays.

Figure 51 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 52 Network Connections: My Network Places: Properties: Example



ZyXEL Internet Sharing Gateway

Manufacturer: ZyXEL

Model Name: ZyXEL Internet Sharing Gateway

Model Number:

Description: ZyXEL Internet Sharing Gateway

Device Address: http://192.168.1.1/

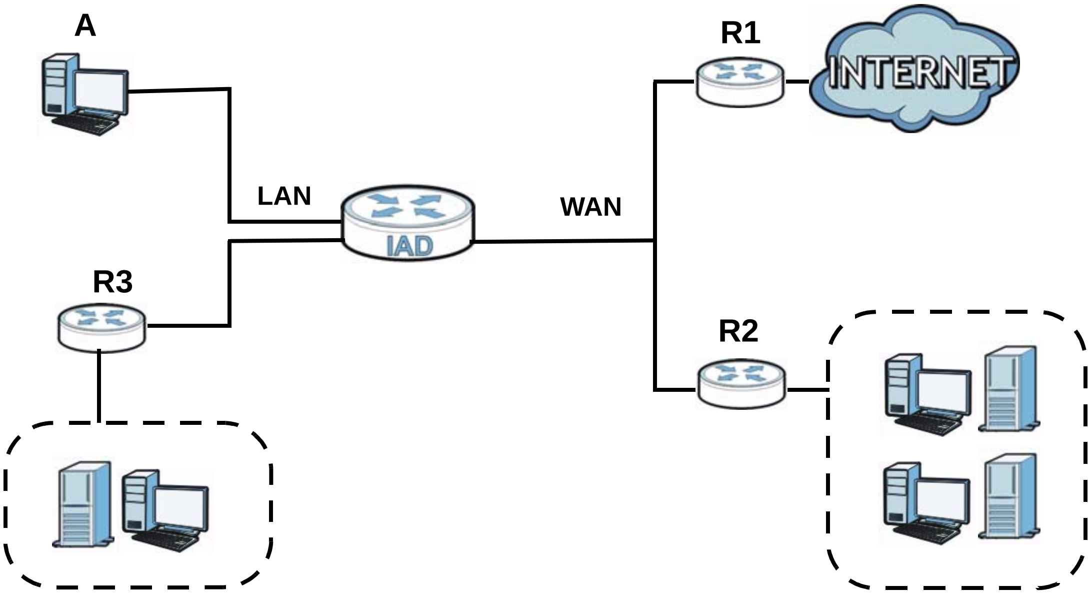
Routing

8.1 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.

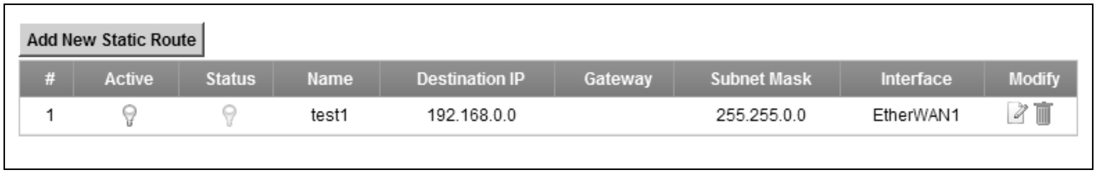
Figure 53 Example of Static Routing Topology



8.2 Configuring Static Route

Use this screen to view and configure IP static routes on the ZyXEL Device. Click **Network Setting > Routing** to open the following screen.

Figure 54 Network Setting > Routing



#	Active	Status	Name	Destination IP	Gateway	Subnet Mask	Interface	Modify
1			test1	192.168.0.0		255.255.0.0	EtherWAN1	

The following table describes the labels in this screen.

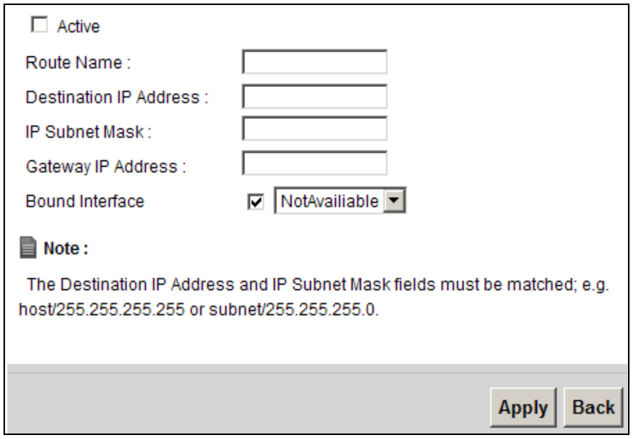
Table 24 Network Setting > Routing

LABEL	DESCRIPTION
Add New Static Route	Click this to set up a new static route on the ZyXEL Device.
#	This is the number of an individual static route.
Active	This indicates whether the rule is active or not. A yellow bulb signifies that this static route is active. A gray bulb signifies that this static route is not active.
Status	This shows whether the static route is currently in use or not. A yellow bulb signifies that this static route is in use. A gray bulb signifies that this static route is not in use.
Name	This is the name that describes or identifies this route.
Destination IP	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
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.
Subnet Mask	This parameter specifies the IP network subnet mask of the final destination.
Interface	This is the WAN interface through which the traffic is routed.
Modify	Click the **Edit** icon to go to the screen where you can set up a static route on the ZyXEL Device. Click the **Delete** icon to remove a static route from the ZyXEL Device.

8.2.1 Add/Edit Static Route

Click **add new Static Route** in the **Routing** screen or click the **Edit** icon next to a rule. The following screen appears. Use this screen to configure the required information for a static route.

Figure 55 Routing: Add/Edit



□ Active

Route Name :	
Destination IP Address :	
IP Subnet Mask :	
Gateway IP Address :	
Bound Interface	☑ NotAvailiable

Note :

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

The following table describes the labels in this screen.

Table 25 Routing: Add/Edit

LABEL	DESCRIPTION
Active	Click this to activate this static route.
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
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.
Gateway IP Address	You can decide if you want to forward packets to a gateway IP address or a bound interface. If you want to configure **Gateway IP Address**, enter the IP address of the next-hop gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Bound Interface	You can decide if you want to forward packets to a gateway IP address or a bound interface. If you want to configure **Bound Interface**, select the check box and choose an interface through which the traffic is sent. You must have the WAN interface(s) already configured in the **Broadband** screen.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to exit this screen without saving.

9

DNS Route

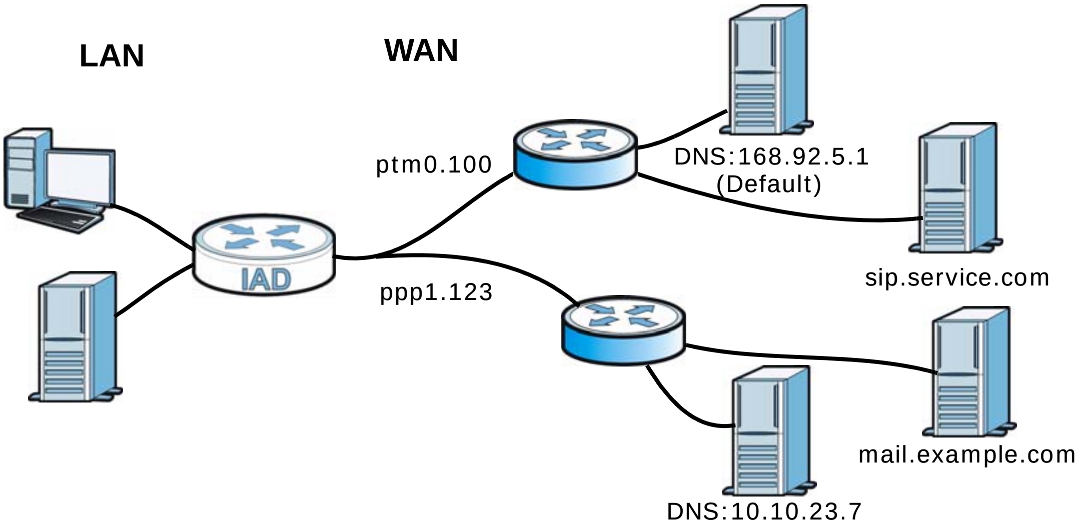
9.1 Overview

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

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

In the following example, the DNS server 168.92.5.1 obtained from the WAN interface ptm0.100 is set to be the system DNS server. The DNS server 10.10.23.7 is obtained from the WAN interface ppp1.123. You configure a DNS route for *example.com to have the ZyXEL Device forward DNS requests for the domain name mail.example.com through the WAN interface ppp1.123 to the DNS server 10.10.23.7.

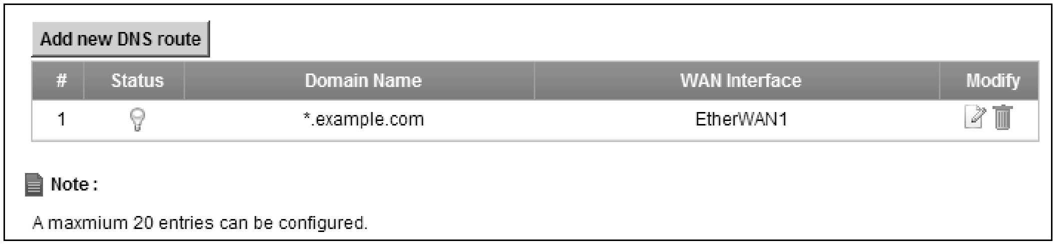
Figure 56 Example of DNS Routing Topology



9.2 The DNS Route Screen

The **DNS Route** screens let you view and configure DNS routes on the ZyXEL Device. Click **Network Setting > DNS Route** to open the **DNS Route** screen.

Figure 57 Network Setting > DNS Route



Add new DNS route

#	Status	Domain Name	WAN Interface	Modify
1	💡	*.example.com	EtherWAN1	✎ 🗑

Note :

A maxmium 20 entries can be configured.

The following table describes the labels in this screen.

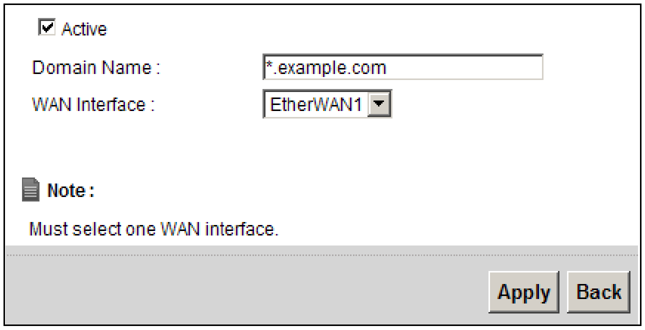
Table 26 Network Setting > DNS Route

LABEL	DESCRIPTION
Add new DNS route	Click this to create a new entry.
#	This is the number of an individual DNS route.
Status	This shows whether the DNS route is currently in use or not. A yellow bulb signifies that this DNS route is in use. A gray bulb signifies that this DNS route is not in use.
Domain Name	This is the domain name to which the DNS route applies.
WAN Interface	This is the WAN interface through which the matched DNS request is routed.
Modify	Click the **Edit** icon to configure a DNS route on the ZyXEL Device. Click the **Delete** icon to remove a DNS route from the ZyXEL Device.

9.2.1 Add/Edit DNS Route Edit

Click **Add new DNS route** in the **DNS Route** screen or the **Edit** icon next to an existing DNS route. Use this screen to configure the required information for a DNS route.

Figure 58 DNS Route: Add/Edit



☑ Active

Domain Name : *.example.com

WAN Interface : EtherWAN1

Note :

Must select one WAN interface.

The following table describes the labels in this screen.

Table 27 DNS Route: Add/Edit

LABEL	DESCRIPTION
Active	Select this to activate this DNS route.
Domain Name	Enter the domain name you want to resolve. You can use the wildcard character, an "*" (asterisk) as the left most part of a domain name, such as *.example.com. The ZyXEL Device forwards DNS queries for any domain name ending in example.com to the WAN interface specified in this route.
WAN Interface	Select a WAN interface through which the matched DNS query is sent. You must have the WAN interface(s) already configured in the **Broadband** screen.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to exit this screen without saving.

10

Quality of Service (QoS)

10.1 Overview

This chapter discusses the ZyXEL Device's **QoS** screens. Use these screens to set up your ZyXEL Device to use QoS for traffic management.

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. QoS allows the ZyXEL Device to group and prioritize application traffic and fine-tune network performance.

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.

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 Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video.

Note: The ZyXEL Device has built-in configurations for Voice over IP (IP). The Quality of Service (QoS) feature does not affect VoIP traffic.

- See Section 10.6 on page 146 for advanced technical information on SIP.

10.1.1 What You Can Do in this Chapter

- Use the **General** screen to enable QoS, set the bandwidth, and allow the ZyXEL Device to automatically assign priority to upstream traffic according to the IEEE 802.1p priority level, IP precedence or packet length (Section 10.2 on page 136).
- Use the **Queue Setup** screen to configure QoS queue assignment (Section 10.3 on page 138).

- Use the **Class Setup** screen to set up classifiers to sort traffic into different flows and assign priority and define actions to be performed for a classified traffic flow (Section 10.4 on page 140).
- Use the **Monitor** screen to view the ZyXEL Device's QoS-related packet statistics (Section 10.5 on page 145).

10.1.2 What You Need to Know

The following terms and concepts may help as you read 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

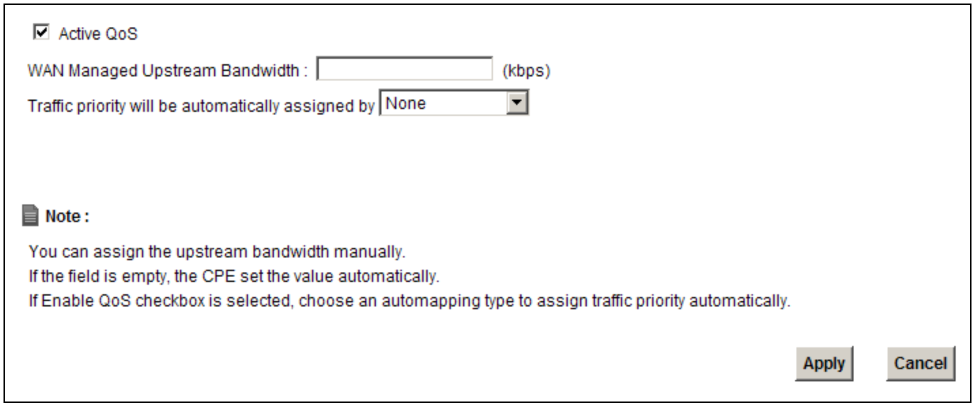
In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or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

10.2 The QoS General Screen

Use this screen to enable or disable QoS, set the bandwidth, and select to have the ZyXEL Device automatically assign priority to upstream traffic according to the IEEE 802.1p priority level, IP precedence or packet length.

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

Figure 59 Network Setting > QoS > General



☑ Active QoS

WAN Managed Upstream Bandwidth : [ ] (kbps)

Traffic priority will be automatically assigned by None

Note :

You can assign the upstream bandwidth manually.
If the field is empty, the CPE set the value automatically.
If Enable QoS checkbox is selected, choose an automapping type to assign traffic priority automatically.

The following table describes the labels in this screen.

Table 28 Network Setting > QoS > General

LABEL	DESCRIPTION
Active QoS	Select the check box to turn on QoS to improve your network performance. You can give priority 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.
WAN Managed Upstream Bandwidth	Enter the amount of bandwidth for the WAN interface that you want to allocate using QoS. The recommendation is to set this speed to match the interface's actual transmission speed. For example, set the WAN interface speed to 100000 kbps if your Internet connection has an upstream transmission speed of 100 Mbps. Setting this number higher than the interface's actual transmission speed will stop lower priority traffic from being sent if higher priority traffic uses all of the actual bandwidth. If you set this number lower than the interface's actual transmission speed, the ZyXEL Device will not use some of the interface's available bandwidth. Leave this field blank to have the ZyXEL Device set this value automatically.
Traffic priority will be automatically assigned by	These fields are ignored if upstream traffic matches a class you configured in the **Class Setup** screen. If you select **Ethernet Priority**, **IP Precedence** or **Packet Length** and traffic does not match a class configured in the **Class Setup** screen, the ZyXEL Device assigns priority to unmatched traffic based on the IEEE 802.1p priority level, IP precedence or packet length. See Section 10.6.1 on page 146 for more information.

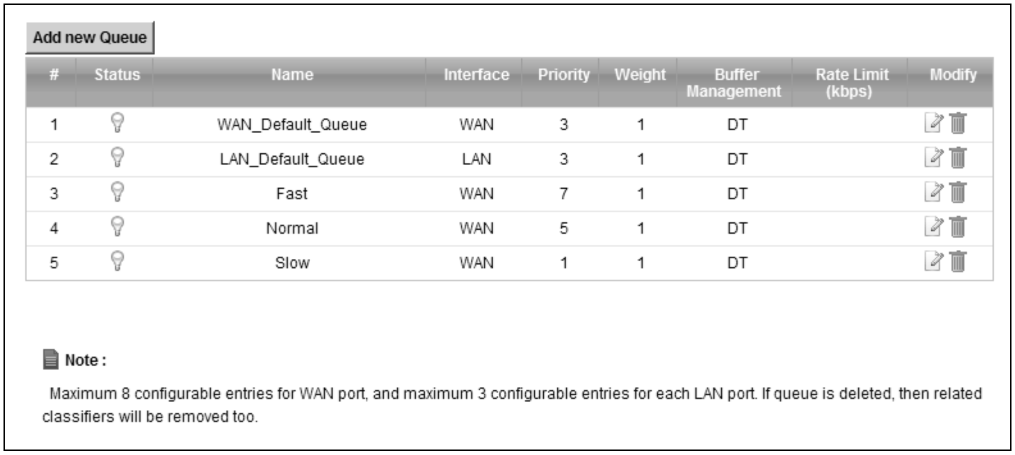
Table 28 Network Setting > QoS > General (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

10.3 The Queue Setup Screen

Use this screen to configure QoS queue assignment. Click **Network Setting > QoS > Queue Setup** to open the screen as shown next.

Figure 60 Network Setting > QoS > Queue Setup



Add new Queue

#	Status	Name	Interface	Priority	Weight	Buffer Management	Rate Limit (kbps)	Modify
1	💡	WAN_Default_Queue	WAN	3	1	DT		✎ 🗑
2	💡	LAN_Default_Queue	LAN	3	1	DT		✎ 🗑
3	💡	Fast	WAN	7	1	DT		✎ 🗑
4	💡	Normal	WAN	5	1	DT		✎ 🗑
5	💡	Slow	WAN	1	1	DT		✎ 🗑

Note :

Maximum 8 configurable entries for WAN port, and maximum 3 configurable entries for each LAN port. If queue is deleted, then related classifiers will be removed too.

The following table describes the labels in this screen.

Table 29 Network Setting > QoS > Queue Setup

LABEL	DESCRIPTION
Add new Queue	Click this to create a new entry.
#	This is the index number of this entry.
Status	This shows whether the queue is activated or not. A yellow bulb signifies that this queue is activated. A gray bulb signifies that this queue is not activated.
Name	This shows the descriptive name of this queue.
Interface	This shows the name of the ZyXEL Device's interface through which traffic in this queue passes.
Priority	This shows the priority of this queue.
Weight	This shows the weight of this queue.
Buffer Management	This shows the queue management algorithm used by the ZyXEL Device.
Rate Limit (kbps)	This shows the maximum transmission rate allowed for traffic on this queue.

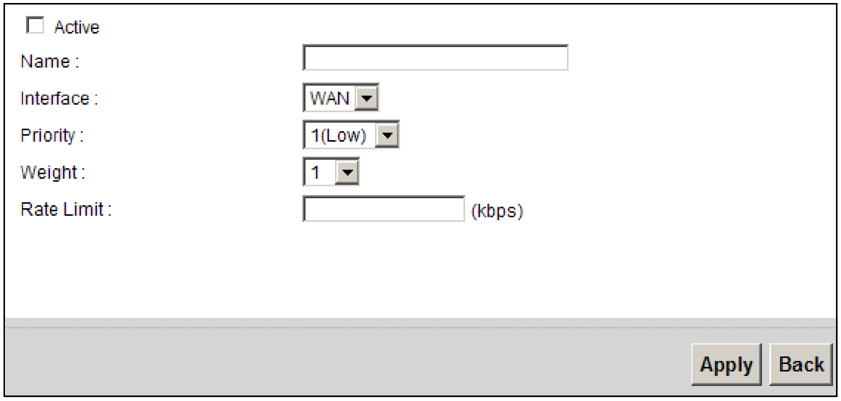
Table 29 Network Setting > QoS > Queue Setup (continued)

LABEL	DESCRIPTION
Modify	Click the **Edit** icon to edit the queue. Click the **Delete** icon to delete an existing queue. Note that subsequent rules move up by one when you take this action.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

10.3.1 Add/Edit a QoS Queue

Use this screen to configure a queue. Click **Add new queue** in the **Queue Setup** screen or the **Edit** icon next to an existing queue.

Figure 61 Queue Setup: Add/Edit



☐ Active

Name :	
Interface :	WAN
Priority :	1(Low)
Weight :	1
Rate Limit :	(kbps)

The following table describes the labels in this screen.

Table 30 Queue Setup: Add/Edit

LABEL	DESCRIPTION
Active	Select to enable or disable this queue.
Name	Enter the descriptive name of this queue.
Interface	Select the interface to which this queue is applied.
Priority	Select the priority level (from 1 to 7) of this queue. The larger the number, the higher the priority level. Traffic assigned to higher priority queues gets through faster while traffic in lower priority queues is dropped if the network is congested.
Weight	Select the weight (from 1 to 15) of this queue. If two queues have the same priority level, the ZyXEL Device divides the bandwidth across the queues according to their weights. Queues with larger weights get more bandwidth than queues with smaller weights.
Rate Limit	Specify the maximum transmission rate (in Kbps) allowed for traffic on this queue.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen without saving.

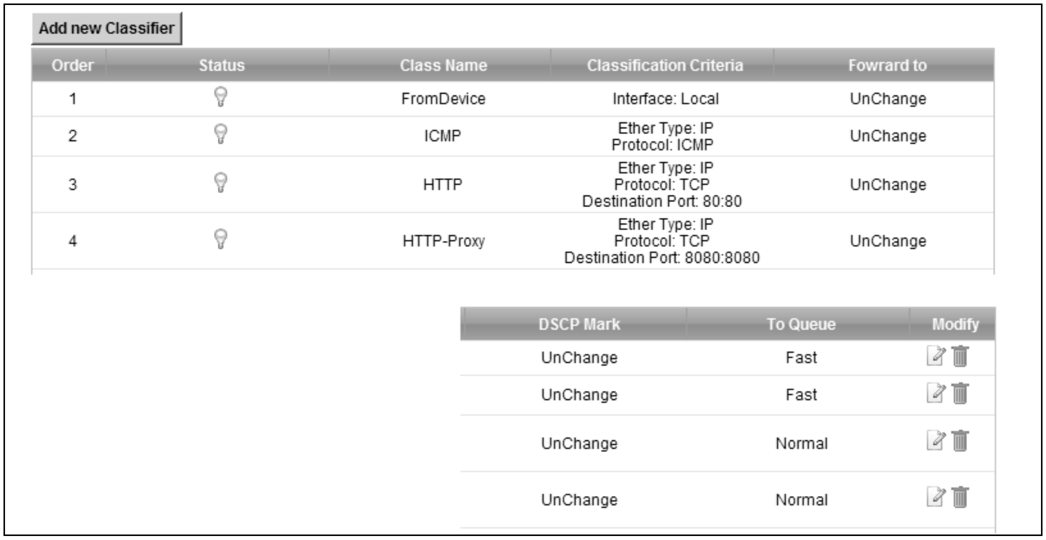
10.4 The Class Setup Screen

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 **Network Setting > QoS > Class Setup** to open the following screen.

Figure 62 Network Setting > QoS > Class Setup



Order	Status	Class Name	Classification Criteria	Fowrard to
1	💡	FromDevice	Interface: Local	UnChange
2	💡	ICMP	Ether Type: IP Protocol: ICMP	UnChange
3	💡	HTTP	Ether Type: IP Protocol: TCP Destination Port: 80:80	UnChange
4	💡	HTTP-Proxy	Ether Type: IP Protocol: TCP Destination Port: 8080:8080	UnChange

DSCP Mark	To Queue	Modify
UnChange	Fast	✎ 🗑
UnChange	Fast	✎ 🗑
UnChange	Normal	✎ 🗑
UnChange	Normal	✎ 🗑

The following table describes the labels in this screen.

Table 31 Network Setting > QoS > Class Setup

LABEL	DESCRIPTION
Add new Classifier	Click this to create a new classifier.
Order	This field displays the order number of the classifier.
Status	This shows whether the classifier is activated or not. A yellow bulb signifies that this classifier is activated. A gray bulb signifies that this classifier is not activated.
Class Name	This is the name of the classifier.
Classification Criteria	This shows criteria specified in this classifier, for example the interface from which traffic of this class should come and the source MAC address of traffic that matches this classifier.

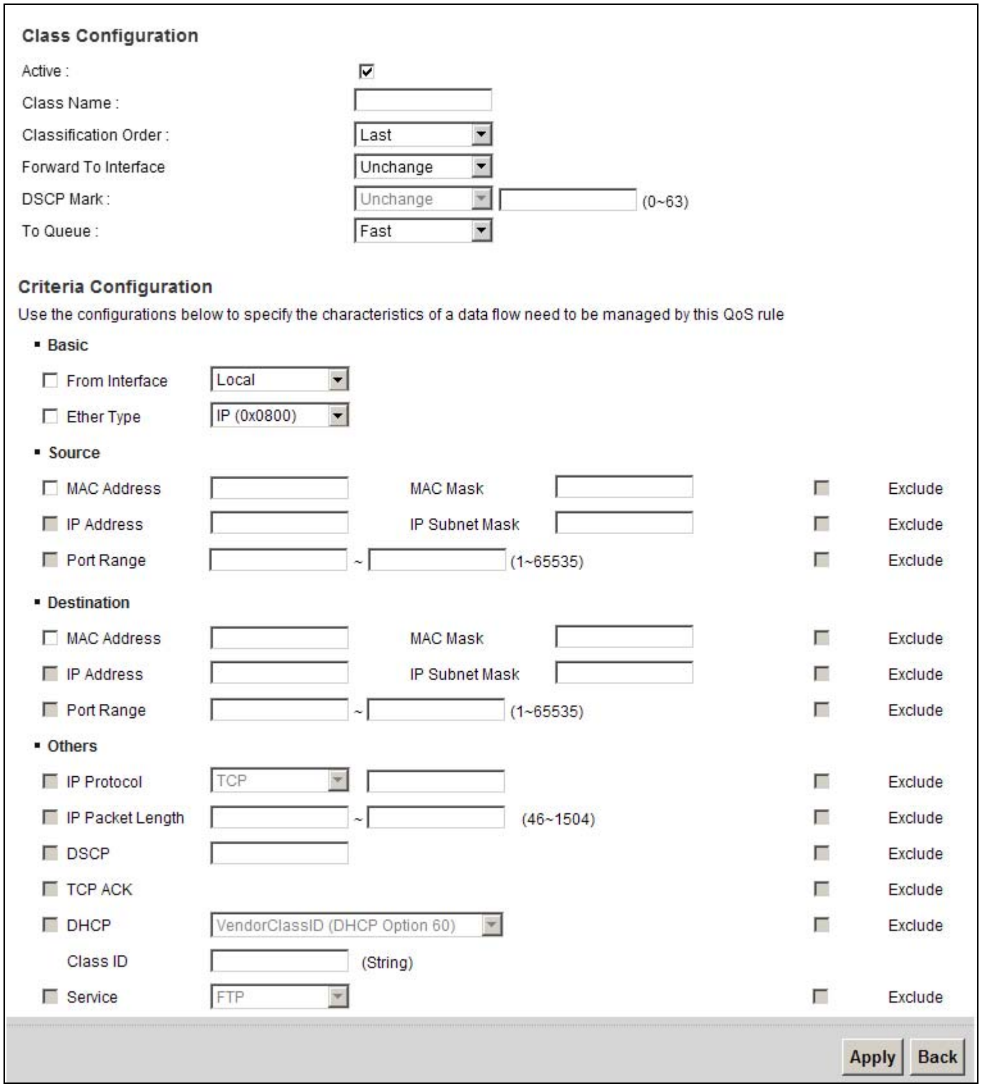
Table 31 Network Setting > QoS > Class Setup (continued)

LABEL	DESCRIPTION
Forward to	This is the interface through which traffic that matches this classifier is forwarded out.
DSCP Mark	This is the DSCP number added to traffic of this classifier.
To Queue	This is the name of the queue in which traffic of this classifier is put.
Modify	Click the **Edit** icon to edit the classifier. Click the **Delete** icon to delete an existing classifier. Note that subsequent rules move up by one when you take this action.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

10.4.1 Add/Edit QoS Class

Click **Add new Classifier** in the **Class Setup** screen or the **Edit** icon next to an existing classifier to configure it.

Figure 63 Class Setup: Add/Edit



Class Configuration

Active : ☑

Class Name :

Classification Order : Last

Forward To Interface Unchange

DSCP Mark : Unchange (0~63)

To Queue : Fast

Criteria Configuration

Use the configurations below to specify the characteristics of a data flow need to be managed by this QoS rule

- Basic

☐ From Interface Local

☐ Ether Type IP (0x0800)

- Source

☐ MAC Address MAC Mask ☐ Exclude

☐ IP Address IP Subnet Mask ☐ Exclude

☐ Port Range ~ (1~65535) ☐ Exclude

- Destination

☐ MAC Address MAC Mask ☐ Exclude

☐ IP Address IP Subnet Mask ☐ Exclude

☐ Port Range ~ (1~65535) ☐ Exclude

- Others

☐ IP Protocol TCP ☐ Exclude

☐ IP Packet Length ~ (46~1504) ☐ Exclude

☐ DSCP ☐ Exclude

☐ TCP ACK ☐ Exclude

☐ DHCP VendorClassID (DHCP Option 60) ☐ Exclude

Class ID (String)

☐ Service FTP ☐ Exclude

The following table describes the labels in this screen.

Table 32 Class Setup: Add/Edit

LABEL	DESCRIPTION
Class Configuration	
Active	Select to enable this classifier.
Class Name	Enter a descriptive name of up to 32 printable English keyboard characters, including spaces.

Table 32 Class Setup: Add/Edit (continued)

LABEL	DESCRIPTION
Classification Order	Select an existing number for where you want to put this classifier to move the classifier to the number you selected after clicking **Apply**. Select **Last** to put this rule in the back of the classifier list.
Forward to Interface	Select a WAN interface through which traffic of this class will be forwarded out. If you select **Unchange**, the ZyXEL Device forward traffic of this class according to the default routing table.
DSCP Mark	This field is available only when you select the **Ether Type** check box in **Criteria Configuration-Basic** section. If you select **Mark**, enter a DSCP value with which the ZyXEL Device replaces the DSCP field in the packets. If you select **Unchange**, the ZyXEL Device keep the DSCP field in the packets.
To Queue	Select a queue that applies to this class. You should have configured a queue in the **Queue Setup** screen already.
Criteria Configuration Use the following fields to configure the criteria for traffic classification.	
Basic	
From Interface	Select whether the traffic class comes from the LAN or a wireless interface.
Ether Type	Select a predefined application to configure a class for the matched traffic. If you select **IP**, you also need to configure source or destination MAC address, IP address, DHCP options, DSCP value or the protocol type. If you select **8021Q**, you can configure an 802.1p priority level and VLAN ID in the **Others** section.
Source	
MAC Address	Select the check box and enter the source MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. 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.
IP Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
IP Subnet Mask	Enter the source subnet mask.
Port Range	If you select **TCP** or **UDP** in the **IP Protocol** field, select the check box and enter the port number(s) of the source.

Table 32 Class Setup: Add/Edit (continued)

LABEL	DESCRIPTION
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Destination	
MAC Address	Select the check box and enter the destination MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. 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.
IP Address	Select the check box and enter the destination IP address in dotted decimal notation. A blank source IP address means any source IP address.
IP Subnet Mask	Enter the destination subnet mask.
Port Range	If you select **TCP** or **UDP** in the **IP Protocol** field, select the check box and enter the port number(s) of the source.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Others	
IP Protocol	This field is available only when you select **IP** in the **Ether Type** field. Select this option and select the protocol (service type) from **TCP** or **UDP**. If you select **User defined**, enter the protocol (service type) number.
IP Packet Length	This field is available only when you select **IP** in the **Ether Type** field. Select this option and enter the minimum and maximum packet length (from 46 to 1504) in the fields provided.
DSCP	This field is available only when you select **IP** in the **Ether Type** field. Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
TCP ACK	This field is available only when you select **IP** in the **Ether Type** field. If you select this option, the matched TCP packets must contain the ACK (Acknowledge) flag.

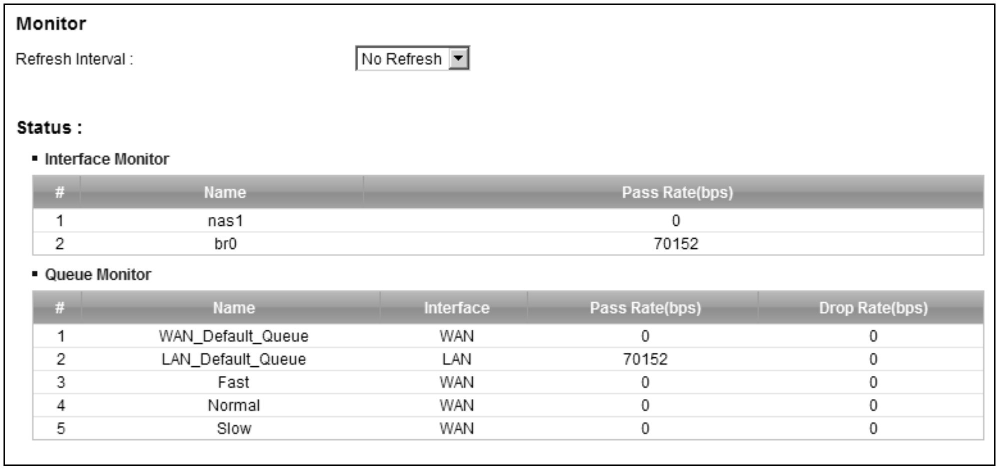
Table 32 Class Setup: Add/Edit (continued)

LABEL	DESCRIPTION
DHCP	This field is available only when you select **IP** in the **Ether Type** field, and **UDP** in the **IP Protocol** field. Select this option and select a DHCP option. If you select **Vendor Class ID (DHCP Option 60)**, enter the **Class ID** of the matched traffic, such as the type of the hardware or firmware. If you select **ClientID (DHCP Option 61)**, enter the **Type** of the matched traffic and **Client ID** of the DHCP client. If you select **User Class ID (DHCP Option 77)**, enter the **User Class Data**, which is a string that identifies the user's category or application type in the matched DHCP packets. If you select **VendorSpecificIntro (DHCP Option 125)**, enter the **Enterprise Number** of the software of the matched traffic and **Vendor Class Data** used by all the DHCP clients.
Service	Select the service classification of the traffic.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen without saving.

10.5 The QoS Monitor Screen

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

Figure 64 Network Setting > QoS > Monitor



Monitor

Refresh Interval : No Refresh

Status :

Interface Monitor

#	Name	Pass Rate(bps)
1	nas1	0
2	br0	70152

Queue Monitor

#	Name	Interface	Pass Rate(bps)	Drop Rate(bps)
1	WAN_Default_Queue	WAN	0	0
2	LAN_Default_Queue	LAN	70152	0
3	Fast	WAN	0	0
4	Normal	WAN	0	0
5	Slow	WAN	0	0

The following table describes the labels in this screen.

Table 33 Network Setting > QoS > Monitor

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

10.6 QoS Technical Reference

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

10.6.1 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 34 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.

10.6.2 IP Precedence

Similar to IEEE 802.1p prioritization at layer-2, you can use IP precedence to prioritize packets in a layer-3 network. IP precedence uses three bits of the eight-bit ToS (Type of Service) field in the IP header. There are eight classes of services (ranging from zero to seven) in IP precedence. Zero is the lowest priority level and seven is the highest.

10.6.3 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 DS (Differentiated Services) 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.

11

Network Address Translation (NAT)

11.1 Overview

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

11.1.1 What You Can Do in this Chapter

- Use the **Port Forwarding** screen to configure forward incoming service requests to the server(s) on your local network (Section 11.2 on page 150).
- Use the **Sessions** screen to limit the number of concurrent NAT sessions each client can use (Section 11.3 on page 153).

11.1.2 What You Need To Know

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

Inside/Outside and Global/Local

Inside/outside denotes where a host is located relative to the ZyXEL Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

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

NAT

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

Port Forwarding

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

Finding Out More

See Section 11.4 on page 154 for advanced technical information on NAT.

11.2 The Port Forwarding Screen

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

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

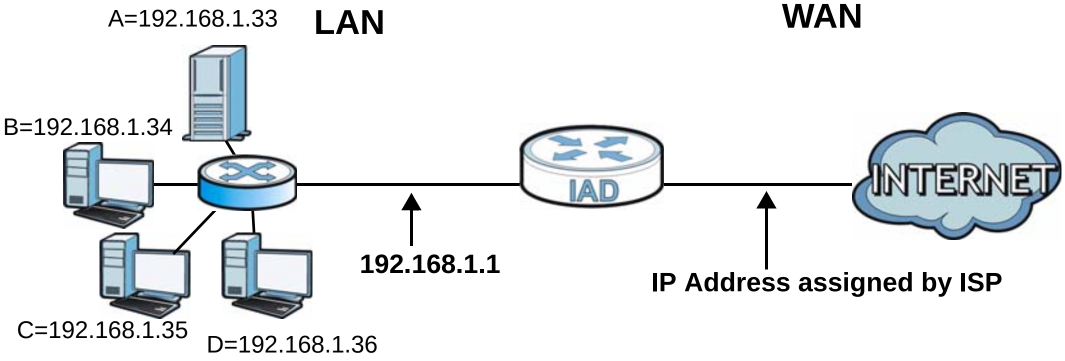
The most often used port numbers and services are shown in Appendix E on page 323. Please refer to RFC 1700 for further information about port numbers.

Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Configuring Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) 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 65 Multiple Servers Behind NAT Example

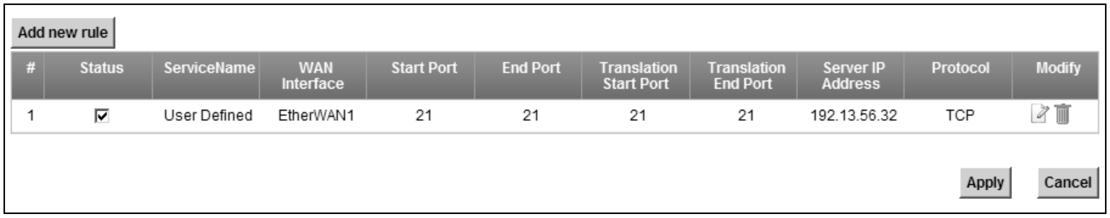


11.2.1 The Port Forwarding Screen

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

See Appendix E on page 323 for port numbers commonly used for particular services.

Figure 66 Network Setting > NAT > Port Forwarding



#	Status	ServiceName	WAN Interface	Start Port	End Port	Translation Start Port	Translation End Port	Server IP Address	Protocol	Modify
1	☑	User Defined	EtherWAN1	21	21	21	21	192.13.56.32	TCP	

The following table describes the fields in this screen.

Table 35 Network Setting > NAT > Port Forwarding

LABEL	DESCRIPTION
Add new rule	Click this to add a new port forwarding rule.
#	This is the index number of the entry.
Status	This field indicates whether the rule is active or not. Clear the check box to disable the rule. Select the check box to enable it.
Service Name	This is the service's name. This shows **User Defined** if you manually added a service. You can change this by clicking the edit icon.
WAN Interface	This shows the WAN interface through which the service is forwarded.
Start Port	This is the first external port number that identifies a service.
End Port	This is the last external port number that identifies a service.

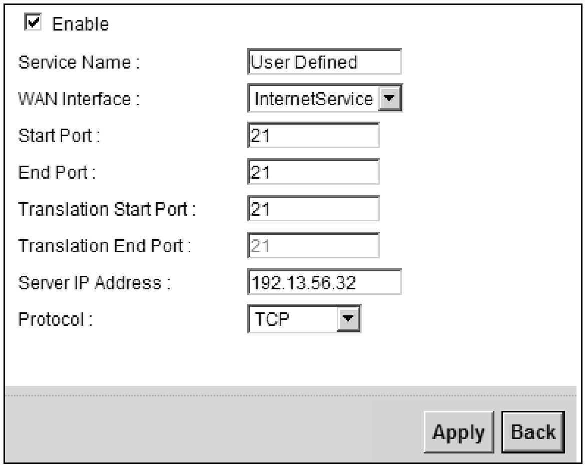
Table 35 Network Setting > NAT > Port Forwarding (continued)

LABEL	DESCRIPTION
Translation Start Port	This is the first internal port number that identifies a service.
Translation End Port	This is the last internal port number that identifies a service.
Server IP Address	This is the server's IP address.
Protocol	This shows the IP protocol supported by this virtual server, whether it is **TCP**, **UDP**, or **TCP/UDP**.
Modify	Click the **Edit** icon to edit the port forwarding rule. Click the **Delete** icon to delete an existing port forwarding rule. Note that subsequent address mapping rules move up by one when you take this action.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

11.2.2 The Port Forwarding Edit Screen

This screen lets you create or edit a port forwarding rule. Click **Add new rule** in the **Port Forwarding** screen or the **Edit** icon next to an existing rule to open the following screen.

Figure 67 Port Forwarding: Add/Edit



☑ Enable

Service Name :	User Defined
WAN Interface :	InternetService
Start Port :	21
End Port :	21
Translation Start Port :	21
Translation End Port :	21
Server IP Address :	192.13.56.32
Protocol :	TCP

The following table describes the labels in this screen.

Table 36 Port Forwarding: Add/Edit

LABEL	DESCRIPTION
Enable	Clear the check box to disable the rule. Select the check box to enable it. This field is available only when you are editing the port forwarding rule.
Service Name	Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on).

Table 36 Port Forwarding: Add/Edit (continued)

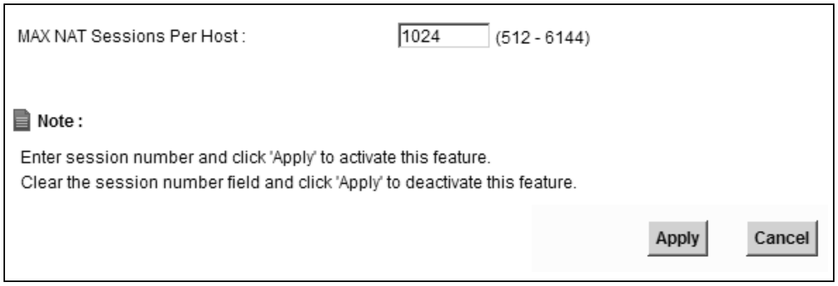
LABEL	DESCRIPTION
WAN Interface	Select the WAN interface through which the service is forwarded. You must have already configured a WAN connection with NAT enabled.
Start Port	Enter the original destination port for the packets. To forward only one port, enter the port number again in the **External End Port** field. To forward a series of ports, enter the start port number here and the end port number in the **External End Port** field.
End Port	Enter the last port of the original destination port range. To forward only one port, enter the port number in the **External Start Port** field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the **External Start Port** field above.
Translation Start Port	This shows the port number to which you want the ZyXEL Device to translate the incoming port. For a range of ports, enter the first number of the range to which you want the incoming ports translated.
Translation End Port	This shows the last port of the translated port range.
Server IP Address	Enter the inside IP address of the virtual server here.
Protocol Type	Select the protocol supported by this virtual server. Choices are **TCP**, **UDP**, or **TCP/UDP**.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen without saving.

11.3 The Sessions Screen

Use the **Sessions** screen to limit the number of concurrent NAT sessions each client can use.

Click **Network Setting > NAT > Sessions** to display the following screen.

Figure 68 Network Setting > NAT > Sessions



MAX NAT Sessions Per Host : 1024 (512 - 6144)

Note :

Enter session number and click 'Apply' to activate this feature.
Clear the session number field and click 'Apply' to deactivate this feature.

The following table describes the fields in this screen.

Table 37 Network Setting > NAT > Sessions

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

11.4 Technical Reference

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

11.4.1 NAT Definitions

Inside/outside denotes where a host is located relative to the ZyXEL Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

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

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

Table 38 NAT Definitions

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

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

11.4.2 What NAT Does

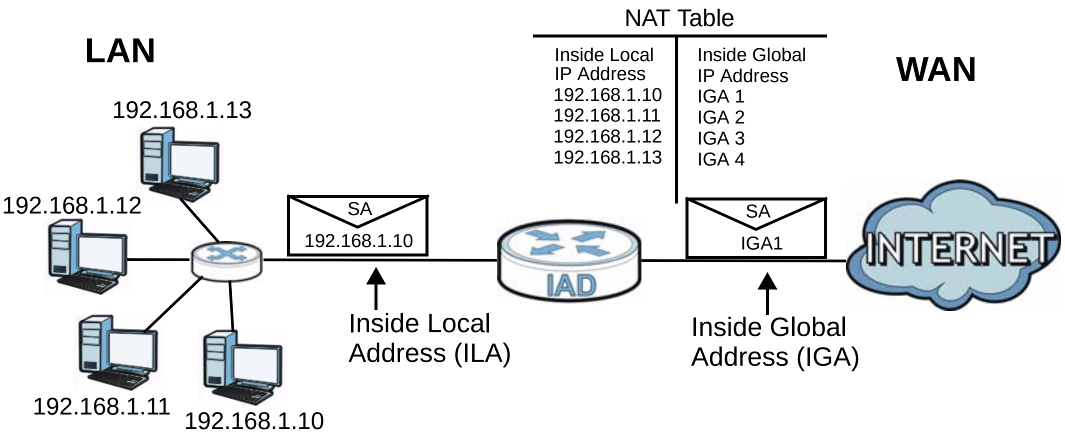
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address)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

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

11.4.3 How NAT Works

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

Figure 69 How NAT Works



NAT Table

Inside Local IP Address	Inside Global IP Address
192.168.1.10	IGA 1
192.168.1.11	IGA 2
192.168.1.12	IGA 3
192.168.1.13	IGA 4

12

Dynamic DNS

12.1 Overview

This chapter discusses how to configure your ZyXEL Device to use Dynamic DNS.

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

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

12.1.1 What You Need To Know

DYNDNS Wildcard

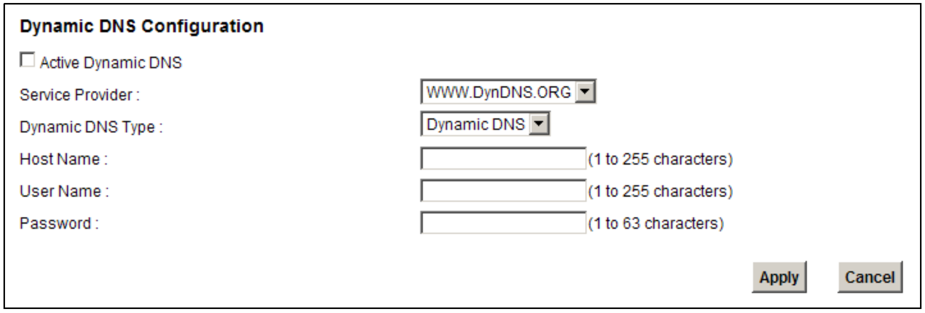
Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

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

12.2 The Dynamic DNS Screen

Use the **Dynamic DNS** screen to enable DDNS and configure the DDNS settings on the ZyXEL Device. To change your ZyXEL Device's DDNS, click **Network Setting > DNS**. The screen appears as shown.

Figure 70 Network Setting > DNS



Dynamic DNS Configuration

□ Active Dynamic DNS

Service Provider :	WWW.DynDNS.ORG
Dynamic DNS Type :	Dynamic DNS
Host Name :	(1 to 255 characters)
User Name :	(1 to 255 characters)
Password :	(1 to 63 characters)

The following table describes the fields in this screen.

Table 39 Network Setting > DNS

LABEL	DESCRIPTION
Dynamic DNS Configuration	
Active Dynamic DNS	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
Dynamic DNS Type	Select the type of service that you are registered for from 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 (",").
User Name	Type your user name.
Password	Type the password assigned to you.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

13

Firewall

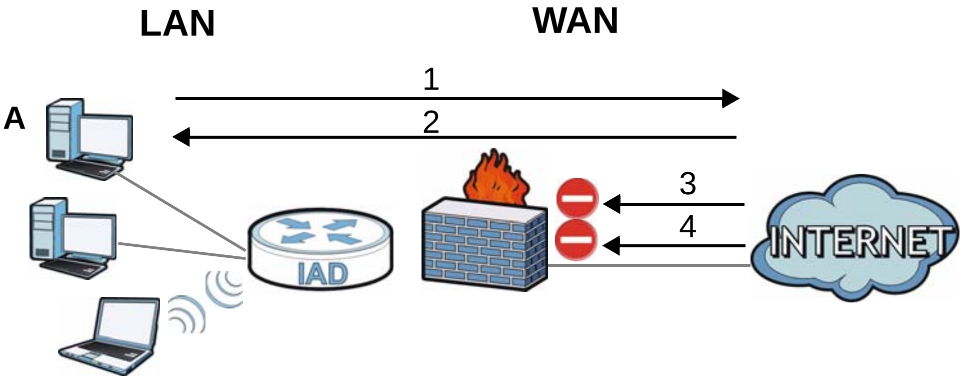
13.1 Overview

Use the ZyXEL Device firewall screens to enable and configure the firewall that protects your ZyXEL Device and network from attacks by hackers on the Internet and control access to it. By default the firewall:

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

The following figure illustrates the default firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN to the WAN (**1**). Return traffic for this session is also allowed (**2**). However other traffic initiated from the WAN is blocked (**3** and **4**).

Figure 71 Default Firewall Action



13.1.1 What You Can Do in this Chapter

- Use the **General** screen to enable or disable the ZyXEL Device's firewall (Section 13.2 on page 161).
- Use the **Services** screen to configure LAN-to-WAN services blocking on the ZyXEL Device (Section 13.3 on page 161).

13.1.2 What You Need to Know

Firewall

The ZyXEL Device's firewall feature physically separates the LAN/WLAN and the WAN and acts as a secure gateway for all data passing between the networks.

It is designed to protect against Denial of Service (DoS) attacks when activated. The ZyXEL Device's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The ZyXEL Device can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network.

The ZyXEL Device is installed between the LAN/WLAN and a broadband modem connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The ZyXEL Device has one Ethernet WAN port and four Ethernet LAN ports, which are used to physically separate the network into two areas.The WAN (Wide Area Network) port attaches to the broadband (cable or DSL) modem to the Internet.

The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP and the World Wide Web. However, "inbound access" is not allowed (by default) unless the remote host is authorized to use a specific service.

ICMP

Internet Control Message Protocol (ICMP) is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.

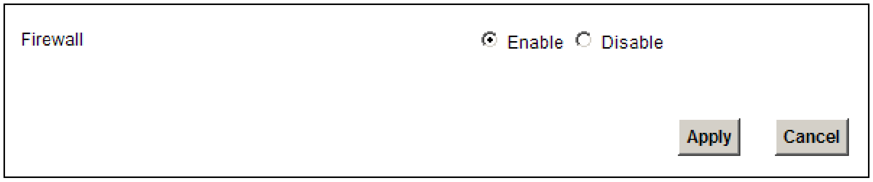
Finding Out More

See Section 13.4 on page 163 for advanced technical information on firewall.

13.2 The General Screen

Use this screen to enable or disable the ZyXEL Device's firewall. Click **Security > Firewall** to open the **General** screen.

Figure 72 Security > Firewall > General



Firewall ● Enable ○ Disable

The following table describes the labels in this screen.

Table 40 Security > Firewall > General

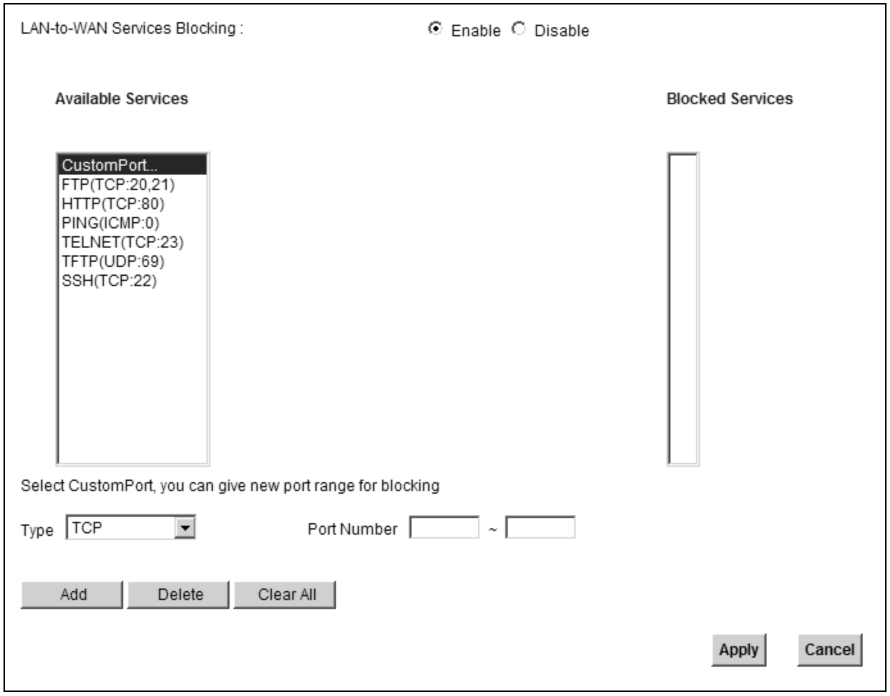
LABEL	DESCRIPTION
Firewall	Select **Enable** to activate the firewall. The ZyXEL Device performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

13.3 The Services Screen

Use this screen to enable service blocking and to maintain the list of services you want to block. To access this screen, click **Security > Firewall > Services**.

Note: These rules specify which computers on the LAN can access which computers or services on the WAN.

Figure 73 Security > Firewall > Services



LAN-to-WAN Services Blocking : ● Enable ○ Disable

Available Services

CustomPort...
FTP(TCP:20,21)
HTTP(TCP:80)
PING(ICMP:0)
TELNET(TCP:23)
TFTP(UDP:69)
SSH(TCP:22)

Blocked Services

Select CustomPort, you can give new port range for blocking

Type TCP

Port Number ~

Each field is described in the following table.

Table 41 Security > Firewall > Services

LABEL	DESCRIPTION
LAN-to-WAN Services Blocking	Select **Enable** to activate service blocking.
Available Services	This is a list of pre-defined services (destination ports) you may prohibit your LAN computers from using. Select the port you want to block, and click **Add** to add the port to the **Blocked Services** field. A custom port is a service that is not available in the pre-defined **Available Services** list. You must define it using the **Type** and **Port Number** fields. See Appendix E on page 323 for some examples of services.
Blocked Services	This is a list of services (ports) that are inaccessible to computers on your LAN when service blocking is effective. To remove a service from this list, select the service, and click **Delete**.
Type	Select **TCP**, **UDP** or **TCP and UDP**, based on which one the custom port uses.
Port Number	Enter the range of port numbers that defines the service. For example, suppose you want to define the Gnutella service. Select **TCP** type and enter a port range of **6345-6349**.
Add	Click this to add the selected service in **Available Services** to the **Blocked Services** list. Note that the service is blocked immediately after clicking this.

Table 41 Security > Firewall > Services (continued)

LABEL	DESCRIPTION
Delete	Select a service in the **Blocked Services**, and click this to remove the service from the list.
Clear All	Click this to remove all the services in the **Blocked Services** list.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

13.4 Firewall Technical Reference

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

13.4.1 Guidelines For Enhancing Security With Your Firewall

1 Change the default password via web configurator.

2 Think about access control before you connect to the network in any way.

3 Limit who can access your ZyXEL Device.

4 Don't enable any local service (such as Telnet or FTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.

5 For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.

6 Keep the firewall in a secured (locked) room.

13.4.2 Security Considerations

Note: Incorrectly configuring the firewall may block valid access or introduce security risks to the ZyXEL Device and your protected network. Use caution when creating or deleting firewall rules and test your rules after you configure them.

Consider these security ramifications before creating a rule:

1 Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?

2 Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?

3 Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.

4 Does this rule conflict with any existing rules?

Once these questions have been answered, adding rules is simply a matter of entering the information into the correct fields in the web configurator screens.

14

MAC Filter

14.1 Overview

This chapter discusses MAC address filtering.

The MAC filter screen allows you to configure the ZyXEL Device to give exclusive access to up to 32 wireless or wired clients (Allow) based on the MAC address of the wireless/wired clients.

Note: The MAC filter applies to wired and wireless connections.

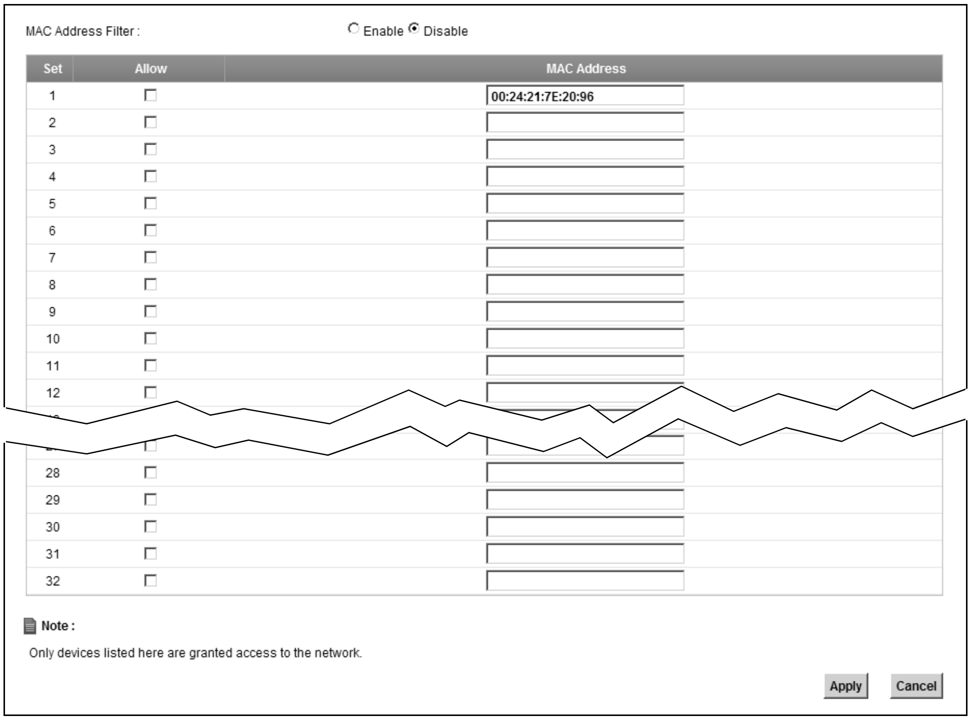
14.1.1 What You Need to Know

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 address of the devices to configure this screen.

14.2 The MAC Filter Screen

Use the **MAC Filter** screen to allow wireless clients access to the ZyXEL Device. To change your ZyXEL Device's MAC filter settings, click **Security** > **MAC Filter**. The screen appears as shown.

Figure 74 Security > MAC Filter



MAC Address Filter : ○ Enable ● Disable

Set	Allow	MAC Address
1	□	00:24:21:7E:20:96
2	□	
3	□	
4	□	
5	□	
6	□	
7	□	
8	□	
9	□	
10	□	
11	□	
12	□	
28	□	
29	□	
30	□	
31	□	
32	□	

Note :

Only devices listed here are granted access to the network.

The following table describes the labels in this menu.

Table 42 Security > MAC Filter

LABEL	DESCRIPTION
MAC Address Filter	Select **Enable** to activate MAC address filtering.
Set	This is the index number of the MAC address.
Allow	Select **Allow** to permit access to the ZyXEL Device. MAC addresses not listed will be denied access to the ZyXEL Device. If you clear this, the **MAC Address** field for this set clears.
MAC Address	Enter the MAC addresses of the wireless station that are allowed access to the ZyXEL Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

15

Certificates

15.1 Overview

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

15.1.1 What You Can Do in this Chapter

- Use the **Local Certificates** screens to view and import the ZyXEL Device's CA-signed certificates (Section 15.2 on page 170).
- Use the **Trusted CA** screens to save the certificates of trusted CAs to the ZyXEL Device. You can also export the certificates to a computer (Section 15.3 on page 172).

15.1.2 What You Need to Know

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

Certification Authorities

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities.

Public and Private Keys

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available; the other key is private and must be kept secure. Public-key encryption in general works as follows.

1. Tim wants to send a private message to Jenny. Tim generates a public-private key pair. What is encrypted with one key can only be decrypted using the other.

2. Tim keeps the private key and makes the public key openly available.

3 Tim uses his private key to encrypt the message and sends it to Jenny.

4 Jenny receives the message and uses Tim's public key to decrypt it.

5 Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

The ZyXEL Device uses certificates based on public-key cryptology to authenticate users attempting to establish a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

Certification Path

A certification path is the hierarchy of certification authority certificates that validate a certificate. The ZyXEL Device does not trust a certificate if any certificate on its path has expired or been revoked.

Certificate Directory Servers

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The ZyXEL Device can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

Advantages of Certificates

Certificates offer the following benefits.

- The ZyXEL Device only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

Certificate File Formats

The certification authority certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. The ZyXEL Device currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses 64 ASCII characters to convert a binary PKCS#7 certificate into a printable form.

Note: Be careful not to convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

15.1.3 Verifying a Certificate

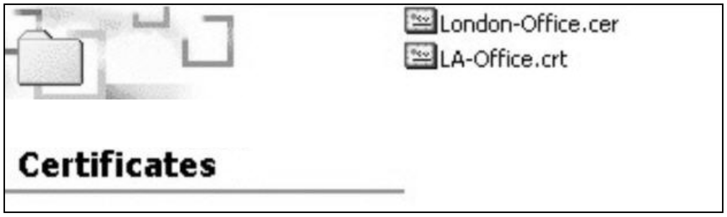
Before you import a trusted CA or trusted remote host certificate into the ZyXEL Device, you should verify that you have the actual certificate. This is especially true of trusted CA certificates since the ZyXEL Device also trusts any valid certificate signed by any of the imported trusted CA certificates.

You can use a certificate's fingerprint to verify it. A certificate's fingerprint is a message digest calculated using the MD5 or SHA1 algorithms. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

1 Browse to where you have the certificate saved on your computer.

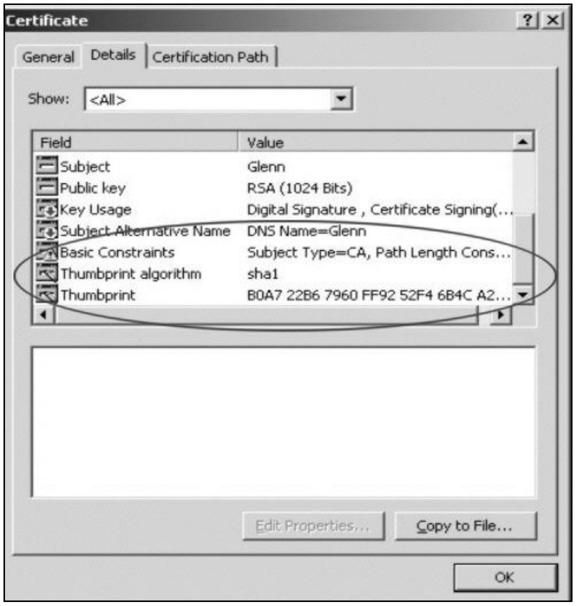
2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 75 Certificates on Your Computer



3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

Figure 76 Certificate Details



Show: <All>

Field	Value
Subject	Glenn
Public key	RSA (1024 Bits)
Key Usage	Digital Signature , Certificate Signing(...
Subject Alternative Name	DNS Name=Glenn
Basic Constraints	Subject Type=CA, Path Length Cons...
Thumbprint algorithm	sha1
Thumbprint	B0A7 22B6 7960 FF92 52F4 6B4C A2...

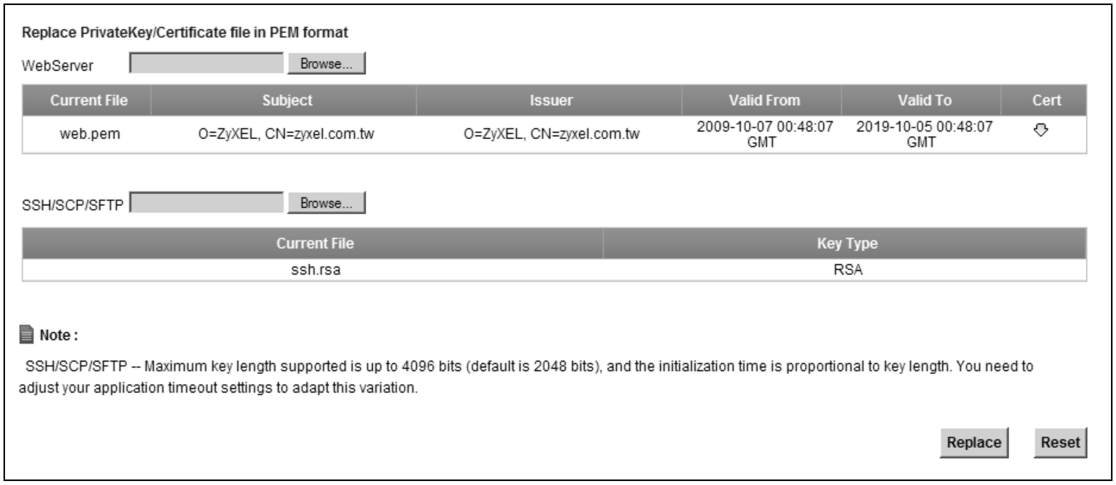
4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may very based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

15.2 Local Certificates

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

- Web Server - This certificate secures HTTP connections.
- SIP TLS - This certificate secures VoIP connections.
- SSH/SCP/SFTP - This certificate secures remote connections.

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



Replace PrivateKey/Certificate file in PEM format

WebServer

Current File	Subject	Issuer	Valid From	Valid To	Cert
web.pem	O=ZyXEL, CN=zyxel.com.tw	O=ZyXEL, CN=zyxel.com.tw	2009-10-07 00:48:07 GMT	2019-10-05 00:48:07 GMT	⇩

SSH/SCP/SFTP

Current File	Key Type
ssh.rsa	RSA

Note :

SSH/SCP/SFTP -- Maximum key length supported is up to 4096 bits (default is 2048 bits), and the initialization time is proportional to key length. You need to adjust your application timeout settings to adapt this variation.

Figure 77 Security > Certificates > Local Certificates

The following table describes the labels in this screen.

Table 43 Security > Certificates > Local Certificates

LABEL	DESCRIPTION
Web Server	Type in the location of the **Web Server** certificate file you want to upload in this field or click **Browse** to find it.
Browse	Click **Browse** to find the certificate file you want to upload.
Current File	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Subject	This field displays identifying information about the certificate’s owner, such as **CN** (Common Name), **OU** (Organizational Unit or department), **O** (Organization or company) and **C** (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate’s issuing certification authority, such as a common name, organizational unit or department, organization or company and country.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a **Not Yet Valid!** message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an **Expiring!** or **Expired!** message if the certificate is about to expire or has already expired.
Cert	Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
SSH/SCP/SFTP	Type in the location of the **SSH/SCP/SFTP** certificate file you want to upload in this field or click **Browse** to find it.
Browse	Click **Browse** to find the certificate file you want to upload.
Current File	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.

Table 43 Security > Certificates > Local Certificates (continued)

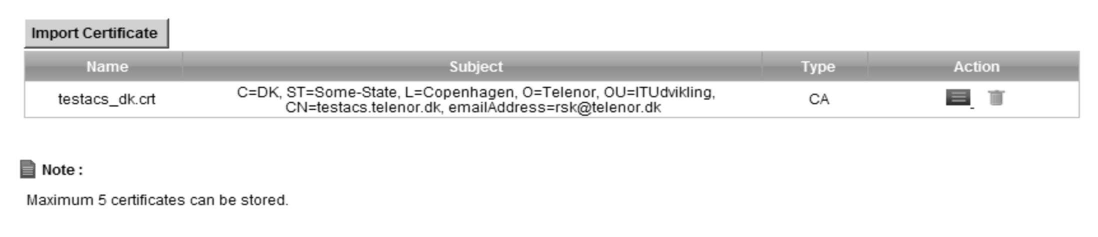
LABEL	DESCRIPTION
Key Type	This field applies to the **SSH / SCP / SFTP** certificate. This shows the file format of the current certificate.
Replace	Click this to replace the certificate(s) and save your changes back to the ZyXEL Device.
Reset	Click this to clear your settings.

15.3 Trusted CA

Use this screen to view a summary list of certificates of the certification authorities that you have set the ZyXEL Device to accept as trusted. The ZyXEL Device accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

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

Figure 78 Security > Certificates > Trusted CA



Name	Subject	Type	Action
testacs_dk.crt	C=DK, ST=Some-State, L=Copenhagen, O=Telenor, OU=ITUdvikling, CN=testacs.telenor.dk, emailAddress=rsk@telenor.dk	CA	

Note :

Maximum 5 certificates can be stored.

The following table describes the labels in this screen.

Table 44 Security > Certificates > Trusted CA

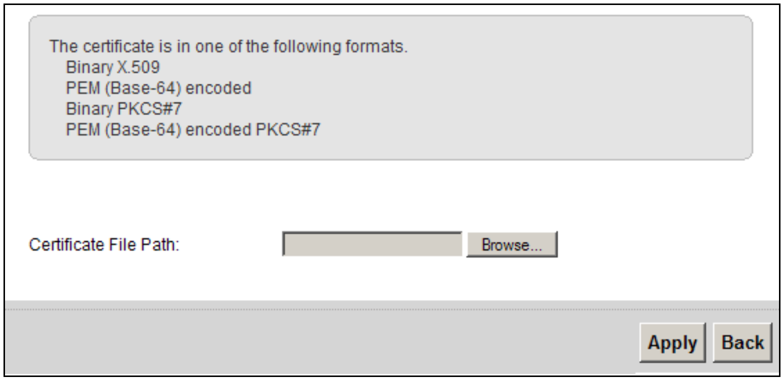
LABEL	DESCRIPTION
Import Certificate	Click this button to open a screen where you can save the certificate of a certification authority that you trust to the ZyXEL Device.
Name	This field displays the name used to identify this certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), OU (Organizational Unit or department), Organization (O), State (ST) and Country (C). It is recommended that each certificate have unique subject information.
Type	This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate.
Action	Click the **View** icon to open a screen with an in-depth list of information about the certificate (or certification request). Click the **Delete** icon to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

15.4 Trusted CA Import

Click **Import Certificate** in the **Trusted CAs** screen to open the **Import Certificate** screen. You can save a trusted certification authority's certificate to the ZyXEL Device.

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

Figure 79 Trusted CA > Import



The certificate is in one of the following formats.
Binary X.509
PEM (Base-64) encoded
Binary PKCS#7
PEM (Base-64) encoded PKCS#7

The following table describes the labels in this screen.

Table 45 Security > Certificates > Trusted CA > Import

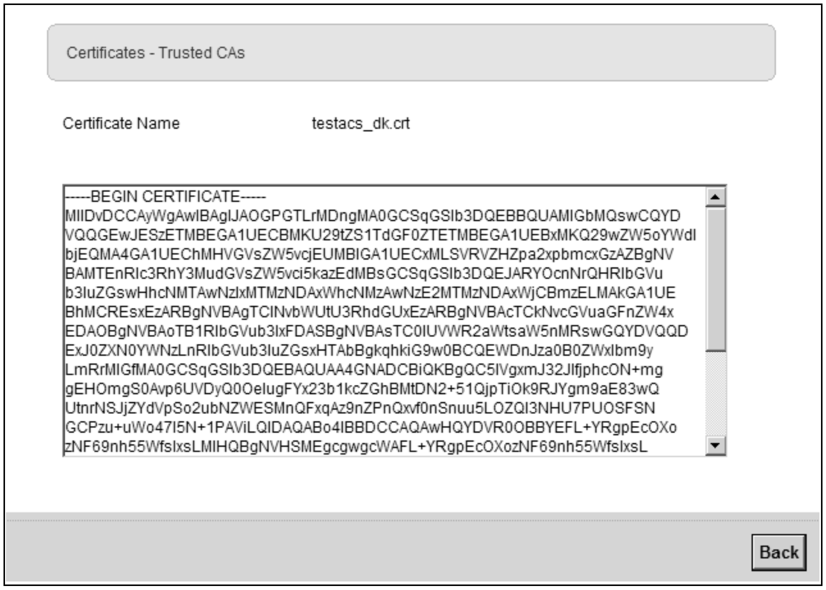
LABEL	DESCRIPTION
Certificate File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click **Browse** to find the certificate file you want to upload.
Apply	Click **Apply** to save the certificate on the ZyXEL Device.
Back	Click **Back** to return to the previous screen.

15.5 View Certificate

Use this screen to view in-depth information about the certification authority's certificate, change the certificate's name and set whether or not you want the ZyXEL Device to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

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

Figure 80 Trusted CA: View



Certificate Name testacs_dk.crt

```
-----BEGIN CERTIFICATE-----
MIIDvDCCAyWgAwIBAgIJAOGPGTLrMDngMA0GCSqGSIb3DQEBBQUAMIGbMQswCQYD
VQQGEwJESzETMBEGA1UECBMKU29tZS1TdGF0ZTETMBEGA1UEBxMKQ29wZW5oYWdl
bjEQMA4GA1UEChMHVGVsZW5vcjEUMBIGA1UECxMLSVRVZHZpa2xpbmcxGzAZBgNV
BAMTEnRlc3RhY3MudGVsZW5vci5kazEdMBsGCSqGSIb3DQEJARYOcnNrQHRlbGVu
b3IuZGswHhcNMTAwNzIxMTMzNDAxWhcNMzAwNzE2MTMzNDAxWjCBmzELMAkGA1UE
BhMCREsxEzARBgNVBAgTClNvbWUtU3RhdGUxEzARBgNVBAcTCkNvcGVuaGFnZW4x
EDAOBgNVBAoTB1RlbGVub3IxFDASBgNVBAsTC0lUVWR2aWtsaW5nMRswGQYDVQQD
ExJ0ZXN0YWNzLnRlbGVub3IuZGsxHTAbBgkqhkiG9w0BCQEWDnJza0B0ZWxlbm9y
LmRrMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC5lVgxmJ32JlfjphcON+mg
gEHOmgS0Avp6UVDyQ0OelugFYx23b1kcZGhBMtDN2+51QjpTiOk9RJYgm9aE83wQ
UtnrNSJjZYdVpSo2ubNZWESMnQFxqAz9nZPnQxvf0nSnuu5LOZQI3NHU7PUOSFSN
GCPzu+uWo47I5N+1PAViLQIDAQABo4IBBDCCAQAwHQYDVR0OBBYEFL+YRgpEcOXo
zNF69nh55WfsIxsLMIHQBgNVHSMEgcgwgcWAFL+YRgpEcOXozNF69nh55WfsIxsL
```

The following table describes the labels in this screen.

Table 46 Trusted CA: View

LABEL	DESCRIPTION
Certificate Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Certificate Detail	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Back	Click this to return to the previous screen.

16

VoIP

16.1 Overview

Use this chapter to:

- Connect an analog phone to the ZyXEL Device.
- Make phone calls over the Internet, as well as the regular phone network.
- Configure settings such as speed dial.
- Configure network settings to optimize the voice quality of your phone calls.

16.1.1 What You Can Do in this Chapter

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

- Use the **SIP Service Provider** screen to configure the SIP server information and QoS for VoIP calls (Section 16.3 on page 181).
- Use the **SIP Account** screen to set up information about your SIP account, control which SIP accounts the phones connected to the ZyXEL Device use and configure audio settings such as volume levels for the phones connected to the ZyXEL Device (Section 16.3 on page 181).
- Use the **Common** screen to configure RFC3262 support on the ZyXEL Device (Section 16.4 on page 186).
- Use the **Phone Device** screen to control which SIP accounts the phones connected to the ZyXEL Device use (Section 16.5 on page 187).
- Use the **Region** screen to change settings that depend on the country you are in (Section 16.6 on page 188).
- Use the **Call Rule** screen to set up shortcuts for dialing frequently-used (VoIP) phone numbers (Section 16.8 on page 190).
- Use the **FXO** screen to set up the PSTN line used to make regular phone calls which do not use the Internet (Section 16.8 on page 190).

You don’t necessarily need to use all these screens to set up your account. In fact, if your service provider did not supply information on a particular field in a screen, it is usually best to leave it at its default setting.

16.1.2 What You Need to Know

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

VoIP

VoIP stands for Voice over IP. IP is the Internet Protocol, which is the message-carrying standard the Internet runs on. So, Voice over IP is the sending of voice signals (speech) over the Internet (or another network that uses the Internet Protocol).

SIP

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

SIP Accounts

A SIP account is a type of VoIP account. It is an arrangement with a service provider that lets you make phone calls over the Internet. When you set the ZyXEL Device to use your SIP account to make calls, the ZyXEL Device is able to send all the information about the phone call to your service provider on the Internet.

Voice Activity Detection/Silence Suppression

Voice Activity Detection (VAD) detects whether or not speech is present. This lets the ZyXEL Device reduce the bandwidth that a call uses by not transmitting “silent packets” when you are not speaking.

Comfort Noise Generation

When using VAD, the ZyXEL Device generates comfort noise when the other party is not speaking. The comfort noise lets you know that the line is still connected as total silence could easily be mistaken for a lost connection.

Echo Cancellation

G.168 is an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.

How to Find Out More

See Chapter 3 on page 35 for a tutorial showing how to set up these screens in an example scenario.

See Section 16.9 on page 191 for advanced technical information on SIP.

16.1.3 Before You Begin

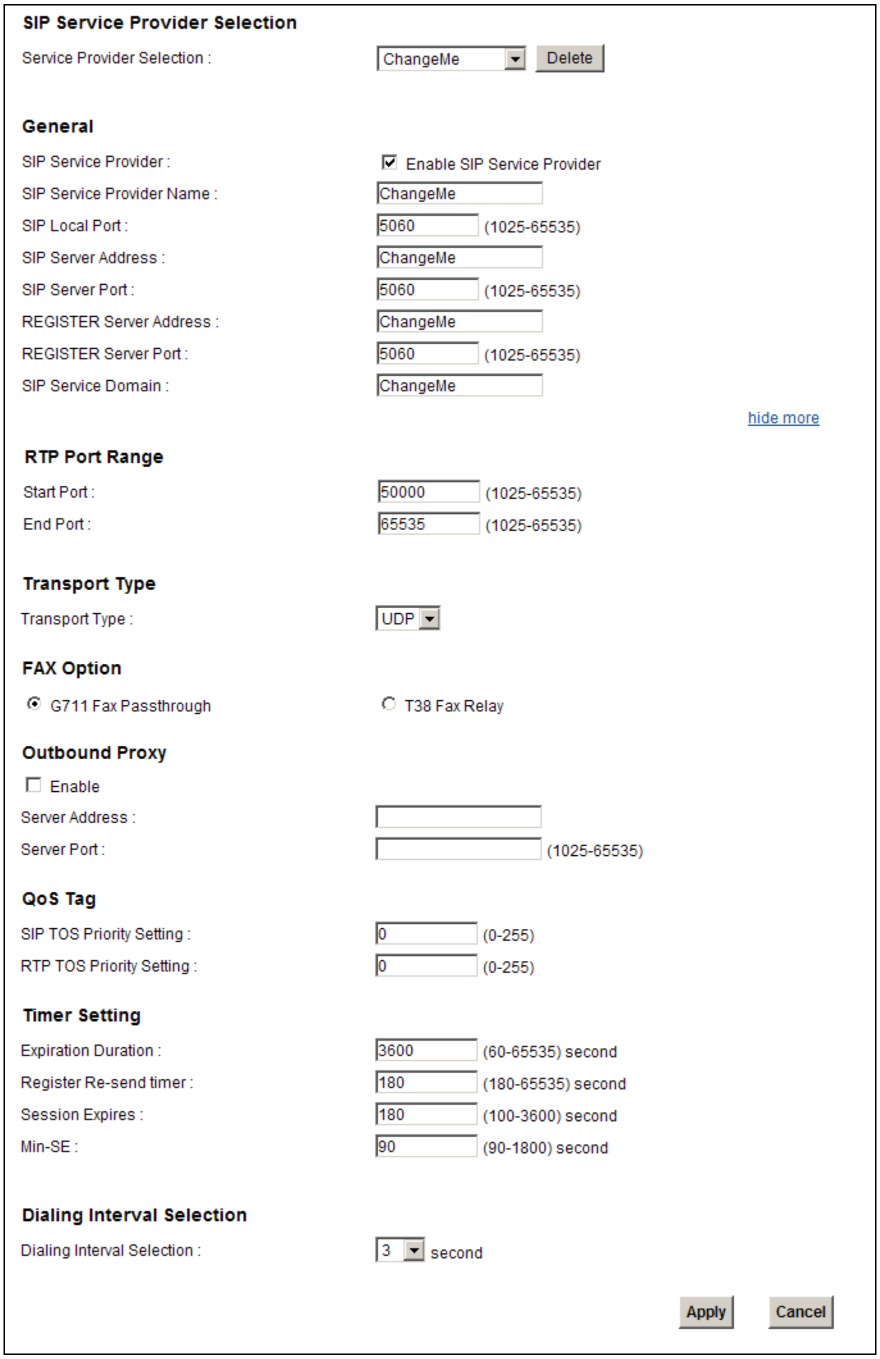
- Before you can use these screens, you need to have a VoIP account already set up. If you don't have one yet, you can sign up with a VoIP service provider over the Internet.
- You should have the information your VoIP service provider gave you ready, before you start to configure the ZyXEL Device.

16.2 The SIP Service Provider Screen

Use this screen to configure the SIP server information and QoS for VoIP calls. Click **VoIP > SIP** to open the **SIP Service Provider** screen.

Note: Click **more...** to see all the fields in the screen. You don't necessarily need to use all these fields to set up your account. Click **hide more** to see and configure only the fields needed for this feature.

Figure 81 VoIP > SIP > SIP Service Provider



SIP Service Provider Selection

Service Provider Selection :	ChangeMe ▾ Delete

General

SIP Service Provider :	☑ Enable SIP Service Provider
SIP Service Provider Name :	ChangeMe
SIP Local Port :	5060 (1025-65535)
SIP Server Address :	ChangeMe
SIP Server Port :	5060 (1025-65535)
REGISTER Server Address :	ChangeMe
REGISTER Server Port :	5060 (1025-65535)
SIP Service Domain :	ChangeMe

hide more

RTP Port Range

Start Port :	50000 (1025-65535)
End Port :	65535 (1025-65535)

Transport Type

Transport Type :	UDP ▾

FAX Option

● G711 Fax Passthrough ○ T38 Fax Relay

Outbound Proxy

□ Enable

Server Address :	
Server Port :	(1025-65535)

QoS Tag

SIP TOS Priority Setting :	0 (0-255)
RTP TOS Priority Setting :	0 (0-255)

Timer Setting

Expiration Duration :	3600 (60-65535) second
Register Re-send timer :	180 (180-65535) second
Session Expires :	180 (100-3600) second
Min-SE :	90 (90-1800) second

Dialing Interval Selection

Dialing Interval Selection :	3 ▾ second

The following table describes the labels in this screen.

Table 47 VoIP > SIP > SIP Service Provider

LABEL	DESCRIPTION
SIP Service Provider Selection	
Service Provider Selection	Select the SIP service provider profile you want to use for the SIP account you configure in this screen. If you change this field, the screen automatically refreshes. If you want to configure a new service provider, select **Add New**.
General	
SIP Service Provider	Select this if you want the ZyXEL Device to use this SIP provider. Clear it if you do not want the ZyXEL Device to use this SIP provider.
SIP Service Provider Name	Enter the name of your SIP service provider.
SIP Local Port	Enter the ZyXEL Device's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
SIP Server Address	Enter the IP address or domain name of the SIP server provided by your VoIP service provider. You can use up to 95 printable ASCII characters. It does not matter whether the SIP server is a proxy, redirect or register server.
SIP Server Port	Enter the SIP server's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
REGISTER Server Address	Enter the IP address or domain name of the SIP register server, if your VoIP service provider gave you one. Otherwise, enter the same address you entered in the **SIP Server Address** field. You can use up to 95 printable ASCII characters.
REGISTER Server Port	Enter the SIP register server's listening port number, if your VoIP service provider gave you one. Otherwise, enter the same port number you entered in the **SIP Server Port** field.
SIP Service Domain	Enter the SIP service domain name. In the full SIP URI, this is the part after the @ symbol. You can use up to 127 printable ASCII Extended set characters.
RTP Port Range	
Start Port End Port	Enter the listening port number(s) for RTP traffic, if your VoIP service provider gave you this information. Otherwise, keep the default values. To enter one port number, enter the port number in the **Start Port** and **End Port** fields. To enter a range of ports, • enter the port number at the beginning of the range in the **Start Port** field. • enter the port number at the end of the range in the **End Port** field.

Table 47 VoIP > SIP > SIP Service Provider (continued)

LABEL	DESCRIPTION
DTMF Mode	Control how the ZyXEL Device handles the tones that your telephone makes when you push its buttons. You should use the same mode your VoIP service provider uses. **RFC2833** - send the DTMF tones in RTP packets. **PCM** - send the DTMF tones in the voice data stream. This method works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729 and G.726) can distort the tones. **SIP INFO** - send the DTMF tones in SIP messages.
Transport Type	
Transport Type	Select the transport layer protocol (**UDP** or **TCP**) used for SIP.
FAX Option	This field controls how the ZyXEL Device handles fax messages.
G711 Fax Passthrough	Select this if the ZyXEL Device should use G.711 to send fax messages. The peer devices must also use G.711.
T38 Fax Relay	Select this if the ZyXEL Device should send fax messages as UDP or TCP/IP packets through IP networks. This provides better quality, but it may have inter-operability problems. The peer devices must also use T.38.
Outbound Proxy	
Enable	Select this if your VoIP service provider has a SIP outbound server to handle voice calls. This allows the ZyXEL Device to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off any SIP ALG on a NAT router in front of the ZyXEL Device to keep it from re-translating the IP address (since this is already handled by the outbound proxy server).
Server Address	Enter the IP address or domain name of the SIP outbound proxy server.
Server Port	Enter the SIP outbound proxy server's listening port, if your VoIP service provider gave you one. Otherwise, keep the default value.
QoS Tag	
SIP TOS Priority Setting	Enter the DSCP (DiffServ Code Point) number for SIP message transmissions. The ZyXEL Device creates Class of Service (CoS) priority tags with this number to SIP traffic that it transmits.
RTP TOS Priority Setting	Enter the DSCP (DiffServ Code Point) number for RTP voice transmissions. The ZyXEL Device creates Class of Service (CoS) priority tags with this number to RTP traffic that it transmits.
Timer Setting	
Expiration Duration	Enter the number of seconds your SIP account is registered with the SIP register server before it is deleted. The ZyXEL Device automatically tries to re-register your SIP account when one-half of this time has passed. (The SIP register server might have a different expiration.)
Register Re-send timer	Enter the number of seconds the ZyXEL Device waits before it tries again to register the SIP account, if the first try failed or if there is no response.
Session Expires	Enter the number of seconds the ZyXEL Device lets a SIP session remain idle (without traffic) before it automatically disconnects the session.

Table 47 VoIP > SIP > SIP Service Provider (continued)

LABEL	DESCRIPTION
Min-SE	Enter the minimum number of seconds the ZyXEL Device lets a SIP session remain idle (without traffic) before it automatically disconnects the session. When two SIP devices start a SIP session, they must agree on an expiration time for idle sessions. This field is the shortest expiration time that the ZyXEL Device accepts.
Dialing Interval Selection	
Dialing Interval Selection	Enter the number of seconds the ZyXEL Device should wait after you stop dialing numbers before it makes the phone call. The value depends on how quickly you dial phone numbers.
PSTN Fail Over (“L” models only)	Select this check box if you want to redirect the outgoing calls to the PSTN line (that do not use the Internet) when your SIP account is unregistered or SIP call has failed.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

16.3 The SIP Account Screen

The ZyXEL Device uses a SIP account to make outgoing VoIP calls and check if an incoming call’s destination number matches your SIP account’s SIP number. In order to make or receive a VoIP call, you need to enable and configure a SIP account, and map it to a phone port. The SIP account contains information that allows your ZyXEL Device to connect to your VoIP service provider.

Use this screen to maintain basic information about the SIP account. You can also enable and disable the SIP account, configure the volume, echo cancellation and VAD (Voice Activity Detection) settings for each individual phone port on the ZyXEL Device.

Voice Activity Detection/Silence Suppression

Voice Activity Detection (VAD) detects whether or not speech is present. This lets the ZyXEL Device reduce the bandwidth that a call uses by not transmitting “silent packets” when you are not speaking.

Comfort Noise Generation

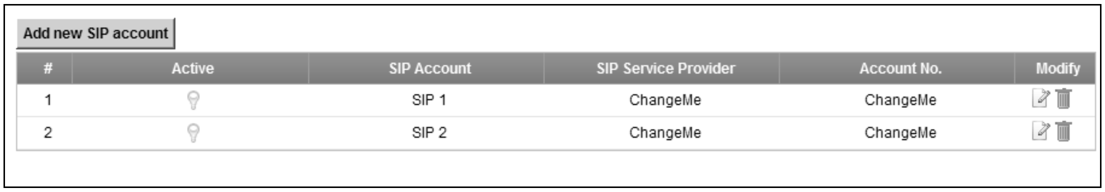
When using VAD, the ZyXEL Device generates comfort noise when the other party is not speaking. The comfort noise lets you know that the line is still connected as total silence could easily be mistaken for a lost connection.

Echo Cancellation

G.168 is an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.

To access the following screen, click **VoIP > SIP > SIP Account**.

Figure 82 VoIP > SIP > SIP Account



#	Active	SIP Account	SIP Service Provider	Account No.	Modify
1	💡	SIP 1	ChangeMe	ChangeMe	✎ 🗑
2	💡	SIP 2	ChangeMe	ChangeMe	✎ 🗑

The following table describes the labels in this screen.

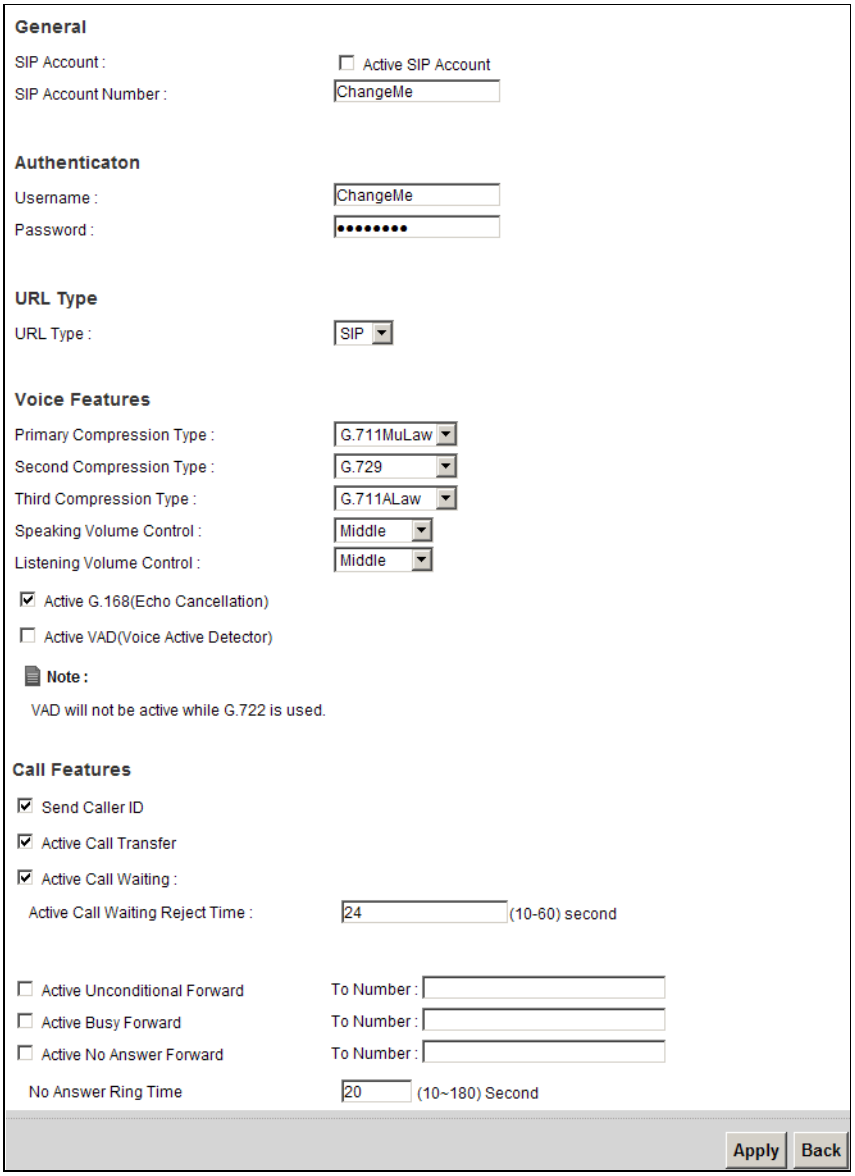
Table 48 VoIP > SIP > SIP Account

LABEL	DESCRIPTION
Add new SIP Account	Click this to configure a new SIP account.
#	This is the index number of the entry.
Active	This shows whether the SIP account is activated or not. A yellow bulb signifies that this SIP account is activated. A gray bulb signifies that this SIP account is deactivated.
SIP Account	This shows the name of the SIP account.
Account No.	This shows the SIP number.
Modify	Click the **Edit** icon to configure the SIP account. Click the **Delete** icon to delete this SIP account from the ZyXEL Device.

16.3.1 Add/Edit SIP Account

You can configure a new SIP account or edit one. To access this screen, click **Add new SIP Account** in the **SIP Account** screen or the **Edit** icon next to an existing account.

Figure 83 SIP Account: Add/Edit



General

SIP Account : □ Active SIP Account

SIP Account Number : ChangeMe

Authenticaton

Username : ChangeMe

Password : ••••••••

URL Type

URL Type : SIP

Voice Features

Primary Compression Type : G.711MuLaw

Second Compression Type : G.729

Third Compression Type : G.711ALaw

Speaking Volume Control : Middle

Listening Volume Control : Middle

☑ Active G.168(Echo Cancellation)

□ Active VAD(Voice Active Detector)

Note :

VAD will not be active while G.722 is used.

Call Features

☑ Send Caller ID

☑ Active Call Transfer

☑ Active Call Waiting :

Active Call Waiting Reject Time : 24 (10-60) second

□ Active Unconditional Forward To Number :

□ Active Busy Forward To Number :

□ Active No Answer Forward To Number :

No Answer Ring Time 20 (10~180) Second

Each field is described in the following table.

Table 49 SIP Account: Add/Edit

LABEL	DESCRIPTION
SIP Service Provider Selection	
Service Provider Selection	Select the SIP service provider profile you want to use for the SIP account you configure in this screen. This field is view-only if you are editing the SIP account.
General	
SIP Account	Select the **Active SIP Account** check box if you want the ZyXEL Device to use this account. Clear it if you do not want the ZyXEL Device to use this account.
SIP Account Number	Enter your SIP number. In the full SIP URI, this is the part before the @ symbol. You can use up to 127 printable ASCII characters.
Authentication	
Username	Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII characters.
Password	Enter the password for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII characters.
URL Type	
URL Type	Select whether or not to include the SIP service domain name when the ZyXEL Device sends the SIP number. **SIP** - include the SIP service domain name. **TEL** - do not include the SIP service domain name.
Voice Features	
Primary Compression Type Secondary Compression Type Third Compression Type	Select the type of voice coder/decoder (codec) that you want the ZyXEL Device to use. G.711 provides higher voice quality but requires more bandwidth (64 kbps). • **G.711MuLaw** is typically used in North America and Japan. • **G.711ALaw** is typically used in Europe. • **G.729** only requires 8 kbps. • **G.726-32** operates at 16, 24, 32 or 40 kbps. • **G.722** operates at 48, 56 and 64 kbps.The ZyXEL Device must use the same codec as the peer. When two SIP devices start a SIP session, they must agree on a codec. • **G.723** provides good voice quality, and requires 20 or 40 kbps. Select the ZyXEL Device's first choice for voice coder/decoder. Select the ZyXEL Device's second choice for voice coder/decoder. Select **None** if you only want the ZyXEL Device to accept the first choice. Select the ZyXEL Device's third choice for voice coder/decoder. Select **None** if you only want the ZyXEL Device to accept the first or second choice.
Speaking Volume Control	Enter the loudness that the ZyXEL Device uses for speech that it sends to the peer device. **Minimum** is the quietest, and **Maximum** is the loudest.

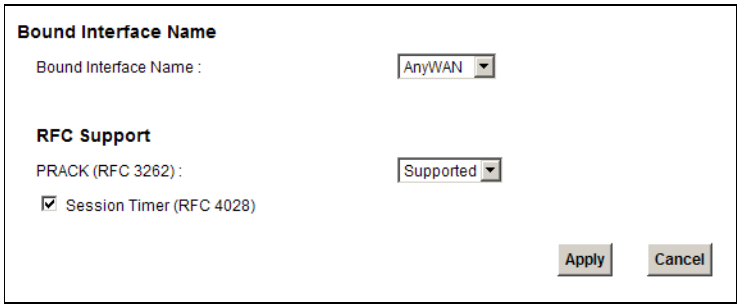
Table 49 SIP Account: Add/Edit (continued)

LABEL	DESCRIPTION
Listening Volume Control	Enter the loudness that the ZyXEL Device uses for speech that it receives from the peer device. **Minimum** is the quietest, and **Maximum** is the loudest.
Active G.168 (Echo Cancellation)	Select this if you want to eliminate the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
Active VAD (Voice Active Detector)	Select this if the ZyXEL Device should stop transmitting when you are not speaking. This reduces the bandwidth the ZyXEL Device uses.
Call Features	
Send Caller ID	Select this if you want to send identification when you make VoIP phone calls. Clear this if you do not want to send identification.
Active Call Transfer	Select this to enable call transfer on the ZyXEL Device. This allows you to transfer an incoming call (that you have answered) to another phone.
Active Call Waiting	Select this to enable call waiting on the ZyXEL Device. This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.
Call Waiting Reject Timer	Specify a time of seconds that the ZyXEL Device waits before rejecting the second call if you do not answer it.
Active Unconditional Forward	Select this if you want the ZyXEL Device to forward all incoming calls to the specified phone number. Specify the phone number in the **To Number** field on the right.
Active Busy Forward	Select this if you want the ZyXEL Device to forward incoming calls to the specified phone number if the phone port is busy. Specify the phone number in the **To Number** field on the right. If you have call waiting, the incoming call is forwarded to the specified phone number if you reject or ignore the second incoming call.
Active No Answer Forward	Select this if you want the ZyXEL Device to forward incoming calls to the specified phone number if the call is unanswered. (See **No Answer Time**.) Specify the phone number in the **To Number** field on the right.
No Answer Ring Time	This field is used by the **Active No Answer Forward** feature. Enter the number of seconds the ZyXEL Device should wait for you to answer an incoming call before it considers the call is unanswered.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen without saving.

16.4 The SIP Common Screen

Use the **Common** screen to configure RFC3262 support on the ZyXEL Device. To access the following screen, click **VoIP > SIP > Common**.

Figure 84 VoIP > SIP > Common



Bound Interface Name

Bound Interface Name : AnyWAN

RFC Support

PRACK (RFC 3262) : Supported

☑ Session Timer (RFC 4028)

Each field is described in the following table.

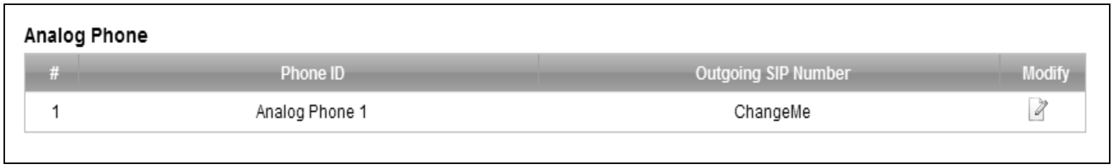
Table 50 VoIP > SIP > Common

LABEL	DESCRIPTION
Bound Interface Name	
Bound Interface Name	If you select **LAN** or **AnyWAN**, the ZyXEL Device automatically activates the VoIP service when any LAN or WAN connection is up. If you select **MultiWAN**, you also need to select the pre-configured WAN connections. The VoIP service is activated only when the selected WAN connection is up.
RFC Support	
PRACK (RFC 3262)	RFC 3262 defines a mechanism to provide reliable transmission of SIP provisional response messages, which convey information on the processing progress of the request. This uses the option tag 100rel and the Provisional Response ACKnowledgement (PRACK) method. Select **Supported** or **Required** to have the ZyXEL Device include a SIP Require/Supported header field with the option tag 100rel in all INVITE requests. When the ZyXEL Device receives a SIP response message indicating that the phone it called is ringing, the ZyXEL Device sends a PRACK message to have both sides confirm the message is received. If you select **Supported**, the peer device supports the option tag 100rel to send provisional responses reliably. If you select **Required**, the peer device requires the option tag 100rel to send provisional responses reliably.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to return to the previous screen without saving.

16.5 The Phone Device Screen

Use this screen to control which SIP account the phone uses. Click **VoIP > Phone** to access the **Phone Device** screen.

Figure 85 VoIP > Phone > Phone Device



Analog Phone

#	Phone ID	Outgoing SIP Number	Modify
1	Analog Phone 1	ChangeMe	✎

The following table describes the labels in this screen.

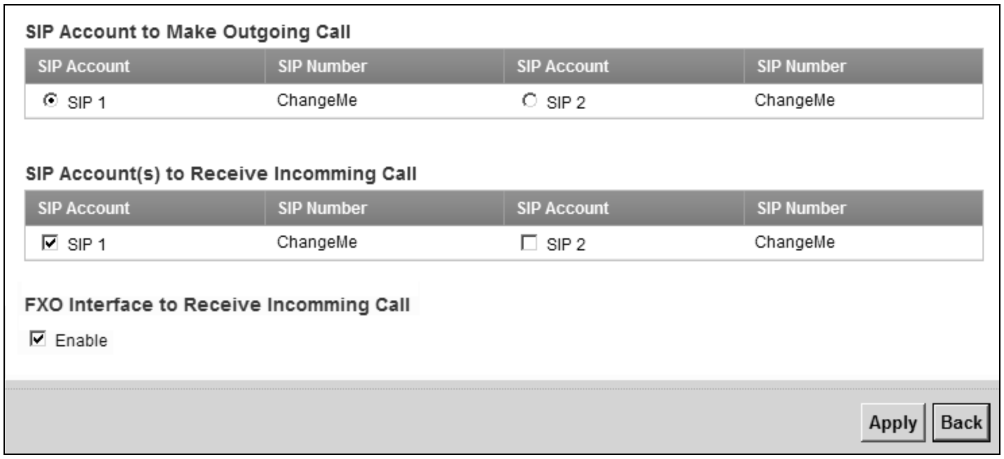
Table 51 VoIP > Phone > Phone Device

LABEL	DESCRIPTION
#	This is the index number of the entry.
Phone ID	This is the phone device number.
Outgoing SIP Number	This is the outgoing SIP number of the phone device.
Modify	Click the **Edit** icon to configure the SIP account.

16.5.1 Edit Phone Device

You can edit the SIP account by clicking the **Edit** icon next it. You cannot edit the account if it is not activated. Go to **VoIP > SIP > SIP Account > Edit** to activate an SIP account (see Section 16.3.1 on page 183 for more information).

Figure 86 Phone Device: Edit



SIP Account to Make Outgoing Call

SIP Account	SIP Number	SIP Account	SIP Number
● SIP 1	ChangeMe	○ SIP 2	ChangeMe

SIP Account(s) to Receive Incomming Call

SIP Account	SIP Number	SIP Account	SIP Number
☑ SIP 1	ChangeMe	□ SIP 2	ChangeMe

FXO Interface to Receive Incomming Call

☑ Enable

The following table describes the labels in this screen.

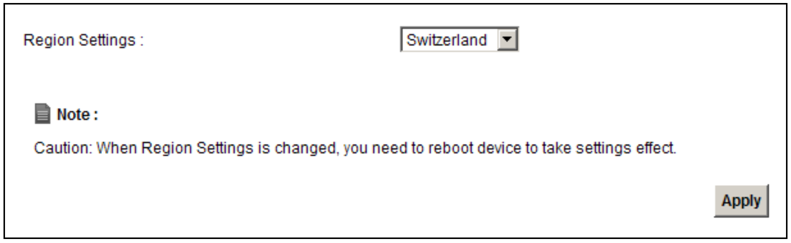
Table 52 Phone Device: Edit

LABEL	DESCRIPTION
SIP Account to Make Outgoing Call	
SIP Account	Select the SIP account you want to use when making outgoing calls with the analog phone connected to this phone port.
SIP Number	This shows the SIP account number.
SIP Account(s) to Receive Incoming Call	
SIP Account	Select a SIP account if you want to receive phone calls for the selected SIP account on this phone port. If you select more than one SIP account for incoming calls, there is no way to distinguish between them when you receive phone calls. If you do not select a source for incoming calls, you cannot receive any calls on this phone port.
SIP Number	This shows the SIP account number.
FXO Interface to Receive Incoming Call	
Enable	Select this if you want to receive phone calls from the PSTN line (that do not use the Internet) on this phone port.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen without saving.

16.6 The Region Screen

Use this screen to maintain settings that depend on which region of the world the ZyXEL Device is in. To access this screen, click **VoIP > Phone > Region**.

Figure 87 VoIP > Phone > Region



Region Settings : Switzerland

Note :

Caution: When Region Settings is changed, you need to reboot device to take settings effect.

Each field is described in the following table.

Table 53 VoIP > Phone > Region

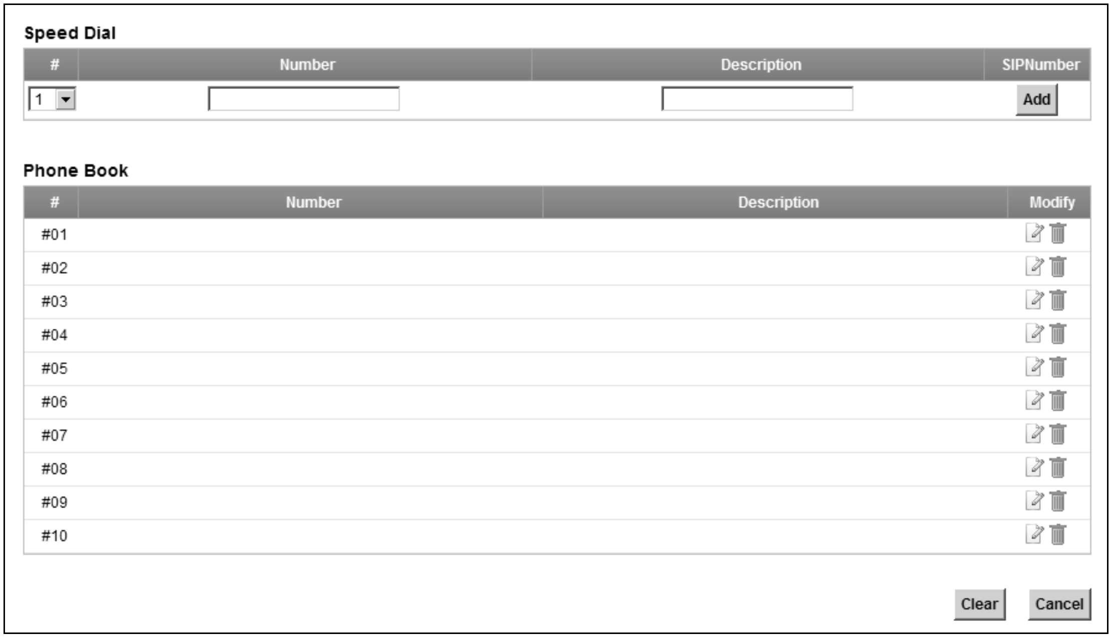
LABEL	DESCRIPTION
Region Settings	Select the place in which the ZyXEL Device is located.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

16.7 The Call Rule Screen

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

To access this screen, click **VoIP > Phone > Call Rule**.

Figure 88 VoIP > Phone > Call Rule



Each field is described in the following table.

Table 54 VoIP > Phone > Call Rule

LABEL	DESCRIPTION
Speed Dial	Use this section to create or edit speed-dial entries.
#	Select the speed-dial number you want to use for this phone number.
Number	Enter the SIP number you want the ZyXEL Device to call when you dial the speed-dial number.
Description	Enter a short description to identify the party you call when you dial the speed-dial number. You can use up to 127 printable ASCII characters.
Add	Click this to use the information in the **Speed Dial** section to update the **Speed Dial Phone Book** section.
Phone Book	Use this section to look at all the speed-dial entries and to erase them.
#	This field displays the speed-dial number you should dial to use this entry.

Table 54 VoIP > Phone > Call Rule (continued)

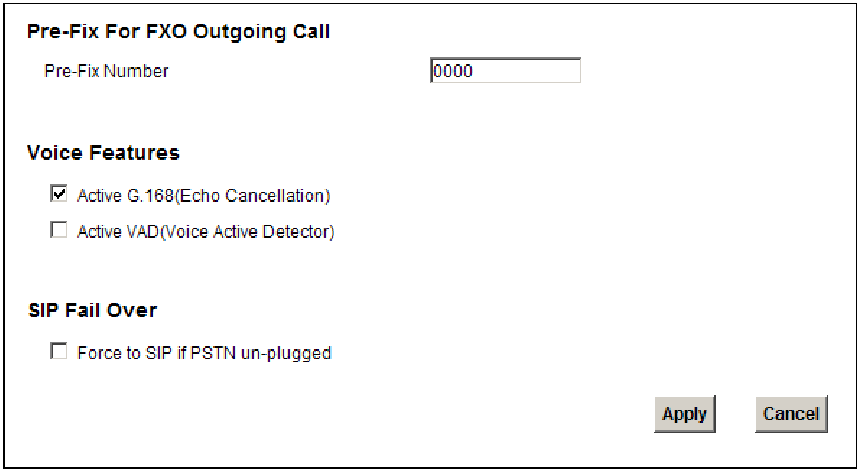
LABEL	DESCRIPTION
Number	This field displays the SIP number the ZyXEL Device calls when you dial the speed-dial number.
Description	This field displays a short description of the party you call when you dial the speed-dial number.
Modify	Use this field to edit or erase the speed-dial entry. Click the **Edit** icon to copy the information for this speed-dial entry into the **Speed Dial** section, where you can change it. Click **Add** when you finish editing to change the configurations. Click the **Delete** icon to erase this speed-dial entry.
Clear	Click this to erase all the speed-dial entries.
Cancel	Click this to set every field in this screen to its last-saved value.

16.8 The FXO Screen (“L” Models Only)

With PSTN line you can make and receive regular PSTN phone calls. Use a prefix number to make a regular call. When the device does not have power, you can make regular calls without dialing a prefix number.

Use the **FXO** screen to set up the PSTN line you use to make regular phone calls which do not use the Internet. To access this screen, click **VoIP > FXO**.

Figure 89 VoIP > FXO



Pre-Fix For FXO Outgoing Call

Pre-Fix Number: 0000

Voice Features

☑ Active G.168(Echo Cancellation)

☐ Active VAD(Voice Active Detector)

SIP Fail Over

☐ Force to SIP if PSTN un-plugged

Each field is described in the following table.

Table 55 VoIP > FXO

LABEL	DESCRIPTION
Pre-Fix For FXO Outgoing Call	
Pre-Fix Number	Enter 1 - 7 numbers you dial before you dial the phone number, if you want to make a regular phone call while one of your SIP accounts is registered. These numbers tell the ZyXEL Device that you want to make a regular phone call.
Voice Features	
Active G.168	Select this if you want to eliminate the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
Active VAD	Select this if the ZyXEL Device should stop transmitting when you are not speaking. This reduces the bandwidth the ZyXEL Device uses.
SIP Fail Over	
Force to SIP if PSTN un-plugged	Select this check box to have the ZyXEL Device redirect outgoing calls to the registered SIP account if the ZyXEL Device is not connected to the PSTN network. When you try to make a PSTN call, but the PSTN port on the ZyXEL Device is unplugged, the ZyXEL Device uses the phone port's registered SIP account to make the call.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

16.9 Technical Reference

This section contains background material relevant to the **VoIP** screens.

16.9.1 VoIP

VoIP is the sending of voice signals over Internet Protocol. This allows you to make phone calls and send faxes over the Internet at a fraction of the cost of using the traditional circuit-switched telephone network. You can also use servers to run telephone service applications like PBX services and voice mail. Internet Telephony Service Provider (ITSP) companies provide VoIP service.

Circuit-switched telephone networks require 64 kilobits per second (Kbps) in each direction to handle a telephone call. VoIP can use advanced voice coding techniques with compression to reduce the required bandwidth.

16.9.2 SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet.

SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

SIP Identities

A SIP account uses an identity (sometimes referred to as a SIP address). A complete SIP identity is called a SIP URI (Uniform Resource Identifier). A SIP account's URI identifies the SIP account in a way similar to the way an e-mail address identifies an e-mail account. The format of a SIP identity is SIP-Number@SIP-Service-Domain.

SIP Number

The SIP number is the part of the SIP URI that comes before the “@” symbol. A SIP number can use letters like in an e-mail address (johndoe@your-ITSP.com for example) or numbers like a telephone number (1122334455@VoIP-provider.com for example).

SIP Service Domain

The SIP service domain of the VoIP service provider is the domain name in a SIP URI. For example, if the SIP address is 1122334455@VoIP-provider.com, then “VoIP-provider.com” is the SIP service domain.

SIP Registration

Each ZyXEL Device is an individual SIP User Agent (UA). To provide voice service, it has a public IP address for SIP and RTP protocols to communicate with other servers.

A SIP user agent has to register with the SIP registrar and must provide information about the users it represents, as well as its current IP address (for the routing of incoming SIP requests). After successful registration, the SIP server knows that the users (identified by their dedicated SIP URIs) are represented by the UA, and knows the IP address to which the SIP requests and responses should be sent.

Registration is initiated by the User Agent Client (UAC) running in the VoIP gateway (the ZyXEL Device). The gateway must be configured with information letting it know where to send the REGISTER message, as well as the relevant user and authorization data.

A SIP registration has a limited lifespan. The User Agent Client must renew its registration within this lifespan. If it does not do so, the registration data will be deleted from the SIP registrar's database and the connection broken.

The ZyXEL Device attempts to register all enabled subscriber ports when it is switched on. When you enable a subscriber port that was previously disabled, the ZyXEL Device attempts to register the port immediately.

Authorization Requirements

SIP registrations (and subsequent SIP requests) require a username and password for authorization. These credentials are validated via a challenge / response system using the HTTP digest mechanism (as detailed in RFC3261, "SIP: Session Initiation Protocol").

SIP Servers

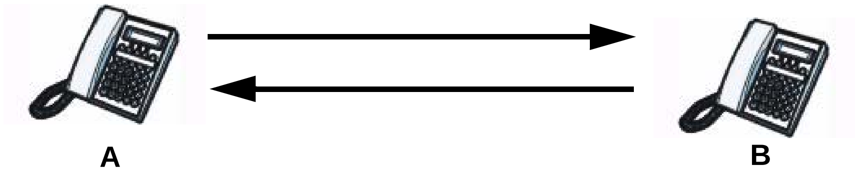
SIP is a client-server protocol. A SIP client is an application program or device that sends SIP requests. A SIP server responds to the SIP requests.

When you use SIP to make a VoIP call, it originates at a client and terminates at a server. A SIP client could be a computer or a SIP phone. One device can act as both a SIP client and a SIP server.

SIP User Agent

A SIP user agent can make and receive VoIP telephone calls. This means that SIP can be used for peer-to-peer communications even though it is a client-server protocol. In the following figure, either **A** or **B** can act as a SIP user agent client to initiate a call. **A** and **B** can also both act as a SIP user agent to receive the call.

Figure 90 SIP User Agent



SIP Proxy Server

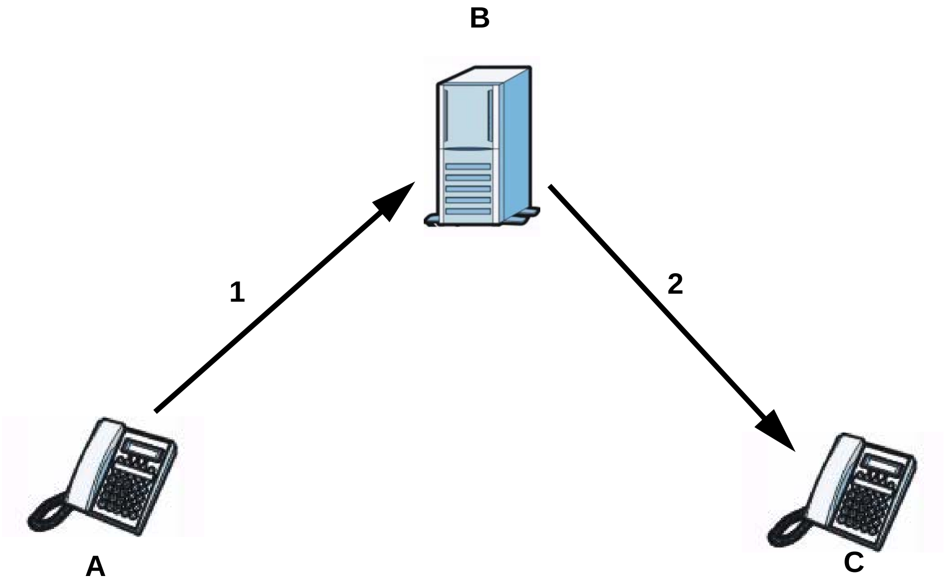
A SIP proxy server receives requests from clients and forwards them to another server.

In the following example, you want to use client device **A** to call someone who is using client device **C**.

1 The client device (**A** in the figure) sends a call invitation to the SIP proxy server **B**.

2 The SIP proxy server forwards the call invitation to **C**.

Figure 91 SIP Proxy Server



SIP Redirect Server

A SIP redirect server accepts SIP requests, translates the destination address to an IP address and sends the translated IP address back to the device that sent the request. Then the client device that originally sent the request can send requests to the IP address that it received back from the redirect server. Redirect servers do not initiate SIP requests.

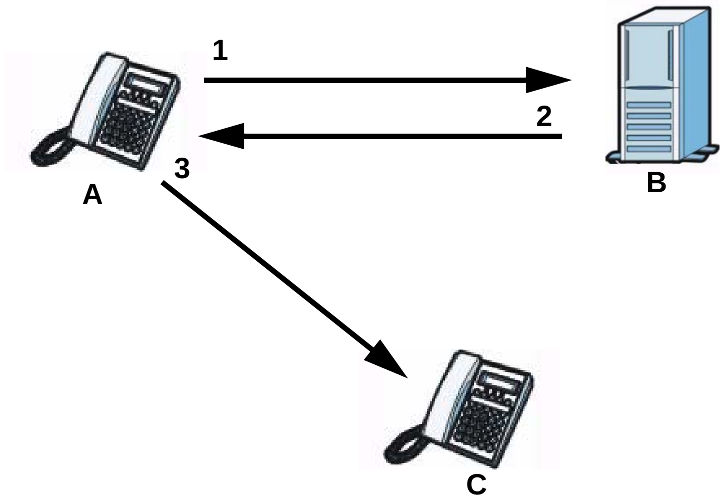
In the following example, you want to use client device **A** to call someone who is using client device **C**.

1 Client device **A** sends a call invitation for **C** to the SIP redirect server **B**.

2 The SIP redirect server sends the invitation back to **A** with **C**’s IP address (or domain name).

3 Client device **A** then sends the call invitation to client device **C**.

Figure 92 SIP Redirect Server



SIP Register Server

A SIP register server maintains a database of SIP identity-to-IP address (or domain name) mapping. The register server checks your user name and password when you register.

RTP

When you make a VoIP call using SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 3550 for details on RTP.

Pulse Code Modulation

Pulse Code Modulation (PCM) measures analog signal amplitudes at regular time intervals and converts them into bits.

SIP Call Progression

The following figure displays the basic steps in the setup and tear down of a SIP call. A calls B.

Table 56 SIP Call Progression

A		B
1. INVITE	→	
	←	2. Ringing
	←	3. OK
4. ACK	→	

Table 56 SIP Call Progression (continued)

A		B
	5.Dialogue (voice traffic)	
6. BYE	→	
	←	7. OK

1 **A** sends a SIP INVITE request to **B**. This message is an invitation for **B** to participate in a SIP telephone call.

2 **B** sends a response indicating that the telephone is ringing.

3 **B** sends an OK response after the call is answered.

4 **A** then sends an ACK message to acknowledge that **B** has answered the call.

5 Now **A** and **B** exchange voice media (talk).

6 After talking, **A** hangs up and sends a BYE request.

7 **B** replies with an OK response confirming receipt of the BYE request and the call is terminated.

Voice Coding

A codec (coder/decoder) codes analog voice signals into digital signals and decodes the digital signals back into analog voice signals. The ZyXEL Device supports the following codecs.

- G.711 is a Pulse Code Modulation (PCM) waveform codec. PCM measures analog signal amplitudes at regular time intervals and converts them into digital samples. G.711 provides very good sound quality but requires 64 kbps of bandwidth.
- G.726 is an Adaptive Differential PCM (ADPCM) waveform codec that uses a lower bitrate than standard PCM conversion. ADPCM converts analog audio into digital signals based on the difference between each audio sample and a prediction based on previous samples. The more similar the audio sample is to the prediction, the less space needed to describe it. G.726 operates at 16, 24, 32 or 40 kbps.
- G.729 is an Analysis-by-Synthesis (AbS) hybrid waveform codec that uses a filter based on information about how the human vocal tract produces sounds. G.729 provides good sound quality and reduces the required bandwidth to 8 kbps.

PSTN Call Setup Signaling

Dual-Tone MultiFrequency (DTMF) signaling uses pairs of frequencies (one lower frequency and one higher frequency) to set up calls. It is also known as Touch Tone®. Each of the keys on a DTMF telephone corresponds to a different pair of frequencies.

Pulse dialing sends a series of clicks to the local phone office in order to dial numbers.[3]

MWI (Message Waiting Indication)

Enable Message Waiting Indication (MWI) enables your phone to give you a message–waiting (beeping) dial tone when you have a voice message(s). Your VoIP service provider must have a messaging system that sends message waiting status SIP packets as defined in RFC 3842.

16.9.3 Quality of Service (QoS)

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to provide bandwidth for real-time multimedia applications.

Type of Service (ToS)

Network traffic can be classified by setting the ToS (Type of Service) values at the data source (for example, at the ZyXEL Device) so a server can decide the best method of delivery, that is the least cost, fastest route and so on.

DiffServ

DiffServ 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 (DSCP) 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.[4]

[3] The ZyXEL Device does not support pulse dialing at the time of writing.

[4] The ZyXEL Device does not support DiffServ at the time of writing.

DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) 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.

Figure 93 DiffServ: Differentiated Service Field

DSCP (6-bit)	Unused (2-bit)

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 priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

VLAN Tagging

Virtual Local Area Network (VLAN) allows a physical network to be partitioned into multiple logical networks. Only stations within the same group can communicate with each other.

Your ZyXEL Device can add IEEE 802.1Q VLAN ID tags to voice frames that it sends to the network. This allows the ZyXEL Device to communicate with a SIP server that is a member of the same VLAN group. Some ISPs use the VLAN tag to identify voice traffic and give it priority over other traffic.

16.9.4 Phone Services Overview

Supplementary services such as call hold, call waiting, and call transfer. are generally available from your VoIP service provider. The ZyXEL Device supports the following services:

- Call Hold
- Call Waiting
- Making a Second Call
- Call Transfer
- Three-Way Conference

- Internal Calls
- Do not Disturb

Note: To take full advantage of the supplementary phone services available through the ZyXEL Device's phone ports, you may need to subscribe to the services from your VoIP service provider.

The Flash Key

Flashing means to press the hook for a short period of time (a few hundred milliseconds) before releasing it. On newer telephones, there should be a "flash" key (button) that generates the signal electronically. If the flash key is not available, you can tap (press and immediately release) the hook by hand to achieve the same effect. However, using the flash key is preferred since the timing is much more precise. With manual tapping, if the duration is too long, it may be interpreted as hanging up by the ZyXEL Device.

You can invoke all the supplementary services by using the flash key.

Europe Type Supplementary Phone Services

This section describes how to use supplementary phone services with the **Europe Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command time-out (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

Table 57 European Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash		Put a current call on hold to place a second call. Switch back to the call (if there is no second call).
Flash	0	Drop the call presently on hold or reject an incoming call which is waiting for answer.
Flash	1	Disconnect the current phone connection and answer the incoming call or resume with caller presently on hold.
Flash	2	1. Switch back and forth between two calls. 2. Put a current call on hold to answer an incoming call. 3. Separate the current three-way conference call into two individual calls (one is on-line, the other is on hold).
Flash	3	Create three-way conference connection.
Flash	*98#	Transfer the call to another phone.

European Call Hold

Call hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key and then “2” to switch back and forth between caller **A** and **B** by putting either one on hold.

Press the flash key and then “0” to disconnect the call presently on hold and keep the current call on line.

Press the flash key and then “1” to disconnect the current call and resume the call on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

European Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to a telephone number, you will hear a call waiting tone. Take one of the following actions.

- Reject the second call.

  Press the flash key and then press “0”.
- Disconnect the first call and answer the second call.

  Either press the flash key and press “1”, or just hang up the phone and then answer the phone after it rings.
- Put the first call on hold and answer the second call.

  Press the flash key and then “2”.

European Call Transfer

Do the following to transfer a call (that you have answered) to another phone number.

1 Press the flash key to put the caller on hold.

2 When you hear the dial tone, dial “*98#” followed by the number to which you want to transfer the call. to operate the Intercom.

3 After you hear the ring signal or the second party answers it, hang up the phone.

European Three-Way Conference

Use the following steps to make three-way conference calls.

1 When you are on the phone talking to someone, press the flash key to put the call on hold and get a dial tone.

2 Dial a phone number directly to make another call.

3 When the second call is answered, press the flash key and press “3” to create a three-way conversation.

4 Hang up the phone to drop the connection.

5 If you want to separate the activated three-way conference into two individual connections (one is on-line, the other is on hold), press the flash key and press “2”.

17

Logs

17.1 Overview

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.

Note: The ZyXEL Device’s log feature is only for Voice over IP (VoIP).

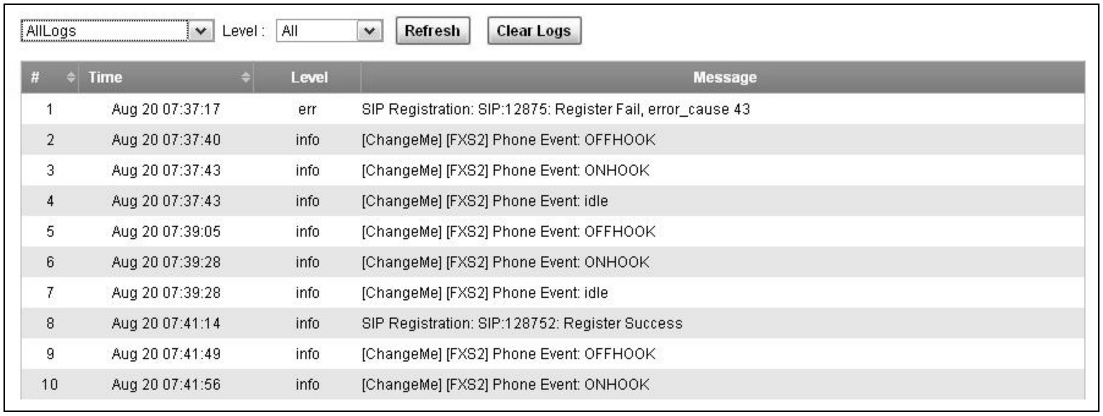
17.1.1 What You Can Do in this Chapter

- Use the **Phone Log** screen to view phone logs and alert messages (Section 17.2 on page 203).
- Use The **VoIP Call History** screen to view the details of the calls performed on the ZyXEL Device (Section 17.3 on page 204).

17.2 The Phone Log Screen

Click **System Monitor > Log** to open the **Phone Log** screen. Use this screen to view phone logs and alert messages. You can select the type of log and level of severity to display.

Figure 94 System Monitor > Log > Phone Log



AllLogs Level : All

#	Time	Level	Message
1	Aug 20 07:37:17	err	SIP Registration: SIP:12875: Register Fail, error_cause 43
2	Aug 20 07:37:40	info	[ChangeMe] [FXS2] Phone Event: OFFHOOK
3	Aug 20 07:37:43	info	[ChangeMe] [FXS2] Phone Event: ONHOOK
4	Aug 20 07:37:43	info	[ChangeMe] [FXS2] Phone Event: idle
5	Aug 20 07:39:05	info	[ChangeMe] [FXS2] Phone Event: OFFHOOK
6	Aug 20 07:39:28	info	[ChangeMe] [FXS2] Phone Event: ONHOOK
7	Aug 20 07:39:28	info	[ChangeMe] [FXS2] Phone Event: idle
8	Aug 20 07:41:14	info	SIP Registration: SIP:128752: Register Success
9	Aug 20 07:41:49	info	[ChangeMe] [FXS2] Phone Event: OFFHOOK
10	Aug 20 07:41:56	info	[ChangeMe] [FXS2] Phone Event: ONHOOK

The following table describes the fields in this screen.

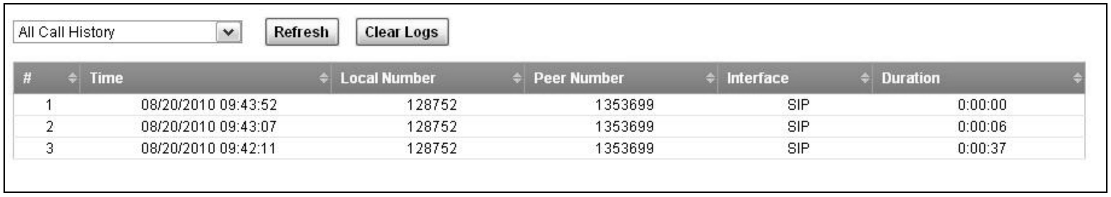
Table 58 System Monitor > Log > Phone Log

LABEL	DESCRIPTION
	Select a category of logs to view from the drop-down list box. select **All Logs** to view all logs.
Level	Select the severity level that you want to view.
Refresh	Click this to renew the log screen.
Clear Logs	Click this to delete all the logs.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Message	This field states the reason for the log.

17.3 The VoIP Call History Screen

Click **System Monitor > Log > Call History** to open the **VoIP Call History** screen. Use this screen to see the details of the calls performed on the ZyXEL Device.

Figure 95 System Monitor > Log > Call History



#	Time	Local Number	Peer Number	Interface	Duration
1	08/20/2010 09:43:52	128752	1353699	SIP	0:00:00
2	08/20/2010 09:43:07	128752	1353699	SIP	0:00:06
3	08/20/2010 09:42:11	128752	1353699	SIP	0:00:37

The following table describes the fields in this screen.

Table 59 System Monitor > Log > Call History

LABEL	DESCRIPTION
	Select a category of call records to view from the drop-down list box. select **All Call History** to view all call records.
Refresh	Click this to renew the log screen.
Clear Logs	Click this to delete all the logs.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the call was recorded.
Local Number	This field displays the phone number you used to make or receive this call.
Peer Number	This field displays the phone number you called or from which this call is made.

Table 59 System Monitor > Log > Call History

LABEL	DESCRIPTION
Interface	This field displays the type of the call.
Duration	This field displays how long the call lasted.

18

System Monitor

18.1 Overview

Use the **Traffic Status** and **VoIP Status** screens to look at network traffic status and statistics of the WAN, LAN interfaces, NAT, and VoIP.

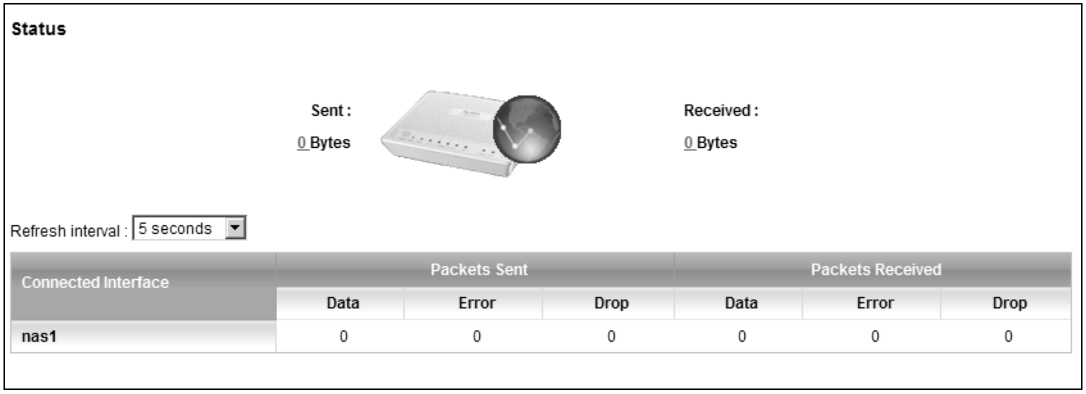
18.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics (Section 18.2 on page 207) .
- Use the **LAN** screen to view the LAN traffic statistics (Section 18.3 on page 208).
- Use the **NAT** screen to view the NAT status of the ZyXEL Device's client(s) (Section 18.4 on page 209).
- Use the **VoIP Status** screen to view the VoIP traffic statistics (Section 18.5 on page 210).

18.2 The WAN Status Screen

Click **System Monitor > Traffic Status** to open the **WAN** screen. You can view the WAN traffic statistics in this screen.

Figure 96 System Monitor > Traffic Status > WAN



Status

Sent : 0 Bytes

Received : 0 Bytes

Refresh interval : 5 seconds

Connected Interface	Packets Sent			Packets Received		
	Data	Error	Drop	Data	Error	Drop
nas1	0	0	0	0	0	0

The following table describes the fields in this screen.

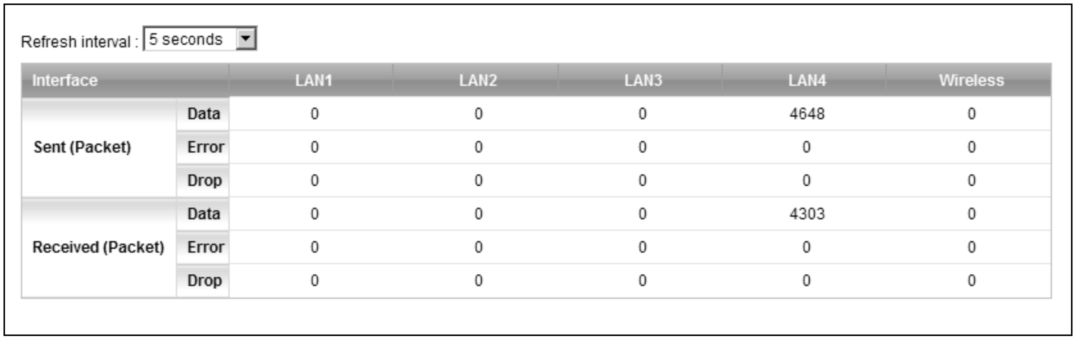
Table 60 System Monitor > Traffic Status > WAN

LABEL	DESCRIPTION
Status	This shows the number of bytes received and sent through the WAN interface of the ZyXEL Device.
Refresh Interval	Select how often you want the ZyXEL Device to update this screen from the drop-down list box.
Connected Interface	This shows the name of the WAN interface that is currently connected.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

18.3 The LAN Status Screen

Click **System Monitor > Traffic Status > LAN** to open the following screen. You can view the LAN traffic statistics in this screen.

Figure 97 System Monitor > Traffic Status > LAN



Refresh interval : 5 seconds

Interface		LAN1	LAN2	LAN3	LAN4	Wireless
Sent (Packet)	Data	0	0	0	4648	0
	Error	0	0	0	0	0
	Drop	0	0	0	0	0
Received (Packet)	Data	0	0	0	4303	0
	Error	0	0	0	0	0
	Drop	0	0	0	0	0

The following table describes the fields in this screen.

Table 61 System Monitor > Traffic Status > LAN

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the ZyXEL Device to update this screen from the drop-down list box.
Interface	This shows the LAN or WLAN interface.

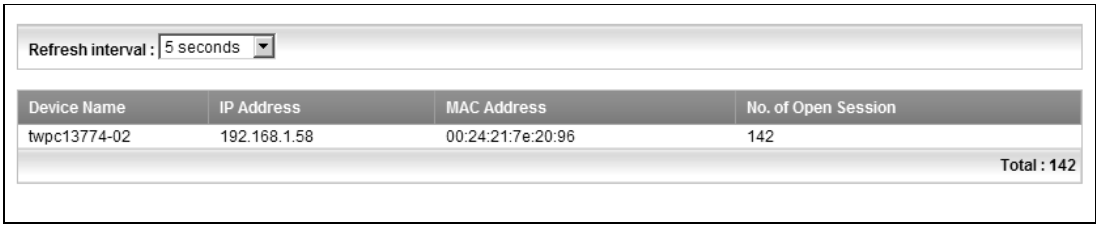
Table 61 System Monitor > Traffic Status > LAN (continued)

LABEL	DESCRIPTION
Sent (Packet)	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Received (Packet)	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

18.4 The NAT Status Screen

Click **System Monitor > Traffic Status > NAT** to open the following screen. You can view the NAT status of the ZyXEL Device's client(s) in this screen.

Figure 98 System Monitor > Traffic Status > NAT



Refresh interval : 5 seconds

Device Name	IP Address	MAC Address	No. of Open Session
twpc13774-02	192.168.1.58	00:24:21:7e:20:96	142

Total : 142

The following table describes the fields in this screen.

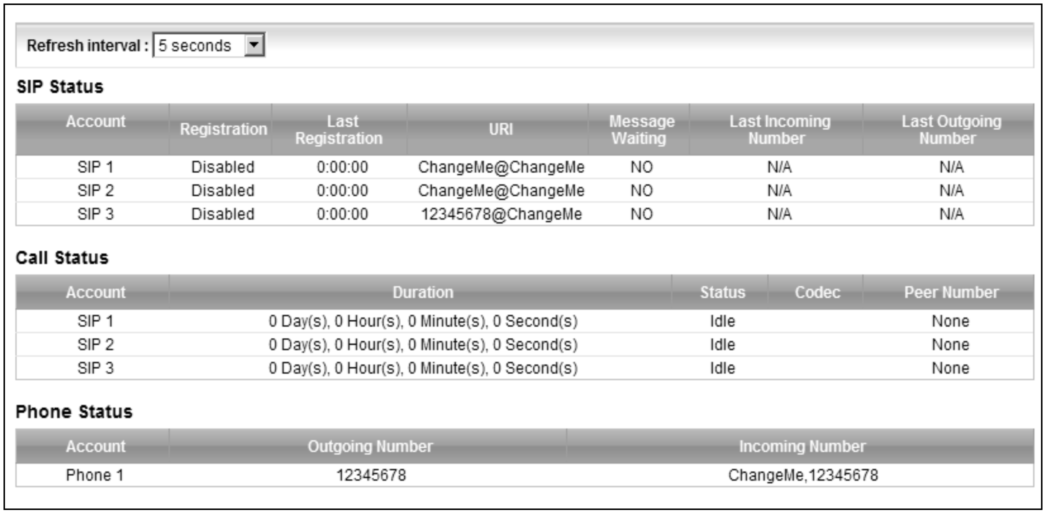
Table 62 System Monitor > Traffic Status > NAT

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the ZyXEL Device to update this screen from the drop-down list box.
Device Name	This shows the name of the client.
IP Address	This shows the IP address of the client.
MAC Address	This shows the MAC address of the client.
No. of Open Session	This shows the number of NAT sessions used by the client.

18.5 The VoIP Status Screen

Click **System Monitor > VoIP Status** to open the following screen. You can view the VoIP traffic statistics in this screen.

Figure 99 System Monitor > VoIP Status



Refresh interval : 5 seconds

SIP Status

Account	Registration	Last Registration	URI	Message Waiting	Last Incoming Number	Last Outgoing Number
SIP 1	Disabled	0:00:00	ChangeMe@ChangeMe	NO	N/A	N/A
SIP 2	Disabled	0:00:00	ChangeMe@ChangeMe	NO	N/A	N/A
SIP 3	Disabled	0:00:00	12345678@ChangeMe	NO	N/A	N/A

Call Status

Account	Duration	Status	Codec	Peer Number
SIP 1	0 Day(s), 0 Hour(s), 0 Minute(s), 0 Second(s)	Idle		None
SIP 2	0 Day(s), 0 Hour(s), 0 Minute(s), 0 Second(s)	Idle		None
SIP 3	0 Day(s), 0 Hour(s), 0 Minute(s), 0 Second(s)	Idle		None

Phone Status

Account	Outgoing Number	Incoming Number
Phone 1	12345678	ChangeMe,12345678

The following table describes the fields in this screen.

Table 63 System Monitor > VoIP Status

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the ZyXEL Device to update this screen from the drop-down list box.
SIP Status	
Account	This column displays each SIP account in the ZyXEL Device.
Registration	This field displays the current registration status of the SIP account. You can change this in the **System Info** screen. **Registered** - The SIP account is registered with a SIP server. **Disabled** - The last time the ZyXEL Device tried to register the SIP account with the SIP server, the attempt failed. The ZyXEL Device automatically tries to register the SIP account when you turn on the ZyXEL Device or when you activate it. **Inactive** - The SIP account is not active. You can activate it in **VoIP > SIP > SIP Account**.
Last Registration	This field displays the last time you successfully registered the SIP account. The field is blank if you never successfully registered this account.
URI	This field displays the account number and service domain of the SIP account. You can change these in the **VoIP > SIP** screens.
Message Waiting	This field indicates whether or not there are any messages waiting for the SIP account.

Table 63 System Monitor > VoIP Status (continued)

LABEL	DESCRIPTION
Last Incoming Number	This field displays the last number that called the SIP account. The field is blank if no number has ever dialed the SIP account.
Last Outgoing Number	This field displays the last number the SIP account called. The field is blank if the SIP account has never dialed a number.
Call Status	
Account	This column displays each SIP account in the ZyXEL Device.
Duration	This field displays how long the current call has lasted.
Status	This field displays the current state of the phone call. **Idle** - There are no current VoIP calls, incoming calls or outgoing calls being made. **Dial** - The callee's phone is ringing. **Ring** - The phone is ringing for an incoming VoIP call. **InCall** - There is a VoIP call in progress. **DISC** - The callee's line is busy, the callee hung up or your phone was left off the hook.
Codec	This field displays what voice codec is being used for a current VoIP call through a phone port.
Peer Number	This field displays the SIP number of the party that is currently engaged in a VoIP call through a phone port.
Phone Status	
Account	This field displays the phone accounts of the ZyXEL Device.
Outgoing Number	This field displays the SIP number that you use to make calls on this phone port.
Incoming Number	This field displays the SIP number that you use to receive calls on this phone port.

19

User Account

19.1 Overview

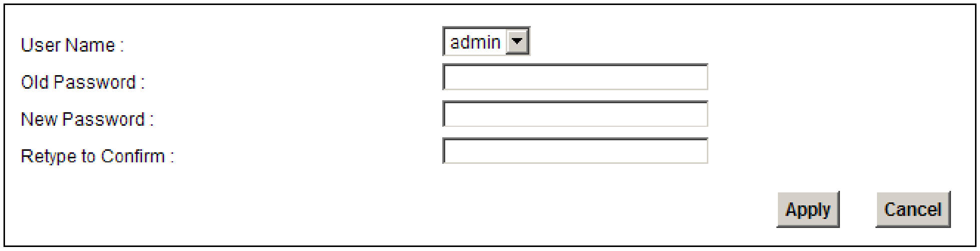
You can configure system password for different user accounts in the **User Account** screen.

19.2 The User Account Screen

Use the **User Account** screen to configure system password.

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

Figure 100 Maintenance > User Account



User Name : admin

Old Password :

New Password :

Retype to Confirm :

The following table describes the labels in this screen.

Table 64 Maintenance > User Account

LABEL	DESCRIPTION
User Name	You can configure the password for the admin or user account . Select **admin** or **user** from the drop-down list box.
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.

Table 64 Maintenance > User Account (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

20

Remote MGMT

20.1 Overview

Remote MGMT allows you to manage your ZyXEL Device from a remote location through the following interfaces:

- LAN and WLAN
- WAN only

Note: The ZyXEL Device is managed using the web configurator.

20.1.1 What You Need to Know

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

TR-064

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

SSH/SCP/SFTP

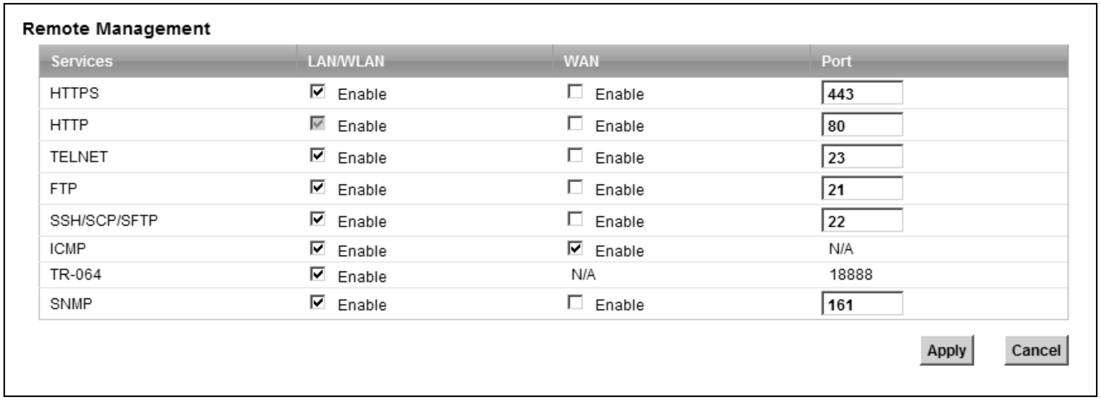
Secure Shell (SSH) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network. The following file transfer methods use SSH:

- **Secure Copy (SC)** is a secure way of transferring files between computers. It uses port 22.
- **SSH File Transfer Protocol or Secure File Transfer Protocol (SFTP)** is an old way of transferring files between computers. It uses port 22.

20.2 The Remote MGMT Screen

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

Figure 101 Maintenance > Remote MGMT



Remote Management

Services	LAN/WLAN	WAN	Port
HTTPS	☑ Enable	□ Enable	443
HTTP	☑ Enable	□ Enable	80
TELNET	☑ Enable	□ Enable	23
FTP	☑ Enable	□ Enable	21
SSH/SCP/SFTP	☑ Enable	□ Enable	22
ICMP	☑ Enable	☑ Enable	N/A
TR-064	☑ Enable	N/A	18888
SNMP	☑ Enable	□ Enable	161

The following table describes the fields in this screen.

Table 65 Maintenance > Remote MGMT

LABEL	DESCRIPTION
Services	This is the service you may use to access the ZyXEL Device.
LAN/WLAN	Select the **Enable** check box for the corresponding services that you want to allow access to the ZyXEL Device from the LAN and WLAN.
WAN	Select the **Enable** check box for the corresponding services that you want to allow access to the ZyXEL Device from the WAN.
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

21

SNMP

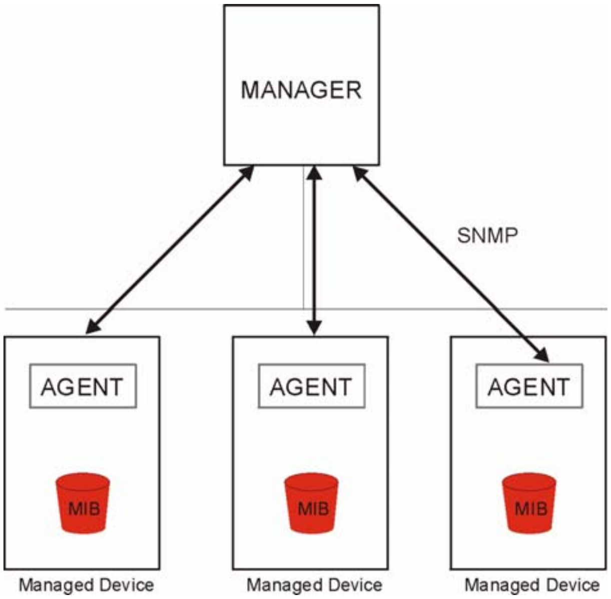
21.1 Overview

This chapter explains how to configure the SNMP settings on the ZyXEL Device.

21.2 The SNMP Screen

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your ZyXEL Device supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyXEL Device through the network. The ZyXEL Device supports SNMP version one (SNMPv1) and version two (SNMPv2c). The next figure illustrates an SNMP management operation.

Figure 102 SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the ZyXEL Device). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

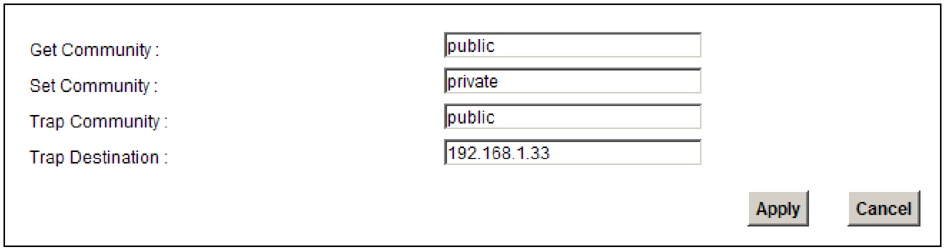
The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

Click **Maintenance > SNMP** to open the following screen. Use this screen to configure the ZyXEL Device SNMP settings.

Figure 103 Maintenance > SNMP



Get Community : public
Set Community : private
Trap Community : public
Trap Destination : 192.168.1.33

The following table describes the fields in this screen.

Table 66 Maintenance > SNMP

LABEL	DESCRIPTION
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the **Set community**, which is the password for incoming Set requests from the management station. The default is public and allows all requests.
Trap Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.

Table 66 Maintenance > SNMP (continued)

LABEL	DESCRIPTION
Trap Destination	Type the IP address of the station to send your SNMP traps to.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to restore your previously saved settings.

22

System

22.1 Overview

You can configure system settings, including the host name, domain name and the inactivity time-out interval in the **System** screen.

22.1.1 What You Need to Know

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

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”.

22.2 The System Screen

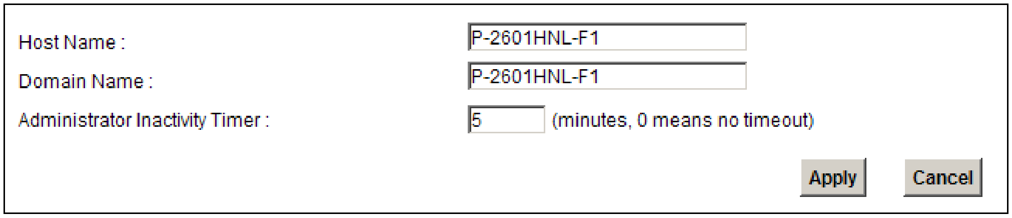
Use the **System** screen to configure the system’s host name, domain name, and inactivity time-out interval.

The **Host Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name". Find the system name of your Windows computer.

In Windows XP, click **start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the ZyXEL Device **System Name**.

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

Figure 104 Maintenance > System



Host Name :	P-2601HNL-F1
Domain Name :	P-2601HNL-F1
Administrator Inactivity Timer :	5 (minutes, 0 means no timeout)

The following table describes the labels in this screen.

Table 67 Maintenance > System

LABEL	DESCRIPTION
Host Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Administrator Inactivity Timer	Type how many minutes a management session (either via the web configurator) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Apply	Click this to save your changes back to the ZyXEL Device.
Cancel	Click this to begin configuring this screen afresh.

23

Time Setting

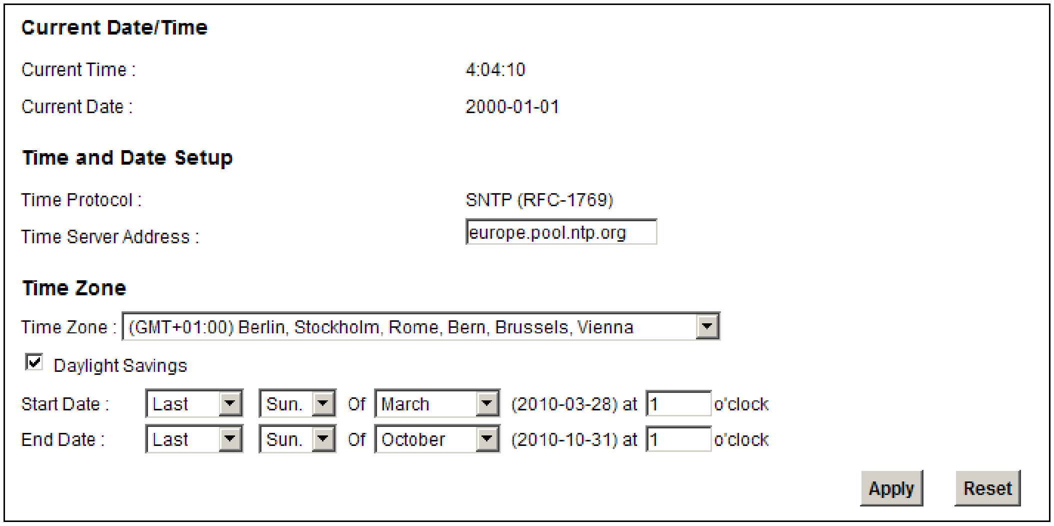
23.1 Overview

You can configure the system's time and date in the **Time Setting** screen.

23.2 The Time Setting Screen

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

Figure 105 Maintenance > Time Setting



Current Date/Time

Current Time : 4:04:10

Current Date : 2000-01-01

Time and Date Setup

Time Protocol : SNTP (RFC-1769)

Time Server Address : europe.pool.ntp.org

Time Zone

Time Zone : (GMT+01:00) Berlin, Stockholm, Rome, Bern, Brussels, Vienna

☑ Daylight Savings

Start Date : Last Sun. Of March (2010-03-28) at 1 o'clock

End Date : Last Sun. Of October (2010-10-31) at 1 o'clock

The following table describes the fields in this screen.

Table 68 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Current Date/Time	
Current Time	This field displays the time of your ZyXEL Device.
Current Date	This field displays the date of your ZyXEL Device.
Time and Date Setup	

Table 68 Maintenance > System > Time Setting (continued)

LABEL	DESCRIPTION
Time Protocol	This shows the time service protocol that your time server sends when you turn on the ZyXEL Device.
Time Server Address	Enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and type **2** in the **o'clock** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type **2** because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and type **2** in the **o'clock** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type **2** because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

24

Log Setting

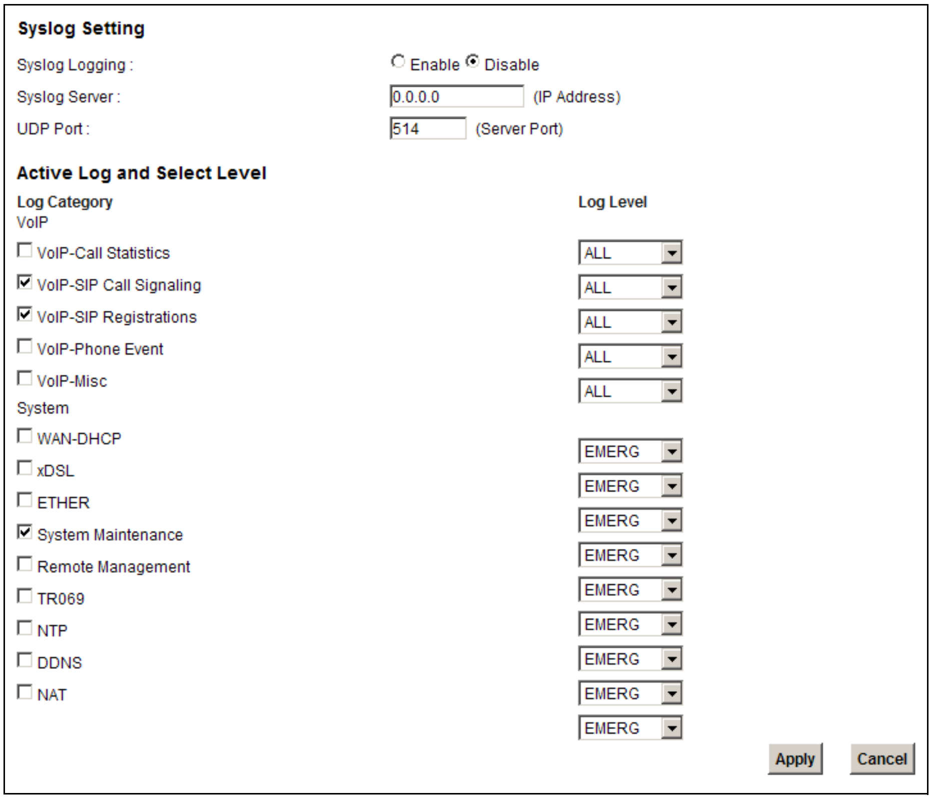
24.1 Overview

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

24.2 The Log Setting Screen

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

Figure 106 Maintenance > Log Setting



Syslog Setting

Syslog Logging :	○ Enable ● Disable
Syslog Server :	0.0.0.0 (IP Address)
UDP Port :	514 (Server Port)

Active Log and Select Level

Log Category	Log Level
VoIP	
□ VoIP-Call Statistics	ALL
☑ VoIP-SIP Call Signaling	ALL
☑ VoIP-SIP Registrations	ALL
□ VoIP-Phone Event	ALL
□ VoIP-Misc	ALL
System	
□ WAN-DHCP	EMERG
□ xDSL	EMERG
□ ETHER	EMERG
☑ System Maintenance	EMERG
□ Remote Management	EMERG
□ TR069	EMERG
□ NTP	EMERG
□ DDNS	EMERG
□ NAT	EMERG
	EMERG

The following table describes the fields in this screen.

Table 69 Maintenance > Log Setting

LABEL	DESCRIPTION
Syslog Logging	The ZyXEL Device sends a log to an external syslog server. Select the **Enable** check box to enable syslog logging.
Syslog Server	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
UDP Port	Enter the port number used by the syslog server.
Active Log and Select Level	
Log Category	Select the categories of logs that you want to record.
Log Level	Select the severity level of logs that you want to record. If you want to record all logs, select **ALL**.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

25

Firmware Upgrade

25.1 Overview

This chapter explains how to upload new firmware to your ZyXEL Device. You can download new firmware releases from your nearest ZyXEL FTP site (or www.zyxel.com) to use to upgrade your device's performance.

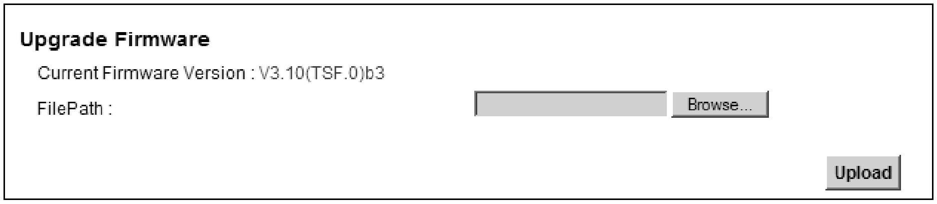
Only use firmware for your device's specific model. Refer to the label on the bottom of your ZyXEL Device.

25.2 The Firmware Upgrade Screen

Click **Maintenance > Firmware Upgrade** to open the following screen. 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 107 Maintenance > Firmware Upgrade



Upgrade Firmware

Current Firmware Version : V3.10(TSF.0)b3

FilePath :

The following table describes the labels in this screen.

Table 70 Maintenance > Firmware Upgrade

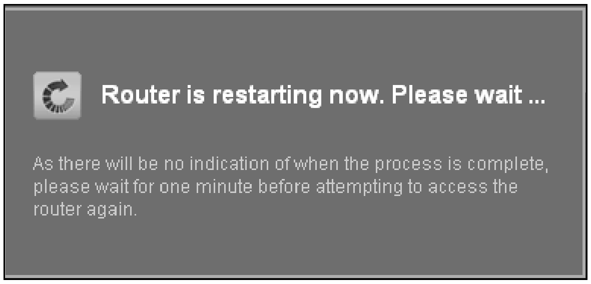
LABEL	DESCRIPTION
Current Firmware Version	This is the present Firmware version.
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.

Table 70 Maintenance > Firmware Upgrade (continued)

LABEL	DESCRIPTION
Browse...	Click this to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click this to begin the upload process. This process may take up to two minutes.

After you see the firmware updating screen, wait five minutes before logging into the ZyXEL Device again.

Figure 108 Firmware Uploading

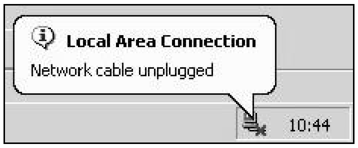


Router is restarting now. Please wait ...

As there will be no indication of when the process is complete, please wait for one minute before attempting to access the router again.

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

Figure 109 Network Temporarily Disconnected



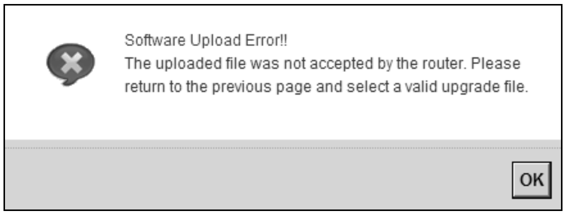
Local Area Connection

Network cable unplugged

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

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

Figure 110 Error Message



Software Upload Error!!

The uploaded file was not accepted by the router. Please return to the previous page and select a valid upgrade file.

26

Backup/Restore

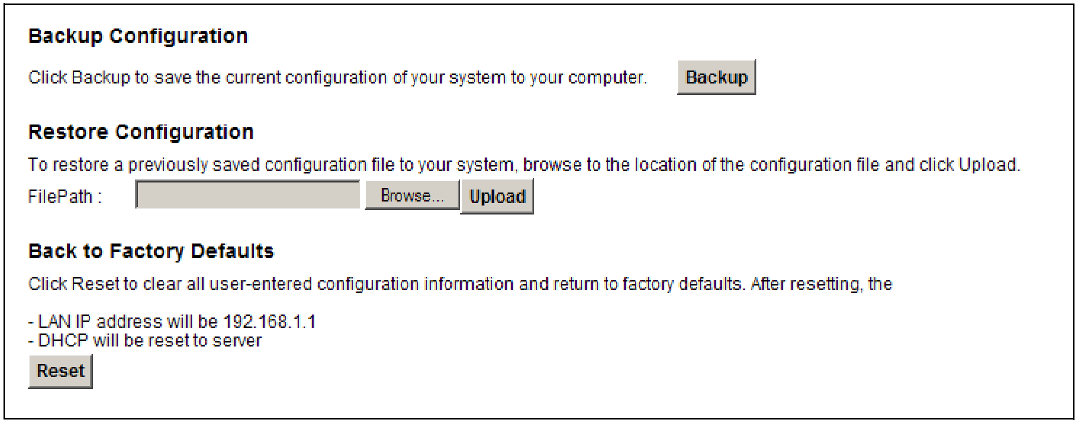
26.1 Overview

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

26.2 The Backup/Restore Screen

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

Figure 111 Maintenance > Backup/Restore



Backup Configuration

Click Backup to save the current configuration of your system to your computer.

Restore Configuration

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.

FilePath :

Back to Factory Defaults

Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the

- LAN IP address will be 192.168.1.1
- DHCP will be reset to server

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 71 Restore Configuration

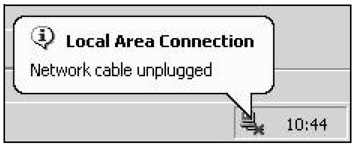
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click this to begin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

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

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

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

Figure 112 Network Temporarily Disconnected



Local Area Connection

Network cable unplugged

10:44

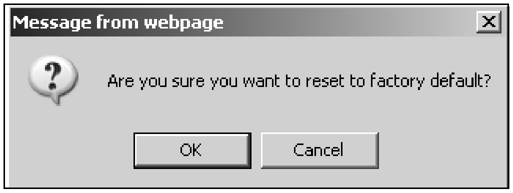
If you restore the default configuration, you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1). See Appendix B on page 265 for details on how to set up your computer's IP address.

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

Reset to Factory Defaults

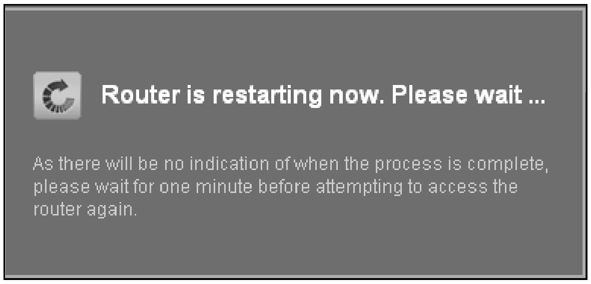
Click the **Reset** button to clear all user-entered configuration information and return the ZyXEL Device to its factory defaults. The following warning screen appears.

Figure 113 Reset Warning Message



Are you sure you want to reset to factory default?

Figure 114 Reset In Process Message



Router is restarting now. Please wait ...

As there will be no indication of when the process is complete, please wait for one minute before attempting to access the router again.

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

26.3 The Reboot Screen

System restart allows you to reboot the ZyXEL Device remotely without turning the power off. You may need to do this if the ZyXEL Device hangs, for example.

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

Diagnostic

27.1 Overview

You can use different diagnostic methods to test a connection and see the detailed information. These read-only screens display information to help you identify problems with the ZyXEL Device.

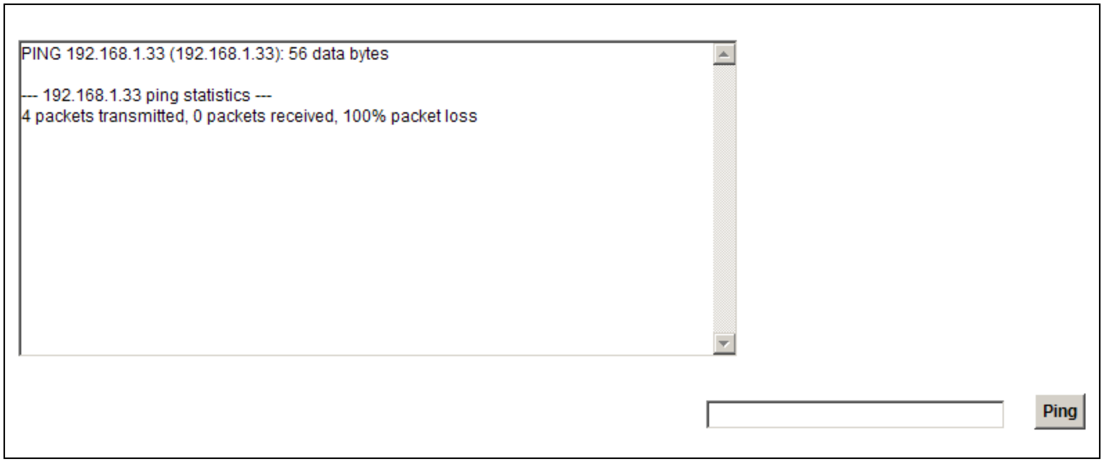
27.1.1 What You Can Do in this Chapter

- Use the **Ping** screen to ping an IP address and see the ping statistics (Section 27.2 on page 233).
- Use the **DSL Line** screen to check or reset your DSL connection (Section 27.3 on page 234).

27.2 The Ping Screen

Use this screen to ping an IP address. Click **Maintenance > Diagnostic** to open the **Ping** screen shown next.

Figure 115 Maintenance > Diagnostic > Ping



```
PING 192.168.1.33 (192.168.1.33): 56 data bytes

--- 192.168.1.33 ping statistics ---
4 packets transmitted, 0 packets received, 100% packet loss
```

The following table describes the fields in this screen.

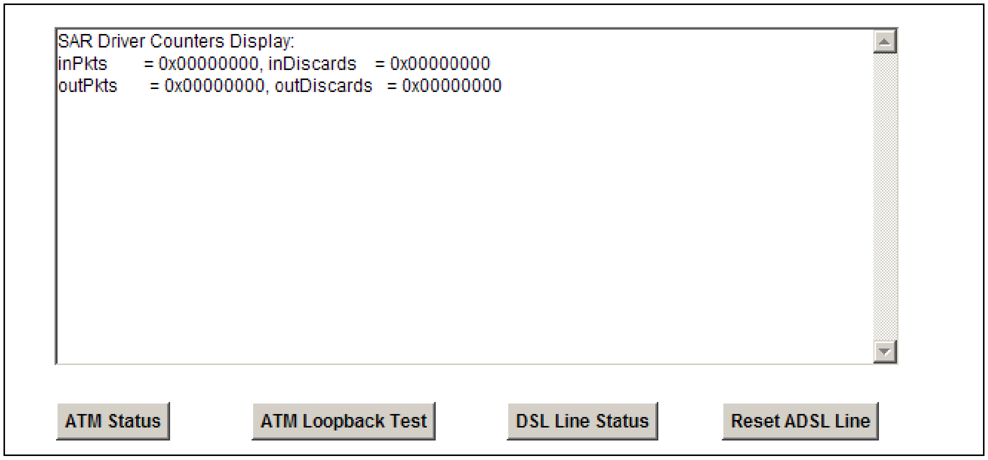
Table 72 Maintenance > Diagnostic > Ping

LABEL	DESCRIPTION
Ping	Type the IP address of a computer that you want to ping in order to test a connection. Click **Ping** and the ping statistics will show in the diagnostic .

27.3 The DSL Line Screen

Click **Maintenance > Diagnostic > DSL Line** to open the screen shown next.

Figure 116 Maintenance > Diagnostic > DSL Line



```
SAR Driver Counters Display:
inPkts      = 0x00000000, inDiscards   = 0x00000000
outPkts      = 0x00000000, outDiscards   = 0x00000000
```

The following table describes the fields in this screen.

Table 73 Maintenance > Diagnostic > DSL Line

ITEM	DESCRIPTION
ATM Status	Click this button to view your DSL connection's Asynchronous Transfer Mode (ATM) statistics. ATM is a networking technology that provides high-speed data transfer. ATM uses fixed-size packets of information called cells. With ATM, a high QoS (Quality of Service) can be guaranteed. The (Segmentation and Reassembly) SAR driver translates packets into ATM cells. It also receives ATM cells and reassembles them into packets. These counters are set back to zero whenever the device starts up. **inPkts** is the number of good ATM cells that have been received. **inDiscards** is the number of received ATM cells that were rejected. **outPkts** is the number of ATM cells that have been sent. **outDiscards** is the number of ATM cells sent that were rejected.
ATM Loopback Test	Click this button to start the ATM loopback test. Make sure you have configured at least one PVC with proper VPIs/VCIs before you begin this test. The ZyXEL Device sends an OAM F5 packet to the DSLAM/ATM switch and then returns it (loops it back) to the ZyXEL Device. The ATM loopback test is useful for troubleshooting problems with the DSLAM and ATM network.

Table 73 Maintenance > Diagnostic > DSL Line (continued)

ITEM	DESCRIPTION
DSL Line Status	Click this button to view statistics about the DSL connections. 1. **noise margin downstream** is the signal to noise ratio for the downstream part of the connection (coming into the ZyXEL Device from the ISP). It is measured in decibels. The higher the number the more signal and less noise there is. 2. **output power upstream** is the amount of power (in decibels) that the ZyXEL Device is using to transmit to the ISP. 3. **attenuation downstream** is the reduction in amplitude (in decibels) of the DSL signal coming into the ZyXEL Device from the ISP. Discrete Multi-Tone (DMT) modulation divides up a line's bandwidth into sub-carriers (sub-channels) of 4.3125 KHz each called tones. The rest of the display is the line's bit allocation. This is displayed as the number (in hexadecimal format) of bits transmitted for each tone. This can be used to determine the quality of the connection, whether a given sub-carrier loop has sufficient margins to support certain ADSL transmission rates, and possibly to determine whether particular specific types of interference or line attenuation exist. Refer to the ITU-T G.992.1 recommendation for more information on DMT. The better (or shorter) the line, the higher the number of bits transmitted for a DMT tone. The maximum number of bits that can be transmitted per DMT tone is 15. There will be some tones without any bits as there has to be space between the upstream and downstream channels.

Reset ADSL Line	Click this button to reinitialize the ADSL line. The large text box above then displays the progress and results of this operation, for example:
	`"Start to reset ADSL`
	`Loading ADSL modem F/W...`
	`Reset ADSL Line Successfully!"`

28

Troubleshooting

28.1 Overview

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
- Phone Calls and VoIP
- Wireless LAN Troubleshooting

28.2 Power, Hardware Connections, and LEDs

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

1 Make sure the ZyXEL Device is turned on.

2 Make sure you are using the power adaptor or cord included with the ZyXEL Device.

3 Make sure the power adaptor or cord is connected to the ZyXEL Device and plugged in to an appropriate power source. Make sure the power source is turned on.

4 Turn the ZyXEL Device off and on.

5 If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.5 on page 24.
2. Check the hardware connections. See the Quick Start Guide.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Turn the ZyXEL Device off and on.
5. If the problem continues, contact the vendor.

28.3 ZyXEL Device Access and Login

I forgot the IP address for the ZyXEL Device.

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

I cannot see or access the **Login** screen in the web configurator.

1. Make sure you are using the correct IP address.
   - The default IP address is 192.168.1.1.
   - If you changed the IP address (Section on page 118), use the new IP address.

- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the ZyXEL Device.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.

3 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled. See Appendix C on page 291.

4 Reset the device to its factory defaults, and try to access the ZyXEL Device with the default IP address. See Section 1.6 on page 25.

5 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the ZyXEL Device using another service, such as Telnet. If you can access the ZyXEL Device, check the remote management settings and firewall rules to find out why the ZyXEL Device does not respond to HTTP.
- If your computer is connected wirelessly, use a computer that is connected to a **LAN** port.

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

1 Make sure you have entered the user name and password correctly. The default user name is **admin**. These fields are case-sensitive, so make sure [Caps Lock] is not on.

2 You cannot log in to the web configurator while someone is using Telnet to access the ZyXEL Device. Log out of the ZyXEL Device in the other session, or ask the person who is logged in to log out.

3 Turn the ZyXEL Device off and on.

4 If this does not work, you have to reset the device to its factory defaults. See Section 28.2 on page 237.

I cannot Telnet to the ZyXEL Device.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

28.4 Internet Access

I cannot access the Internet.

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

2 Make sure you entered your ISP account information correctly. These fields are case-sensitive, so make sure [Caps Lock] is not on.

3 If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.

4 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.

5 If the problem continues, contact your ISP.

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

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

2 Turn the ZyXEL Device off and on.

3 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1 There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.5 on page 24. If the ZyXEL Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

2 Check the signal strength. If the signal strength is low, try moving the ZyXEL Device closer to the AP 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.

28.5 Phone Calls and VoIP

The telephone port won’t work or the telephone lacks a dial tone.

Check the telephone connections and telephone wire.

I can access the Internet, but cannot make VoIP calls.

1 The **PHONE** light should come on. Make sure that your telephone is connected to the **PHONE** port.

2 You can also check the VoIP status in the **Status** screen.

28.6 Wireless LAN Troubleshooting

I cannot access the ZyXEL Device or ping any computer from the WLAN (wireless AP or router).

1 Make sure the wireless LAN is enabled on the ZyXEL Device.

2 Make sure the wireless adapter on the wireless station is working properly.

3 Make sure the wireless adapter installed on your computer is IEEE 802.11 compatible and supports the same wireless standard as the ZyXEL Device.

4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the ZyXEL Device.

5 Check that both the ZyXEL Device and your wireless station are using the same wireless and wireless security settings.

6 Check if MAC Filter is configured to deny wireless access to certain MAC addresses to the ZyXEL Device. See Chapter 6 on page 81 in the User's Guide for more information.

29

Product Specifications

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

Hardware Specifications

Table 74 Hardware Specifications

Dimensions	189 (W) x 132 (D) x 40 (H) mm
Weight	316g
Power Specification	12V 1A, K.21 6KV
Built-in Switch	Four auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports
DSL Port	P-2601HN(L)-F1: One RJ-11 DSL port P-2601HN(L)-F3: One RJ-45 DSL port
PHONE Ports	1 RJ-11 FXS POTS port
Line Port ("L" models only)	One FXO (Foreign Exchange Office) lifeline port
RESET Button	Restores the ZyXEL Device's factory default settings if pressed for more than 5 seconds Restarts/reboots the ZyXEL Device if pressed for more than 2 second
WIRELESS ON/OFF button	Press for 1 to 5 second/s: Turn on or off WLAN Press for more than 5 seconds: Turn on WPS
Operation Temperature	0º C ~ 40º C
Storage Temperature	-30º ~ 60º C
Operation Humidity	20% ~ 95% RH
Storage Humidity	20% ~ 95% RH

Firmware Specifications

Table 75 Firmware Specifications

Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default User Name	admin
Default Password	1234.
DHCP Server IP Pool	Starting Address: 192.168.1.64 Size: 32
Static DHCP Addresses	128
Static Routes	32
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 802.11n, IEEE 802.11b and/or IEEE 802.11g wireless clients to connect to the ZyXEL Device wirelessly. Enable wireless security (WPA-PSK and WPA2-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 upgrade the ZyXEL Device. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the ZyXEL Device's configuration. You can put it back on the ZyXEL Device later if you decide to revert back to an earlier configuration.
Pass-through Traffic Type	SIP/RTP PPTP/L2TP/IPSec VPN
Network Address Translation (NAT)	Each computer on your network must have its own unique IP address. Use NAT to convert your public IP address(es) to multiple private IP addresses for the computers on your network. Full cone NAT NAT server (port forwarding) NAT session 6k total, 1k per LAN IP NAT traversal
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.

Table 75 Firmware Specifications (continued)

Dynamic DNS Support	With Dynamic DNS (Domain Name System) support, you can use a fixed URL, www.zyxel.com for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.
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. Supports flexible traffic classification by: Physical Port ETH TYPE (IPoE/PPPoE) Source IP Source MAC 802.1P priority bit DSCP (Different Service control protocol) value Supports 4 priority Queue with Strict Priority (SP) scheme Assigns classified traffic to queues, VLAN or PVC Application binding with dedicated PVC IP Layer QoS (Media Bandwidth Management) TOS prioritization Differentiated Services (DiffServ)
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. UPnP IGD compliance UPnP DCP framework UPnP dynamic port mapping Dynamic port mapping for both TCP and UDP UPnP Show list in WebGUI - Show which ports, protocols and destination IPís have been configured by UPnP.
Firewall	Your device has a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN. The firewall supports TCP/UDP inspection, DoS detection and prevention, real time alerts, reports and logs.

Table 75 Firmware Specifications (continued)

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. Supports HTTP/Telnet/SSH/SCP/SFTP/HTTPS Secure remote management via Web/Telnet/FTP/SSH SSH supports public/private RSA keys of at least 2048 bits for authentication Configurable port number Firmware upgrade via HTTP/SCP/SFTP/GUI/FTP/ TR-069 HTTPS response slowly due to software encryption. Download bins with custom default settings Configuration download using HTTP(s)
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
Helpdesk	Allow remote access, one at a time

Table 75 Firmware Specifications (continued)

ADSL Standards	ADSL2 compliance: ANSI T1.413 Issue 2 ITU-T G.992.1 Annex A, B (G.dmt) ITU-T G.994.1 (G.hs) ITU-T G.992.3 Annex A, B (G.dmt.bis) ITU-T G.992.4 Annex A, B (G.lite.bis) ADSL2+ compliance ITU-T G.992.5 Annex A, B Up to 8 PVC/12 PVC I.610 F4/F5 OAM VC-based and LLC-based multiplexing Multi-protocol over AAL5 (RFC2684/1483) PPP over ATM/AAL5 (RFC2364) Traffic shaping (CBR, VBR-rt/nrt, UBR) PPPoE (RFC2516) RE-ADSL (Reach-Extended ADSL) SRA (Seamless Rate Adaption) Auto-negotiating rate adaption EOC specified in ITU-T G.992.1 ADSL physical connection AAL5 (ATM Adaptation Layer type 5)
Other Protocol Support	PPP (Point-to-Point Protocol) link layer protocol Transparent bridging for unsupported network layer protocols ICMP SNTP IPTV ATM QoS IGMP v1/v2/v3
Management	Embedded Web Configurator CLI (Command Line Interpreter) for administrator account Embedded FTP Server for firmware upgrade and configuration filerestore Telnet for remote management Remote Management Control: Telnet, FTP, Web and DNS. Remote Firmware Upgrade Syslog

Voice Specifications

Note: To take full advantage of the supplementary phone services available through the ZyXEL Device's phone port, you may need to subscribe to the services from your VoIP service provider.

Note: Not all features are supported by all service providers. Consult your service provider for more information.

Table 76 Voice Features

Call Return	With call return, you can place a call to the last number that called you (either answered or missed). The last incoming call can be through either SIP or PSTN.
Country Code	Phone standards and settings differ from one country to another, so the settings on your ZyXEL Device must be configured to match those of the country you are in. The country code feature allows you to do this by selecting the country from a list rather than changing each setting manually. Configure the country code feature when you move the ZyXEL Device from one country to another.
Phone config	The phone config table allows you to customize the phone keypad combinations you use to access certain features on the ZyXEL Device, such as call waiting, call return, and call forward. The phone config table is configurable in command interpreter mode.
Call waiting	This feature allows you to hear an alert when you are already using the phone and another person calls you. You can then either reject the new incoming call, put your current call on hold and receive the new incoming call, or end the current call and receive the new incoming call.
Call forwarding	With this feature, you can set the forward calls to a specified number, either unconditionally (always), when your number is busy, or when you do not answer. You can also forward incoming calls from one specified number to another.
Caller ID	The ZyXEL Device supports caller ID, which allows you to see the originating number of an incoming call (on a phone with a suitable display).
Dynamic Jitter Buffer	The built-in adaptive buffer helps to smooth out the variations in delay (jitter) for voice traffic. This helps ensure good voice quality for your conversations.
Multiple Voice Channels	Your device can simultaneously handle multiple voice channels (telephone calls). Additionally you can answer an incoming phone call on a VoIP account, even while someone else is using the account for a phone call.
Voice Activity Detection/Silence Suppression	Voice Activity Detection (VAD) reduces the bandwidth that a call uses by not transmitting when you are not speaking.
Comfort Noise Generation	Your device generates background noise to fill moments of silence when the other device in a call stops transmitting because the other party is not speaking (as total silence could easily be mistaken for a lost connection).

Table 76 Voice Features

Echo Cancellation	You device supports G.168, an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
QoS (Quality of Service)	Quality of Service (QoS) mechanisms help to provide better service on a per-flow basis. Your device supports Type of Service (ToS) tagging and Differentiated Services (DiffServ) tagging. This allows the device to tag voice frames so they can be prioritized over the network.
Other Voice Features	SIP version 2 (Session Initiatiion Protocol RFC 3261) SDP (Session Description Protocol RFC 2327) RTP (RFC 1889) RTCP (RFC 1890) Voice codecs (coder/decoders) G.711 mu-law, G.711 a-law, G.729, 726-32, 722 Fax and data modem discrimination DTMF Detection and Generation DTMF: In-band and Out-band traffic (RFC 2833),(PCM), (SIP INFO) Quick dialing through predefined phone book, which maps the phone dialing number.

Wireless Features

Table 77 Wireless Features

Wireless LAN MAC Address Filtering	Your device can check the MAC addresses of wireless stations against a list of allowed or denied MAC addresses.
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 77 Wireless Features

WPS	Wi-Fi Protected Setup
Other Wireless Features	IEEE 802.11b/g/n Compliance Frequency Range: 2.4 GHz ISM Band Operating Frequency: • 802.11b/g/n ISM band: 802.11n 20MHz/40MHz • 2.412G~2.472GHz: (ETSI/TELEC) EU(CH1~CH11) Advanced Orthogonal Frequency Division Multiplexing (OFDM) Data Rates: • 802.11n (draft): 15, 30, 45, 60, 90, 120, 135 and 150Mbps • 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps • 802.11b: 1, 2, 5.5, 11Mbps Auto Fallback Modulation Technique: • IEEEE 802.11n (OFDMDSSS): BPSK, QPSK, 16-QAM, 64-QAM • IEEEE 802.11g (OFDMDSSS): BPSK, QPSK, 16-QAM, 64-QAM • 802.11b (DSSS): CCK (11Mbps, 5.5Mbps), DQPSK (2Mbps), DBPSK (1Mbps) Turn on-off WLAN by **WLAN** button (press the **WLAN** button for one second to turn the WLAN on or turn off; five seconds to turn on WPS) IEEE 802.11e (APSD) WLAN bridge to LAN Up to 32 MAC Address filters Scheduling lets you set when the WLAN is on

Standards and Certifications

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

Table 78 Standards Supported

STANDARD	DESCRIPTION
RFC 867	Daytime Protocol
RFC 868	Time Protocol.
RFC 1305	Network Time Protocol (NTP version 3)
RFC 1631	IP Network Address Translator (NAT)

Table 78 Standards Supported (continued)

STANDARD	DESCRIPTION
RFC 1661	The Point-to-Point Protocol (PPP)
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2766	Network Address Translation - Protocol
IEEE 802.11	Also known by the brand Wi-Fi, denotes a set of Wireless LAN/ WLAN standards developed by working group 11 of the IEEE LAN/MAN Standards Committee (IEEE 802).
IEEE 802.11b	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11g	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11n	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11d	Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges
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.992.3 (G.dmt.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.
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)

FUNCTION	REGION AND CERTIFICATION
Safety	European Union (CE mark) EN 60950-1:2006 + A11:2009 IEC 60950-1:2005 (2nd Edition)
EMI	European Union (CE mark) EN55022 Class B EN61000-3-2 EN61000-3-3
EMS	European Union (CE mark) EN55024
Overvoltage	K.21 Enhanced Level (6 kV), EN 60950-1 with National ammendments (SE) K.45 Enhanced Level ,content K.21 Enhanced Level (10 KV)

FUNCTION	REGION AND CERTIFICATION
EuP	Lot6 off-mode EPS (external power supply) lot7
Electrostatic Discharge	EN61000-4-2
Radio-Frequency Electromagnetic Field	EN61000-4-3
EFT/Burst	EN61000-4-4
Surge	EN61000-4-5
Conducted Susceptibility	EN61000-4-6
Voltage Dips/ Interruption	EN61000-4-11
Overvoltage	K.21 Enhanced Level (6 kV), EN 60950-1 with National amendments. (SE)
Others	EN 301 489-1, 17

A

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (such as computers, servers, routers, and printers) 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.

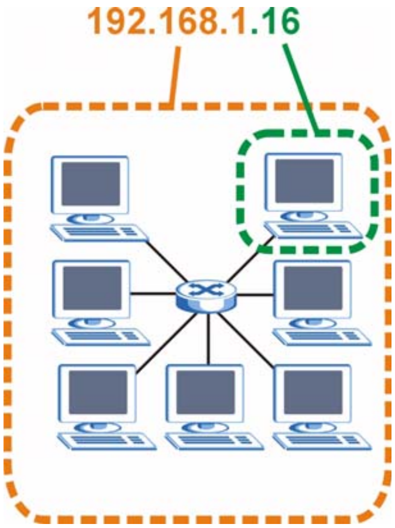
Structure

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 117 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 79 IP Address Network Number and Host ID Example

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

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

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

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

Table 80 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 81 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 82 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

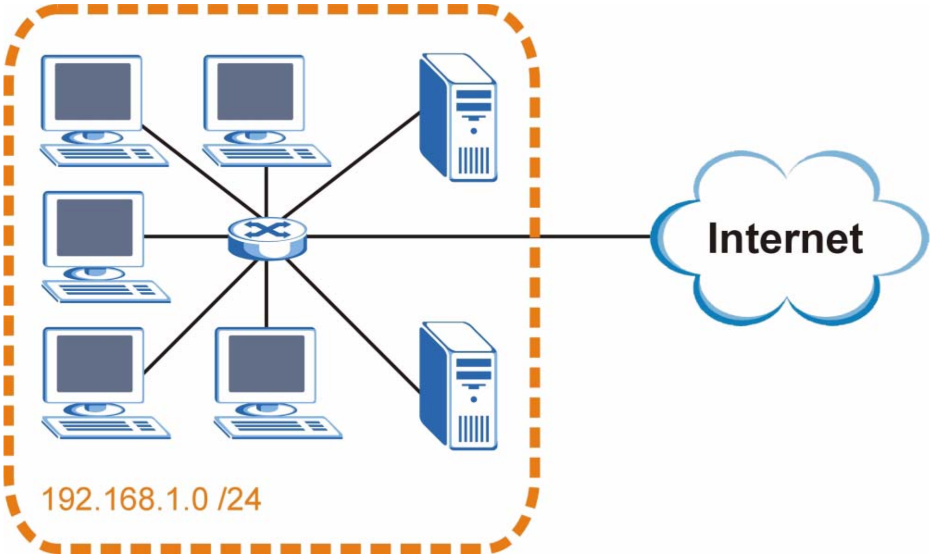
Subnetting

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 118 Subnetting Example: Before Subnetting

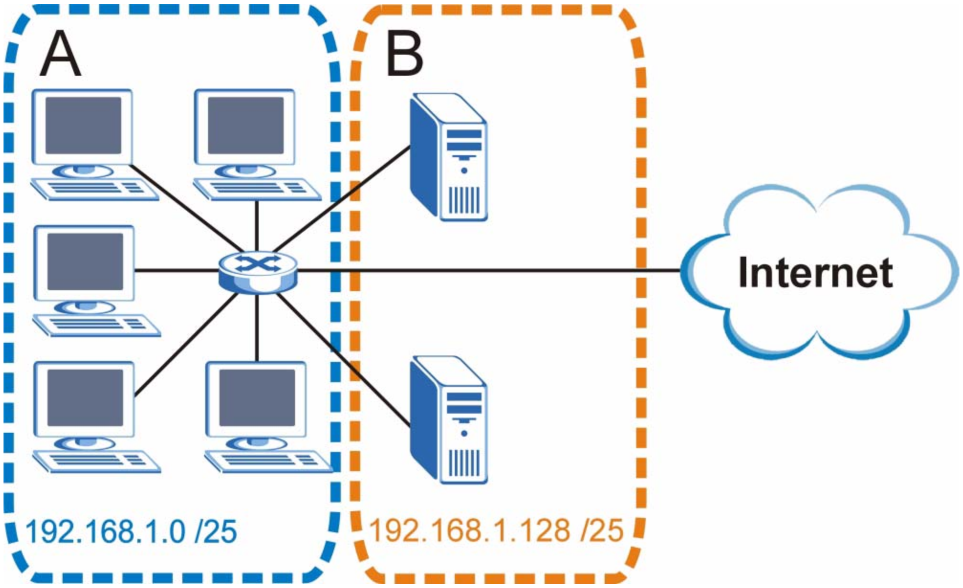


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

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 119 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.**11**000000) 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 83 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
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 84 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
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 85 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
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 86 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
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 87 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 88 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 89 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

Table 89 16-bit Network Number Subnet Planning (continued)

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
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.

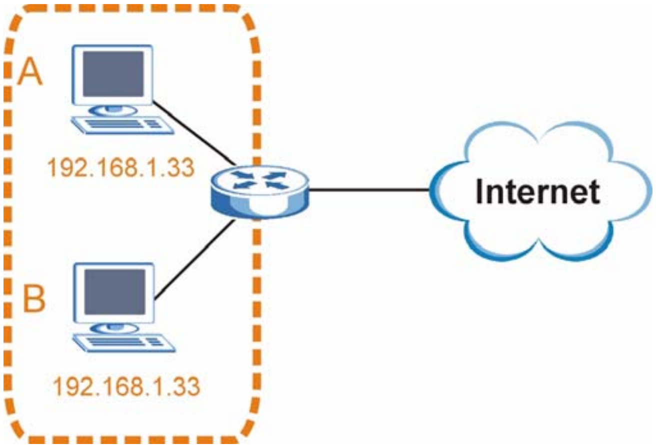
IP Address Conflicts

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.

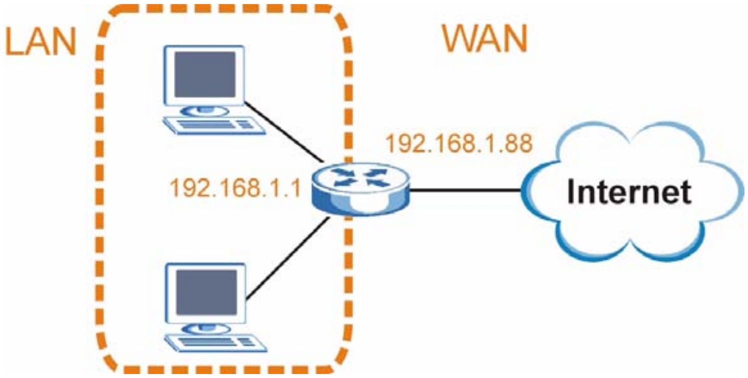
Figure 120 Conflicting Computer IP Addresses Example



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 121 Conflicting Computer IP Addresses Example

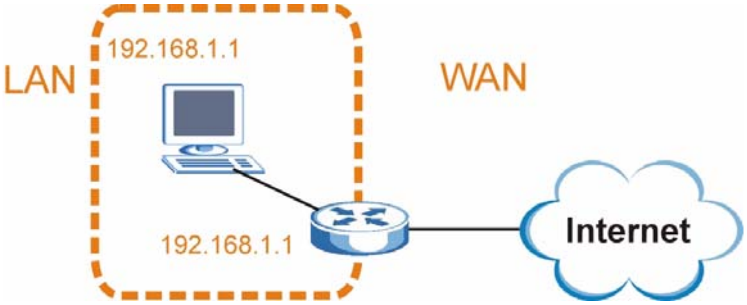


Conflicting Computer and Router IP Addresses Example

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 122 Conflicting Computer and Router IP Addresses Example



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:

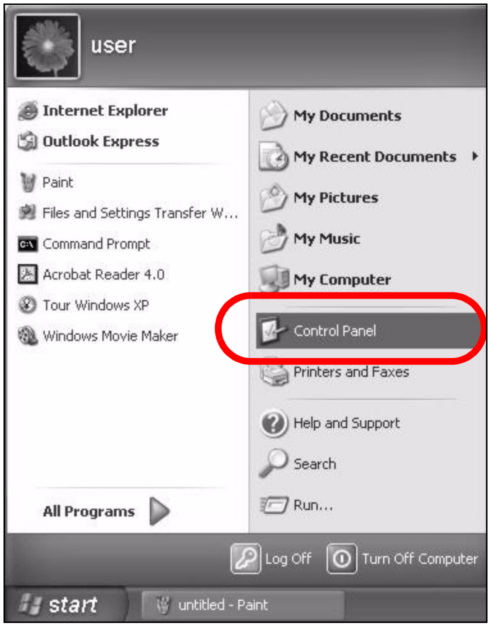
- Windows XP/NT/2000 on page 265
- Windows Vista on page 268
- Windows 7 on page 272
- Mac OS X: 10.3 and 10.4 on page 275
- Mac OS X: 10.5 on page 279
- Linux: Ubuntu 8 (GNOME) on page 282
- Linux: openSUSE 10.3 (KDE) on page 285

Windows XP/NT/2000

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

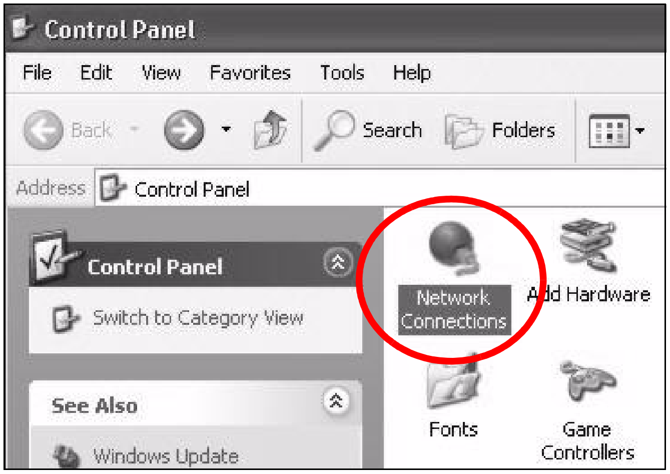
1 Click **Start** > **Control Panel**.

Figure 123 Windows XP: Start Menu



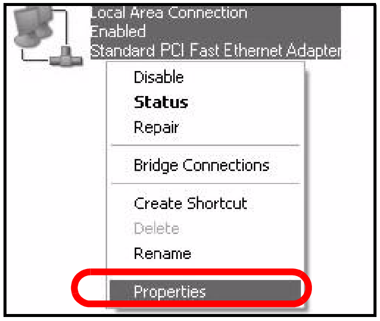
2 In the **Control Panel**, click the **Network Connections** icon.

Figure 124 Windows XP: Control Panel



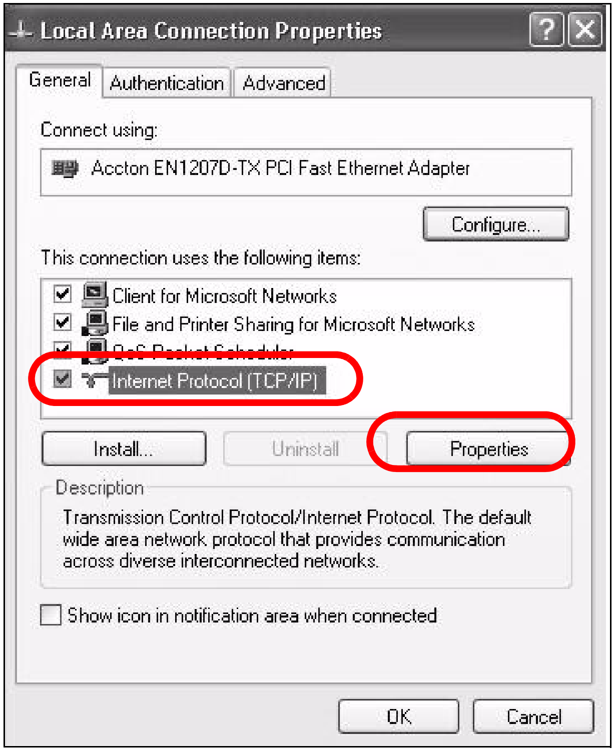
3 Right-click **Local Area Connection** and then select **Properties**.

Figure 125 Windows XP: Control Panel > Network Connections > Properties



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

Figure 126 Windows XP: Local Area Connection Properties



Connect using:

Accton EN1207D-TX PCI Fast Ethernet Adapter

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol (TCP/IP)

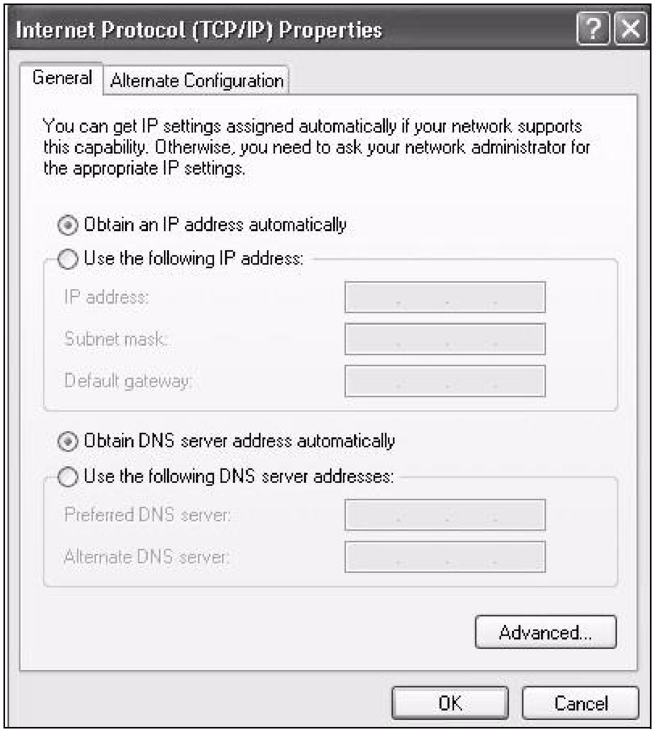
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

□ Show icon in notification area when connected

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

Figure 127 Windows XP: Internet Protocol (TCP/IP) Properties



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

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].

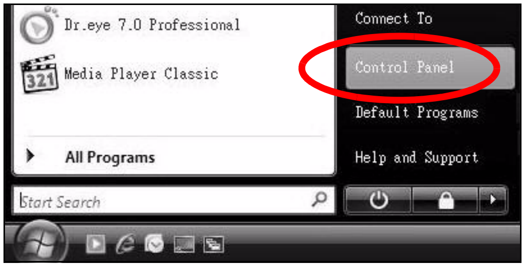
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Windows Vista

This section shows screens from Windows Vista Professional.

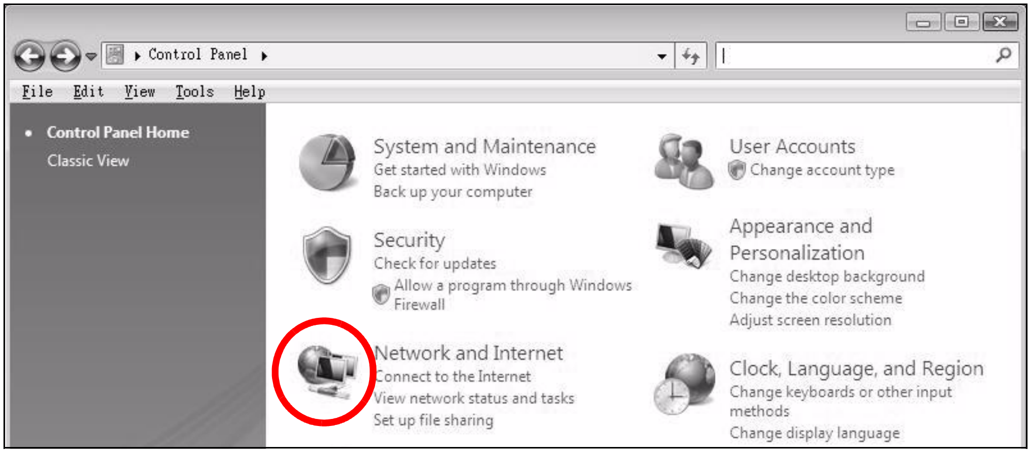
1 Click **Start** > **Control Panel**.

Figure 128 Windows Vista: Start Menu



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

Figure 129 Windows Vista: Control Panel



Control Panel ▸

File Edit View Tools Help

- Control Panel Home
- Classic View

System and Maintenance
Get started with Windows
Back up your computer

User Accounts
Change account type

Security
Check for updates
Allow a program through Windows Firewall

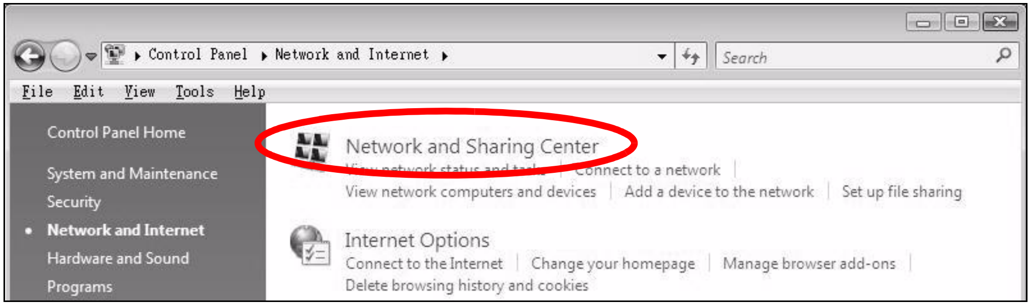
Appearance and Personalization
Change desktop background
Change the color scheme
Adjust screen resolution

Network and Internet
Connect to the Internet
View network status and tasks
Set up file sharing

Clock, Language, and Region
Change keyboards or other input methods
Change display language

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

Figure 130 Windows Vista: Network And Internet



Control Panel ▸ Network and Internet ▸

Search

File Edit View Tools Help

Control Panel Home

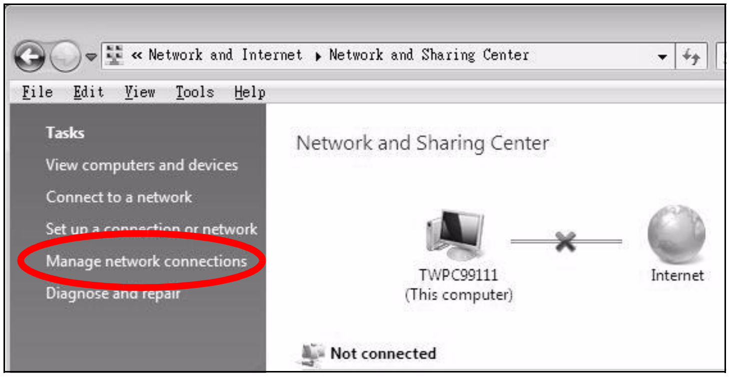
System and Maintenance
Security
- Network and Internet
Hardware and Sound
Programs

Network and Sharing Center
View network status and tasks | Connect to a network |
View network computers and devices | Add a device to the network | Set up file sharing

Internet Options
Connect to the Internet | Change your homepage | Manage browser add-ons |
Delete browsing history and cookies

4 Click **Manage network connections**.

Figure 131 Windows Vista: Network and Sharing Center



« Network and Internet ▸ Network and Sharing Center

File Edit View Tools Help

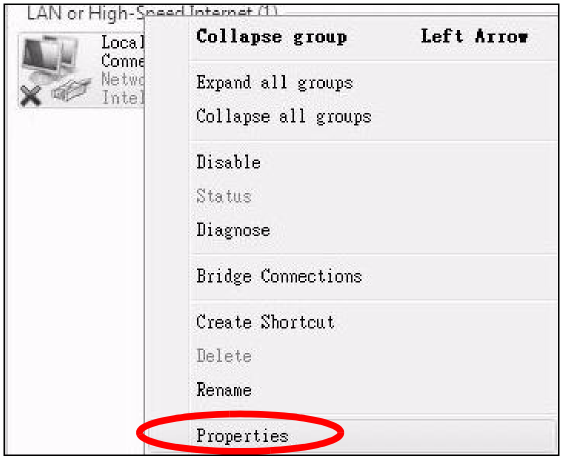
Tasks
View computers and devices
Connect to a network
Set up a connection or network
Manage network connections
Diagnose and repair

Network and Sharing Center

Not connected

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

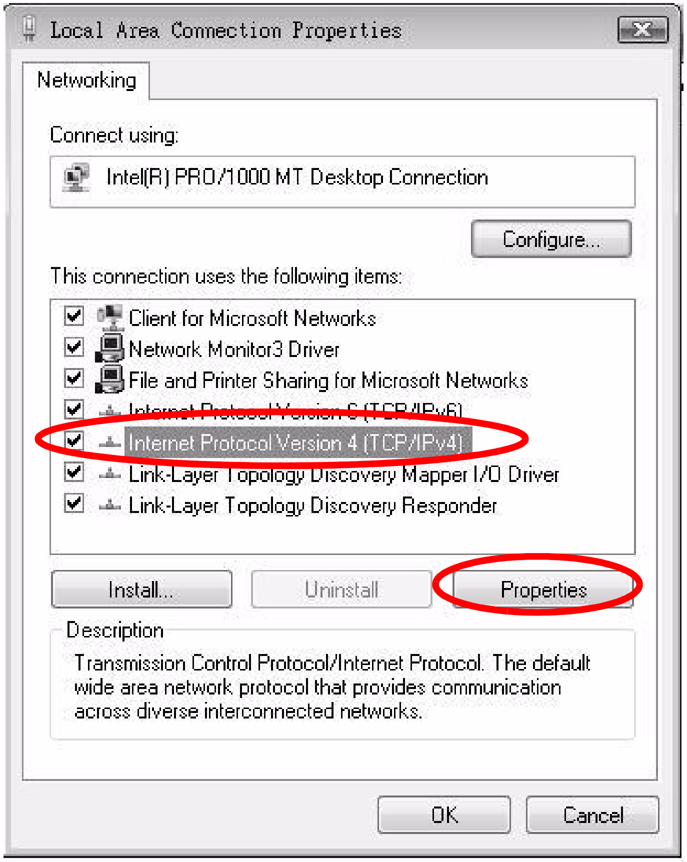
Figure 132 Windows Vista: Network and Sharing Center



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 133 Windows Vista: Local Area Connection Properties



Connect using:

Intel(R) PRO/1000 MT Desktop Connection

This connection uses the following items:

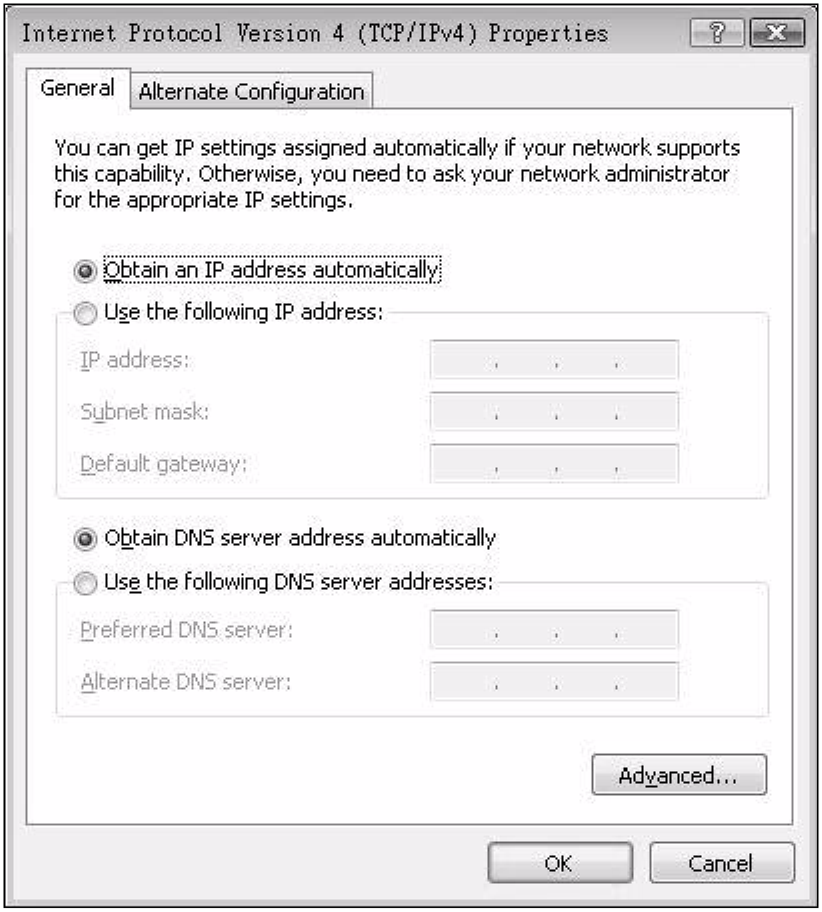
☑ Client for Microsoft Networks
☑ Network Monitor3 Driver
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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

Figure 134 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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].

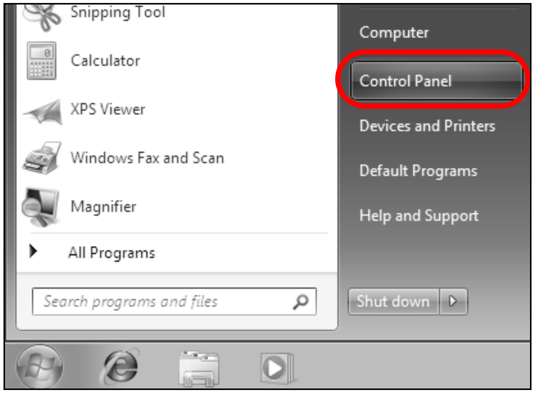
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Windows 7

This section shows screens from Windows 7 Enterprise.

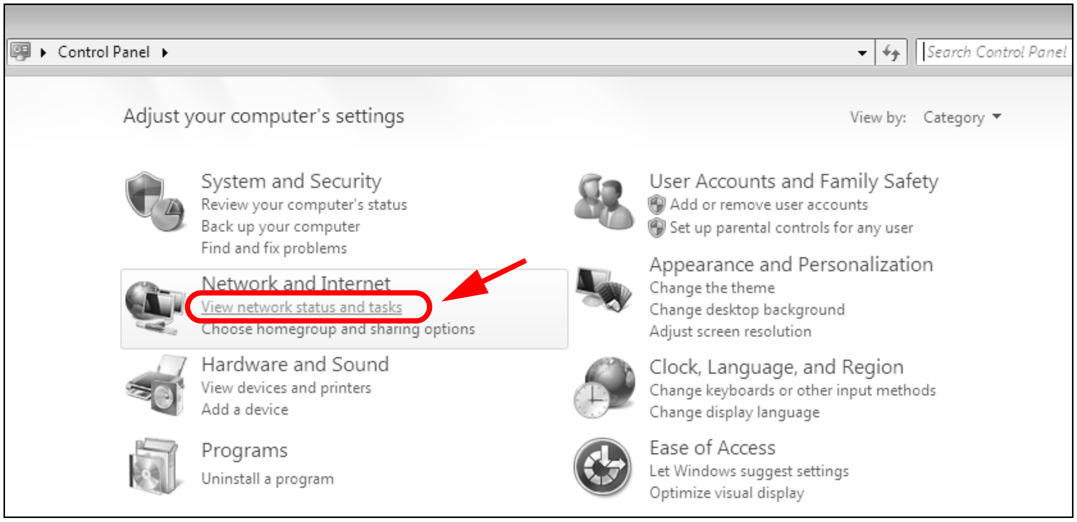
1 Click **Start** > **Control Panel**.

Figure 135 Windows 7: Start Menu



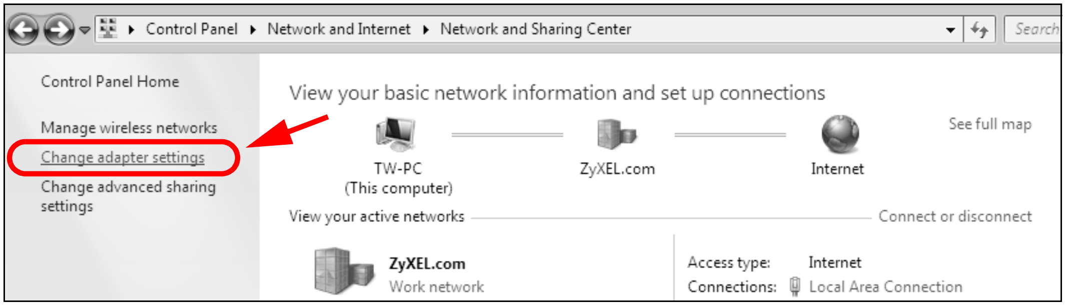
2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.

Figure 136 Windows 7: Control Panel


Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Back up your computer
Find and fix problems
Network and Internet
View network status and tasks
Choose homegroup and sharing options
Hardware and Sound
View devices and printers
Add a device
Programs
Uninstall a program
User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user
Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution
Clock, Language, and Region
Change keyboards or other input methods
Change display language
Ease of Access
Let Windows suggest settings
Optimize visual display

3 Click **Change adapter settings**.

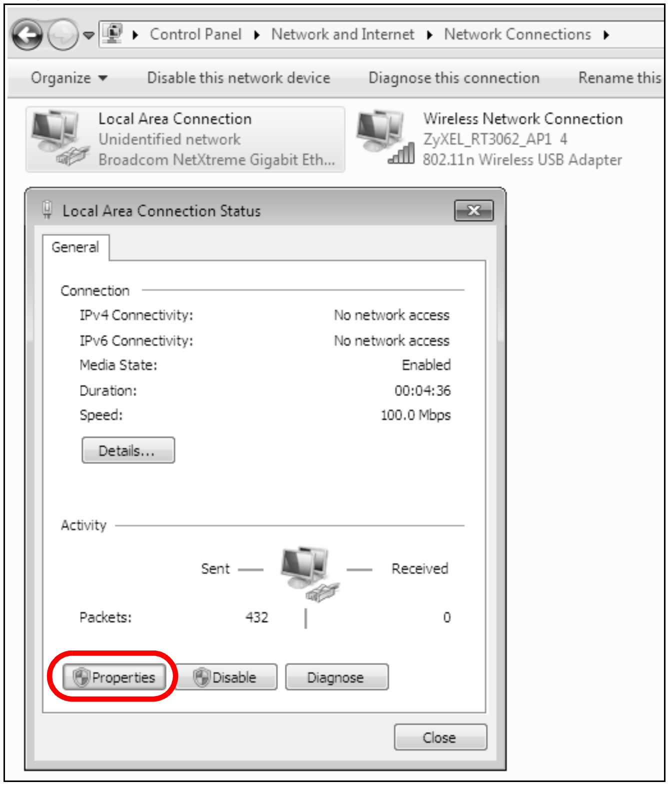
Figure 137 Windows 7: Network And Sharing Center


Control Panel ▸ Network and Internet ▸ Network and Sharing Center
Search
Control Panel Home
Manage wireless networks
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
TW-PC
(This computer)
ZyXEL.com
Internet
View your active networks
Connect or disconnect
ZyXEL.com
Work network

Access type: Internet
Connections: Local Area Connection

4 Double click **Local Area Connection** and then select **Properties**.

Figure 138 Windows 7: Local Area Connection Status


Control Panel ▸ Network and Internet ▸ Network Connections ▸
Organize ▾
Disable this network device
Diagnose this connection
Rename this
Local Area Connection
Unidentified network
Broadcom NetXtreme Gigabit Eth...
Wireless Network Connection
ZyXEL_RT3062_AP1 4
802.11n Wireless USB Adapter
Local Area Connection Status
General
Connection
Details...
Activity
Sent
Received
Properties
Disable
Diagnose
Close

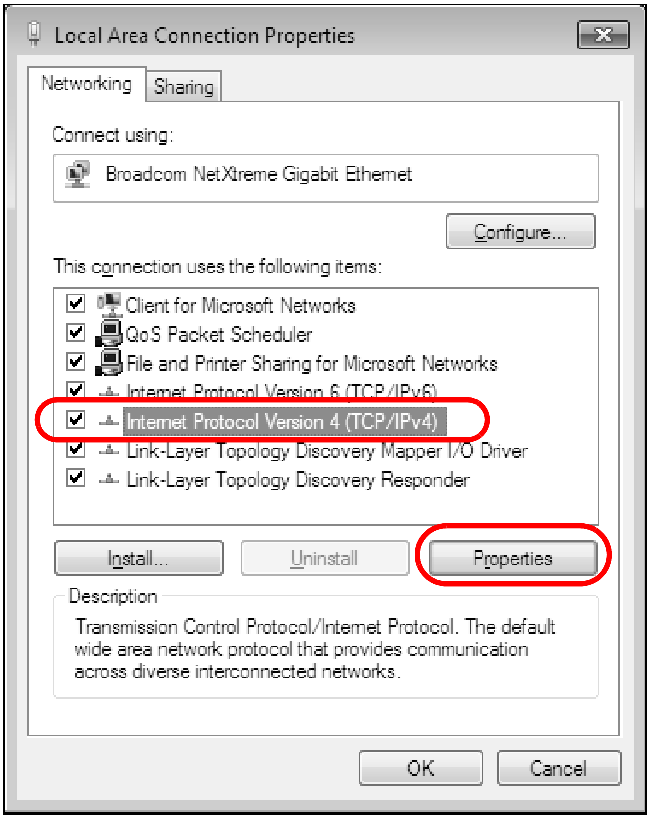
IPv4 Connectivity: No network access
IPv6 Connectivity: No network access
Media State: Enabled
Duration: 00:04:36
Speed: 100.0 Mbps

Packets: 432 0

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

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

Figure 139 Windows 7: Local Area Connection Properties



Connect using:

Broadcom NetXtreme Gigabit Ethernet

This connection uses the following items:

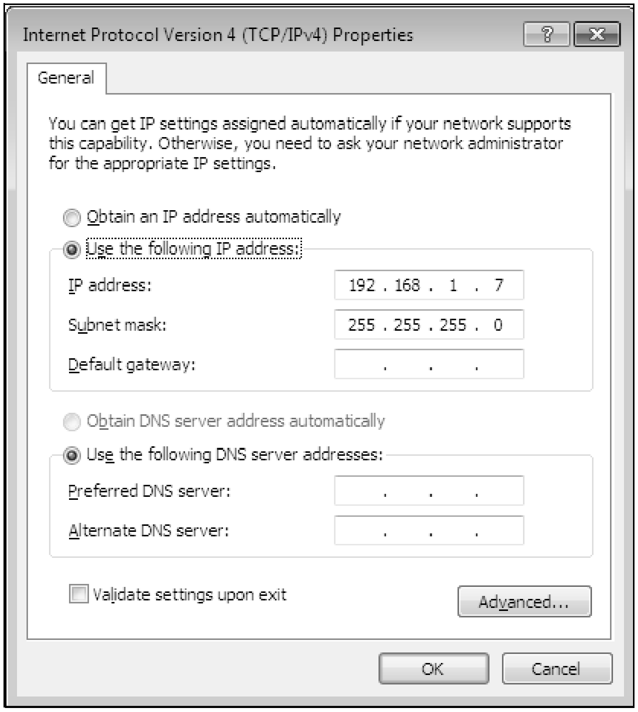
- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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

Figure 140 Windows 7: Internet Protocol Version 4 (TCP/IPv4) Properties



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 7

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

7 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** if you want to configure advanced settings for IP, DNS and WINS.

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **OK** to close the **Local Area Connection Properties** window.

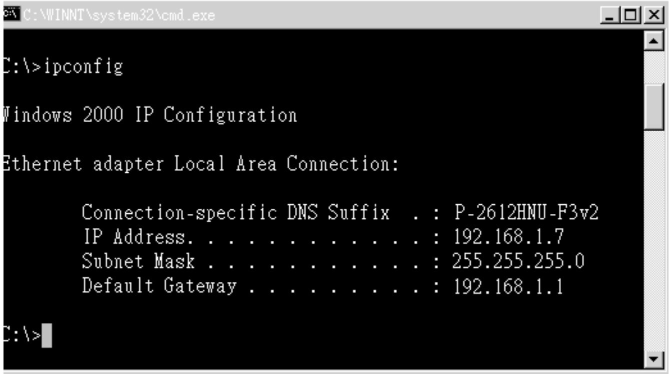
Verifying Settings

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

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

3 The IP settings are displayed as follows.

Figure 141 Windows 7: Internet Protocol Version 4 (TCP/IPv4) Properties



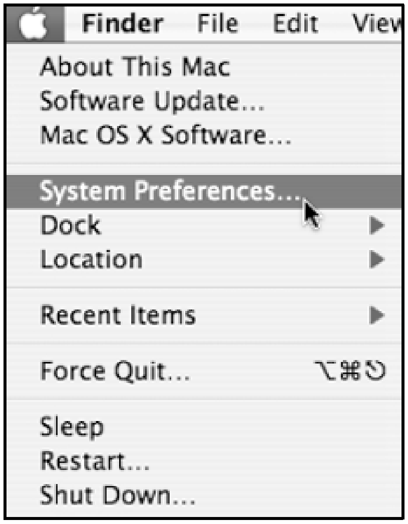
```
C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : P-2612HNU-F3v2
        IP Address. . . . . . . . . . . . : 192.168.1.7
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\>
```

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.

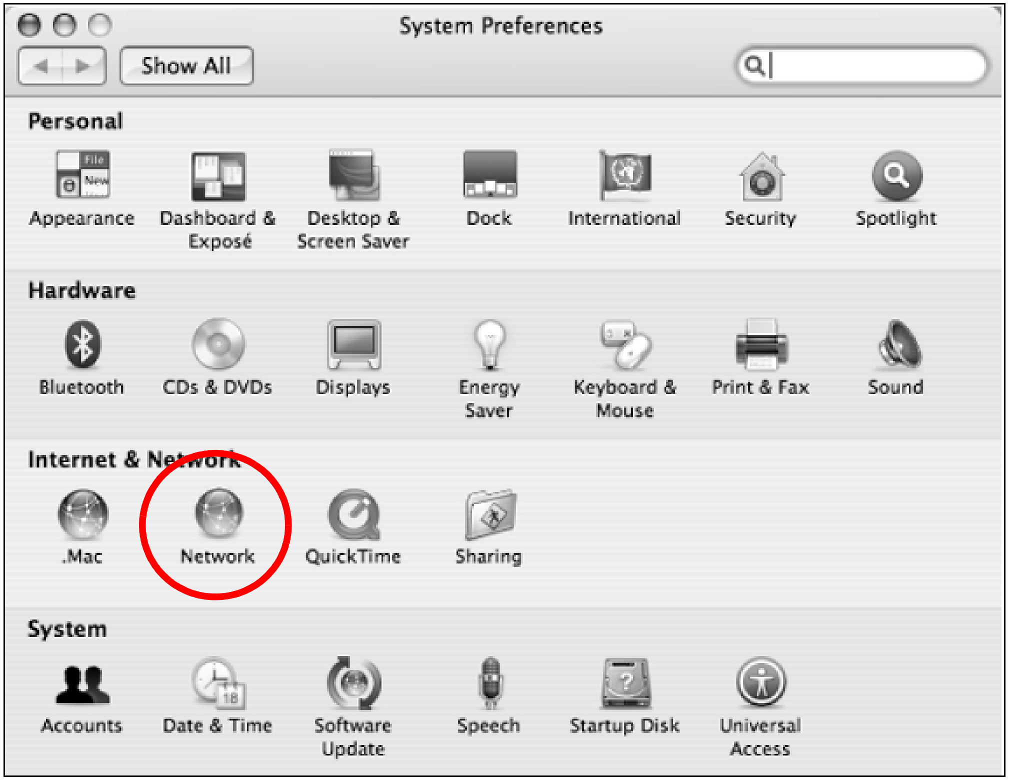
1 Click **Apple** > **System Preferences**.

Figure 142 Mac OS X 10.4: Apple Menu



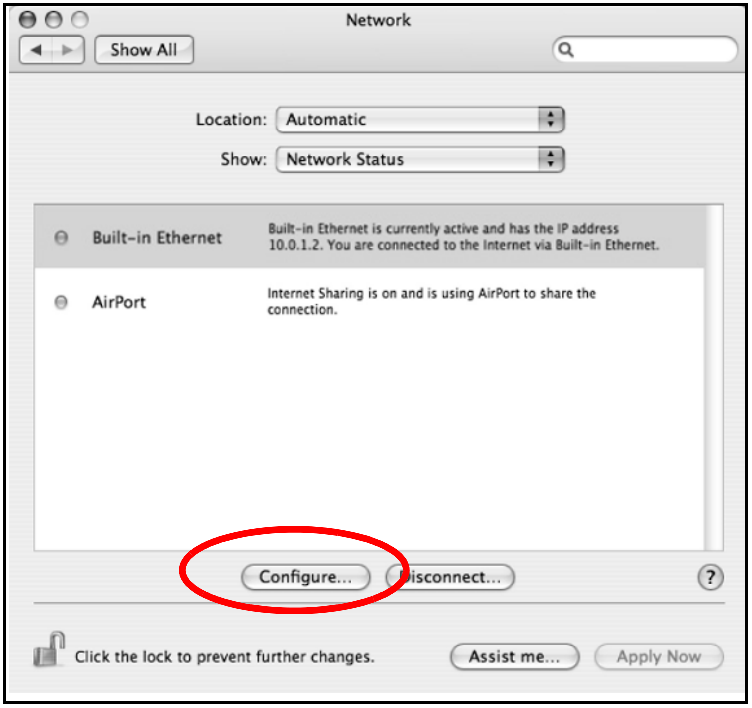
2 In the **System Preferences** window, click the **Network** icon.

Figure 143 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 144 Mac OS X 10.4: Network Preferences



Location: Automatic

Show: Network Status

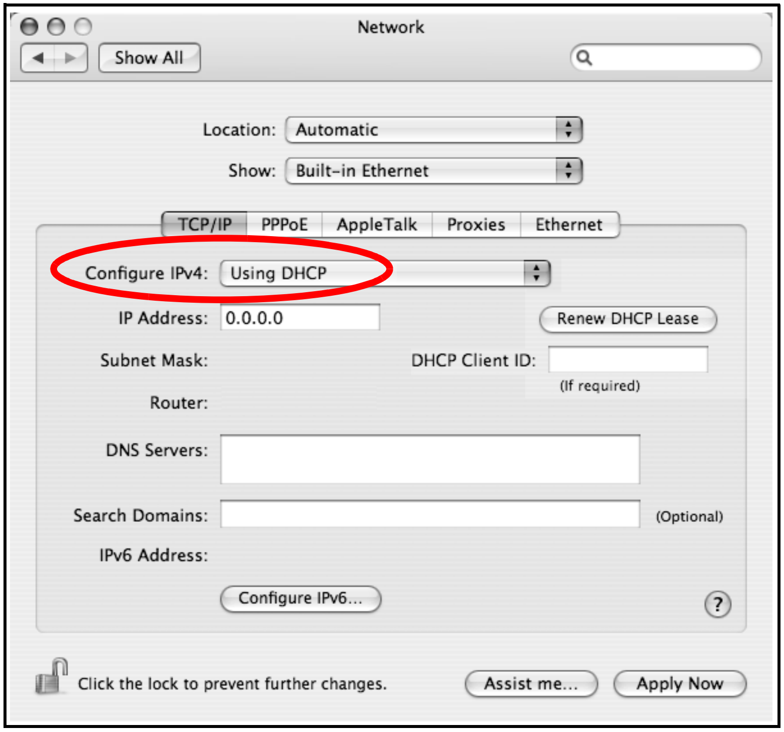
Built-in Ethernet — Built-in Ethernet is currently active and has the IP address 10.0.1.2. You are connected to the Internet via Built-in Ethernet.

AirPort — Internet Sharing is on and is using AirPort to share the connection.

Click the lock to prevent further changes.

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

Figure 145 Mac OS X 10.4: Network Preferences > TCP/IP Tab.



Location: Automatic

Show: Built-in Ethernet

Configure IPv4: Using DHCP

IP Address: 0.0.0.0

Subnet Mask:

DHCP Client ID: (If required)

Router:

DNS Servers:

Search Domains: (Optional)

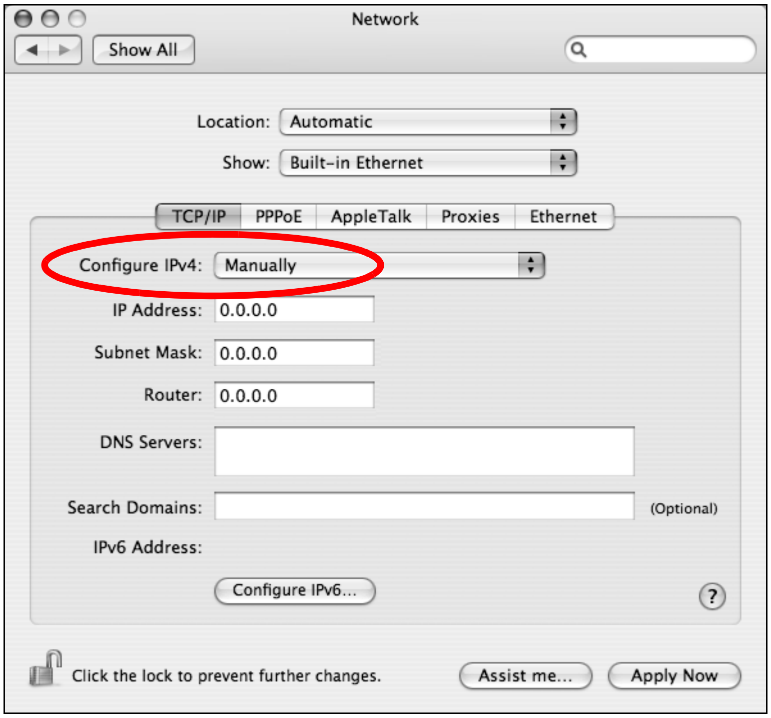
IPv6 Address:

Click the lock to prevent further changes.

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 146 Mac OS X 10.4: Network Preferences > Ethernet



Location: Automatic

Show: Built-in Ethernet

Configure IPv4: Manually

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Router: 0.0.0.0

DNS Servers:

Search Domains: (Optional)

IPv6 Address:

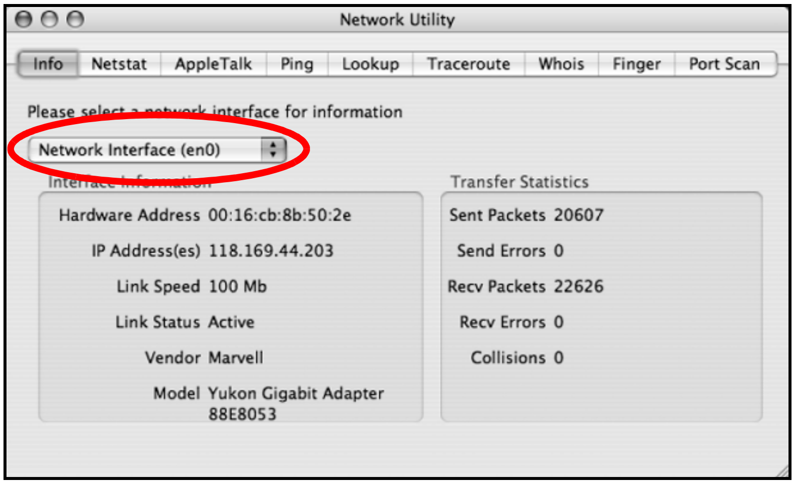
Click the lock to prevent further changes.

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 147 Mac OS X 10.4: Network Utility



Please select a network interface for information

Network Interface (en0)

Interface Information

Hardware Address 00:16:cb:8b:50:2e
IP Address(es) 118.169.44.203
Link Speed 100 Mb
Link Status Active
Vendor Marvell
Model Yukon Gigabit Adapter 88E8053

Transfer Statistics

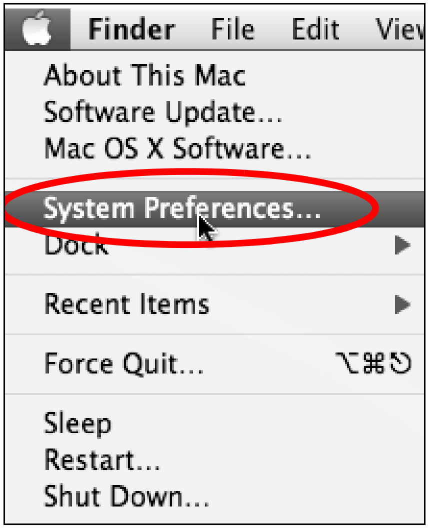
Sent Packets 20607
Send Errors 0
Recv Packets 22626
Recv Errors 0
Collisions 0

Mac OS X: 10.5

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

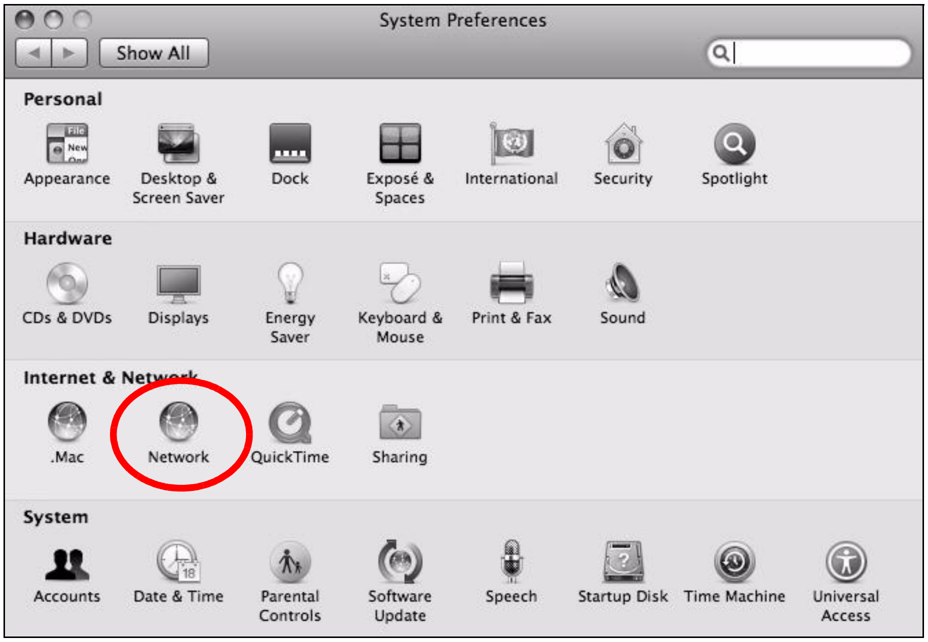
1 Click **Apple** > **System Preferences**.

Figure 148 Mac OS X 10.5: Apple Menu



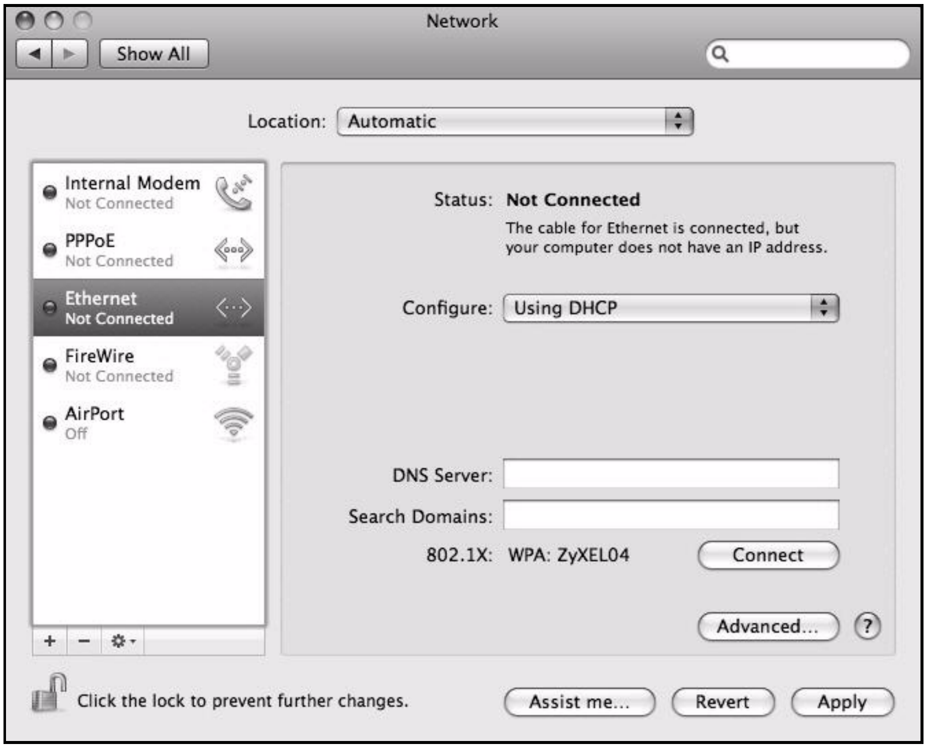
2 In **System Preferences**, click the **Network** icon.

Figure 149 Mac OS X 10.5: Systems Preferences



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

Figure 150 Mac OS X 10.5: Network Preferences > Ethernet



Location: Automatic

Status: Not Connected

The cable for Ethernet is connected, but your computer does not have an IP address.

Configure: Using DHCP

DNS Server:

Search Domains:

802.1X: WPA: ZyXEL04

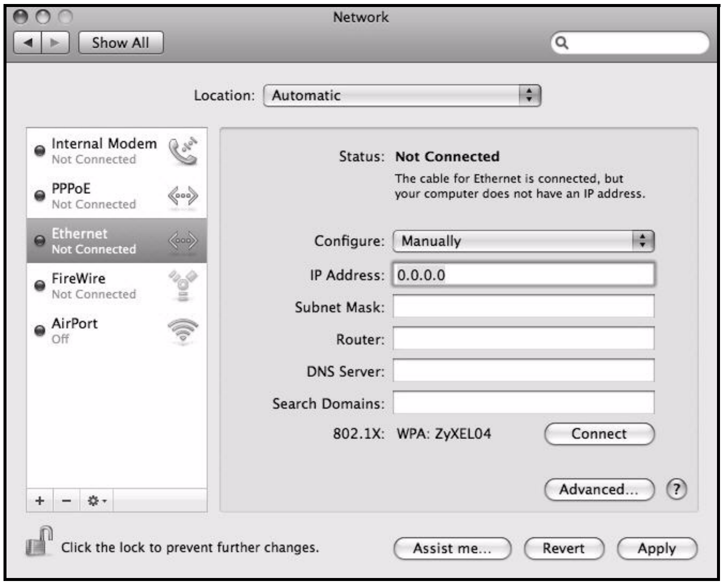
Click the lock to prevent further changes.

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 151 Mac OS X 10.5: Network Preferences > Ethernet



Location: Automatic

Internal Modem Not Connected
PPPoE Not Connected
Ethernet Not Connected
FireWire Not Connected
AirPort Off

Status: Not Connected
The cable for Ethernet is connected, but your computer does not have an IP address.

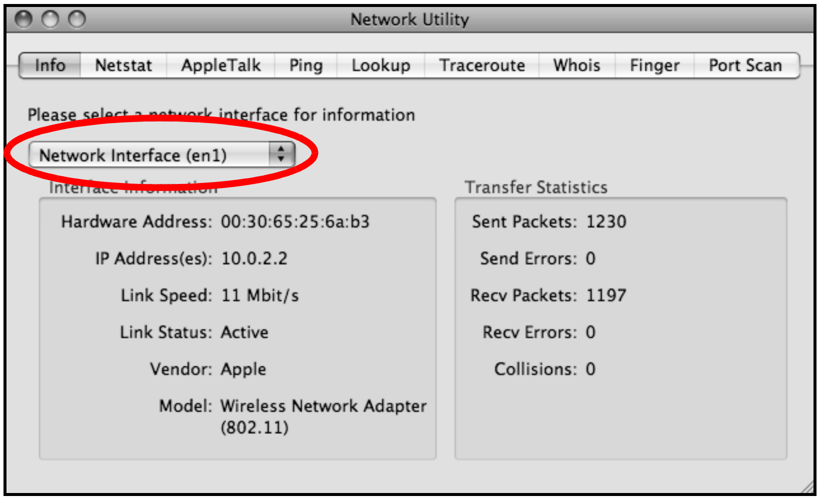
Configure: Manually
IP Address: 0.0.0.0
Subnet Mask:
Router:
DNS Server:
Search Domains:
802.1X: WPA: ZyXEL04

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 152 Mac OS X 10.5: Network Utility



Please select a network interface for information

Network Interface (en1)

Interface Information

Hardware Address: 00:30:65:25:6a:b3
IP Address(es): 10.0.2.2
Link Speed: 11 Mbit/s
Link Status: Active
Vendor: Apple
Model: Wireless Network Adapter (802.11)

Transfer Statistics

Sent Packets: 1230
Send Errors: 0
Recv Packets: 1197
Recv Errors: 0
Collisions: 0

Linux: Ubuntu 8 (GNOME)

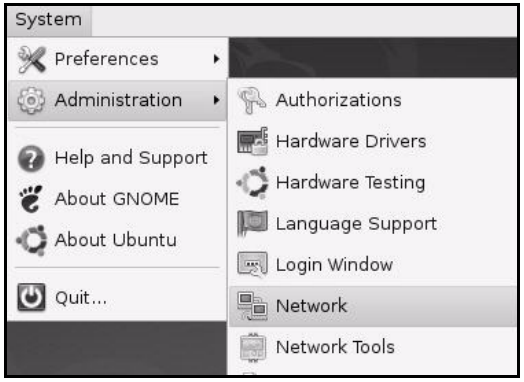
This section shows you how to configure your computer’s TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following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

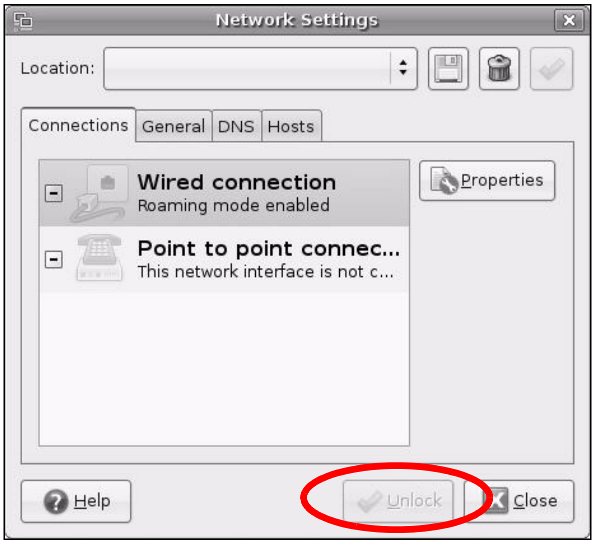
1 Click **System > Administration > Network**.

Figure 153 Ubuntu 8: System > Administration Menu



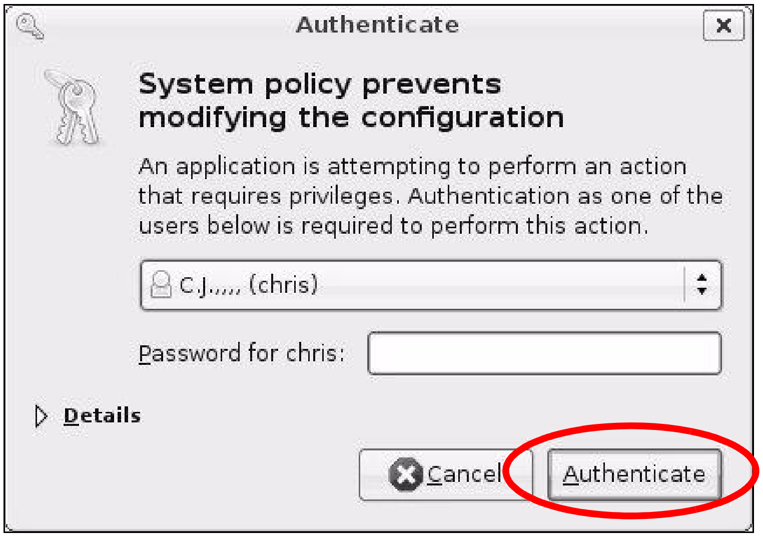
2 When the **Network Settings** window opens, click **Unlock** to open the **Authenticate** window. (By default, the **Unlock** button is greyed out until clicked.) You cannot make changes to your configuration unless you first enter your admin password.

Figure 154 Ubuntu 8: Network Settings > Connections



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

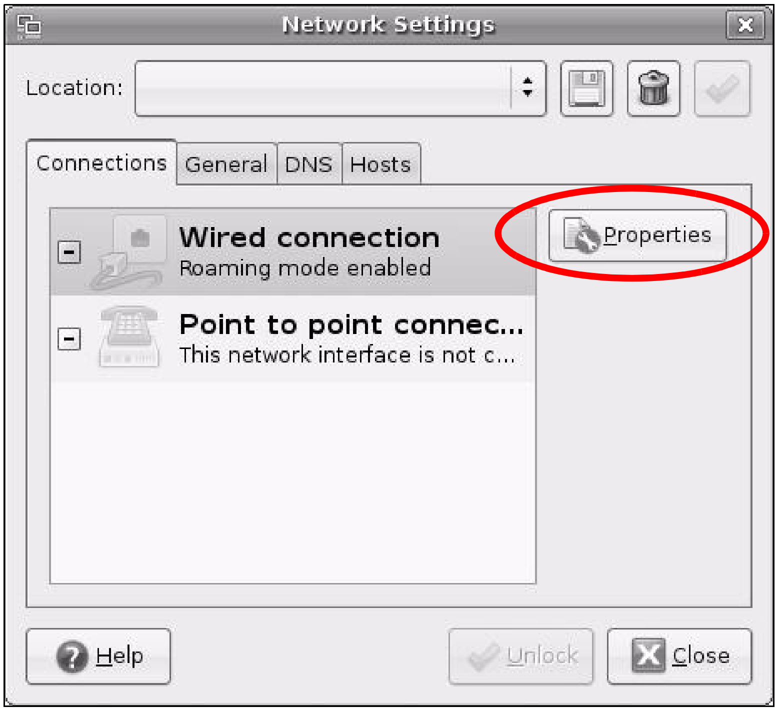
Figure 155 Ubuntu 8: Administrator Account Authentication



Authenticate
System policy prevents modifying the configuration
An application is attempting to perform an action that requires privileges. Authentication as one of the users below is required to perform this action.
C.J.,,,, (chris)
Password for chris:
Details
Cancel
Authenticate

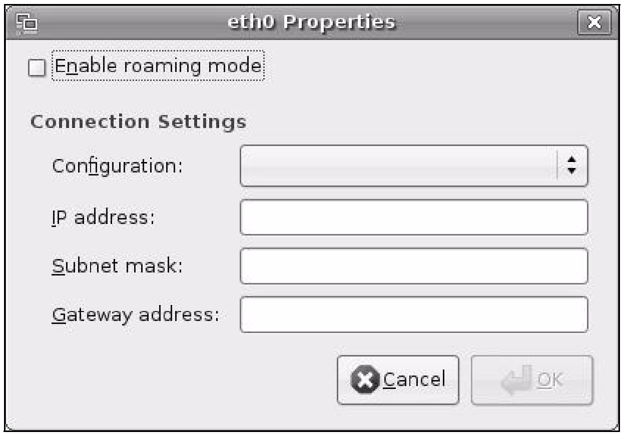
4 In the **Network Settings** window, select the connection that you want to configure, then click **Properties**.

Figure 156 Ubuntu 8: Network Settings > Connections



5 The **Properties** dialog box opens.

Figure 157 Ubuntu 8: Network Settings > Properties

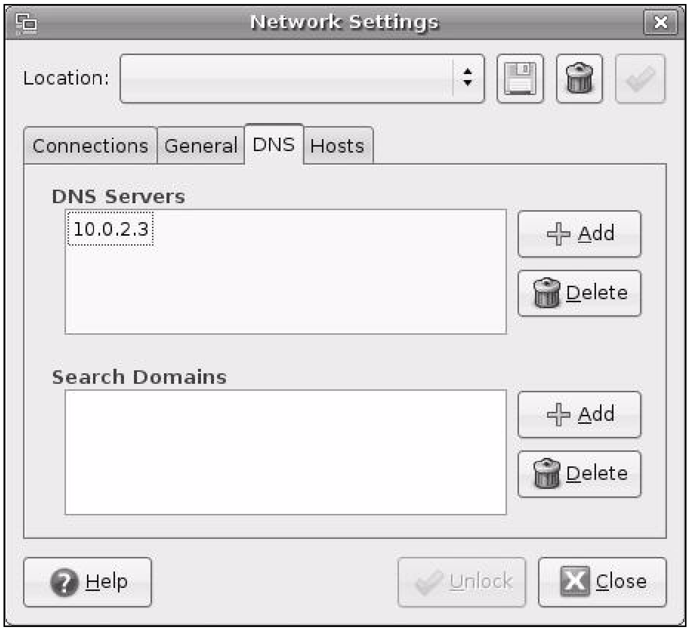


- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
- In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.

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 158 Ubuntu 8: Network Settings > DNS



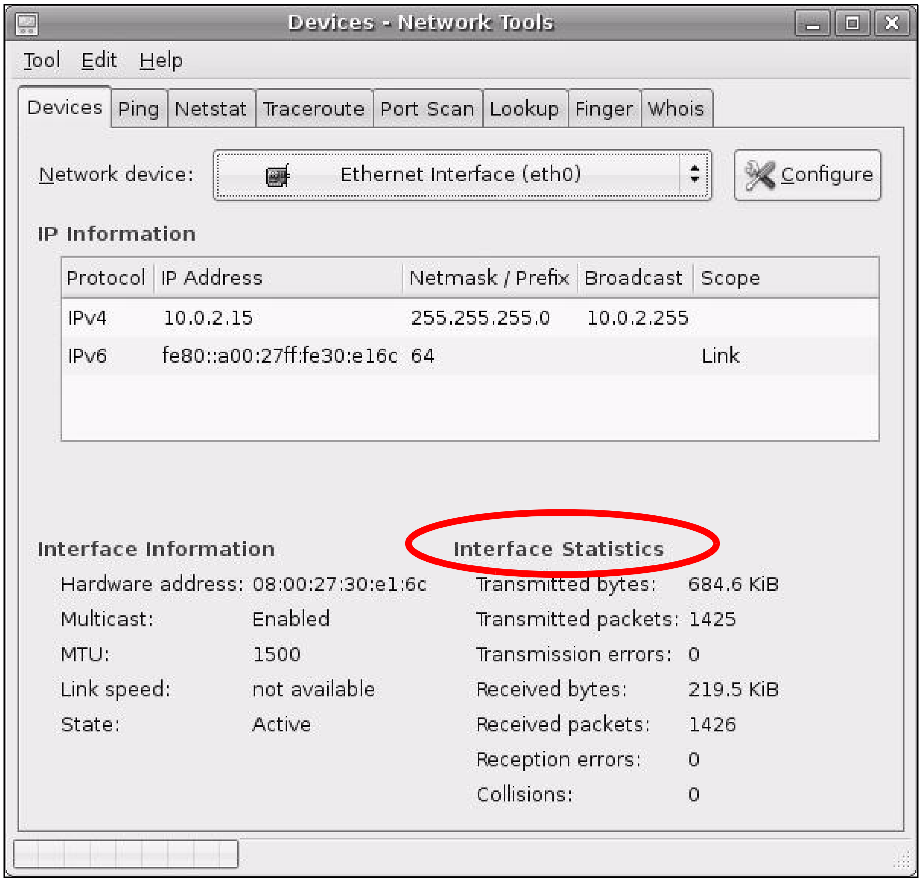
DNS Servers: 10.0.2.3

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 159   Ubuntu 8: Network Tools



Network device: Ethernet Interface (eth0)

IP Information

Protocol	IP Address	Netmask / Prefix	Broadcast	Scope
IPv4	10.0.2.15	255.255.255.0	10.0.2.255	
IPv6	fe80::a00:27ff:fe30:e16c	64		Link

Interface Information

Hardware address:	08:00:27:30:e1:6c
Multicast:	Enabled
MTU:	1500
Link speed:	not available
State:	Active

Interface Statistics

Transmitted bytes:	684.6 KiB
Transmitted packets:	1425
Transmission errors:	0
Received bytes:	219.5 KiB
Received packets:	1426
Reception errors:	0
Collisions:	0

Linux: openSUSE 10.3 (KDE)

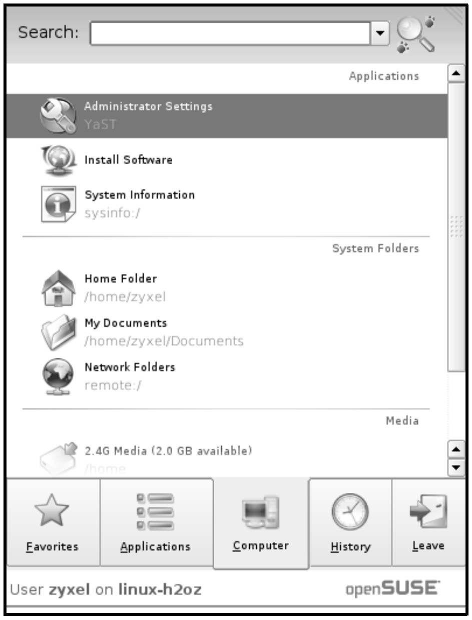
This section shows you how to configure your computer’s TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following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

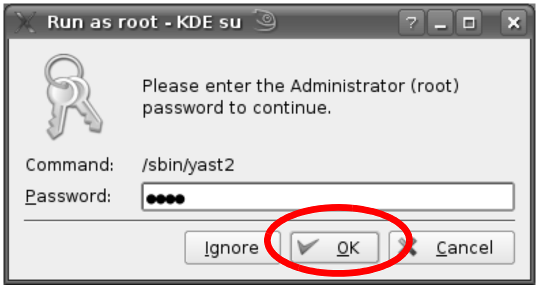
1 Click **K Menu > Computer > Administrator Settings (YaST)**.

Figure 160 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 161 openSUSE 10.3: K Menu > Computer Menu


Run as root - KDE su

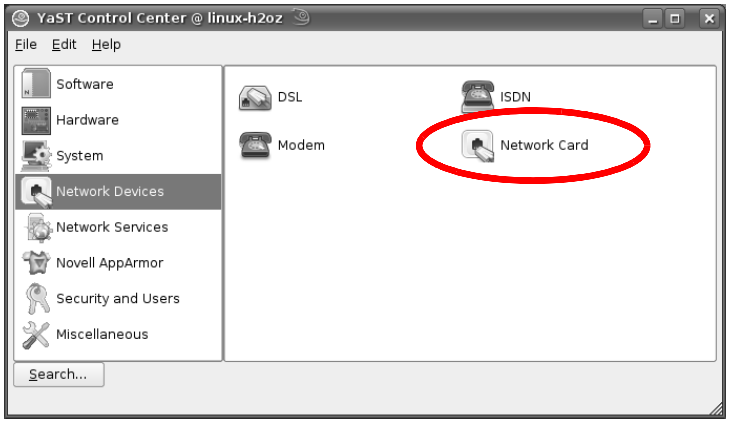
Please enter the Administrator (root) password to continue.

Command: /sbin/yast2

Password: ●●●●

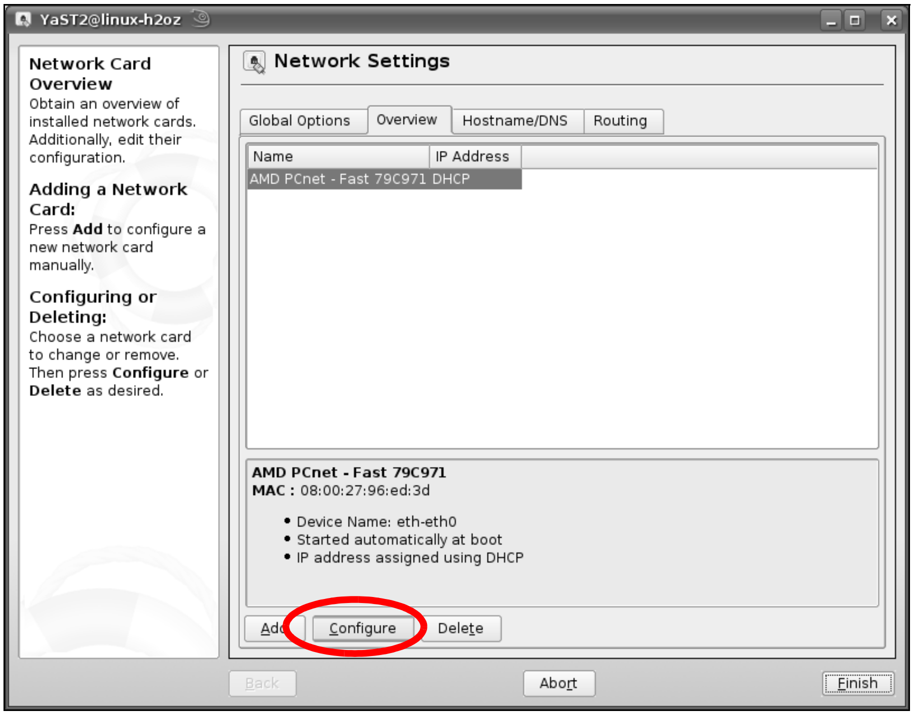
3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.

Figure 162 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 163 openSUSE 10.3: Network Settings



Network Card Overview
Obtain an overview of installed network cards. Additionally, edit their configuration.

Adding a Network Card:
Press **Add** to configure a new network card manually.

Configuring or Deleting:
Choose a network card to change or remove. Then press **Configure** or **Delete** as desired.

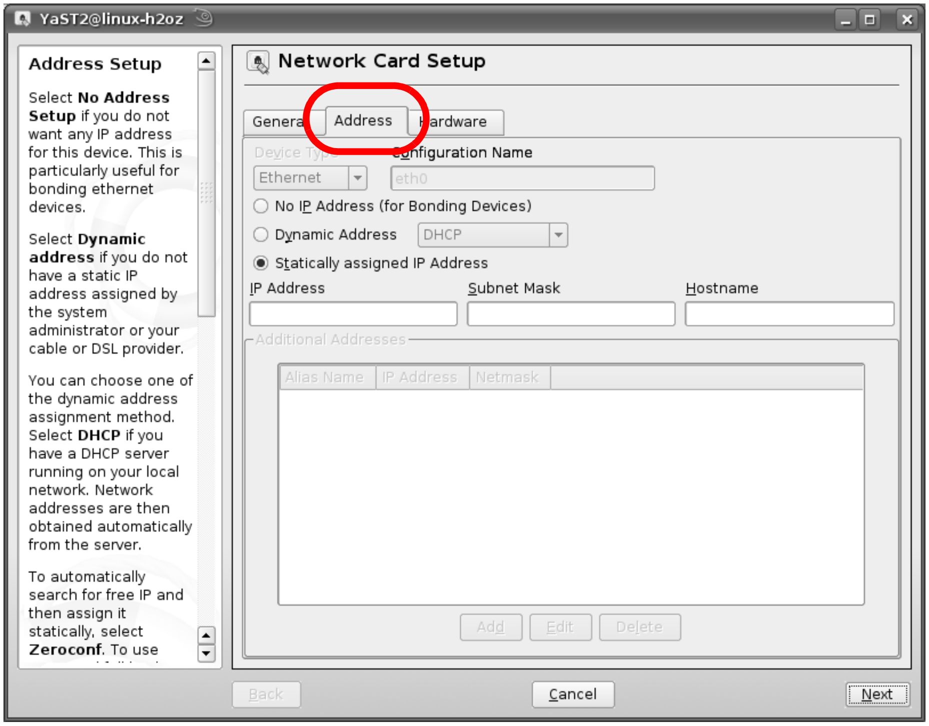
Name	IP Address
AMD PCnet - Fast 79C971	DHCP

AMD PCnet - Fast 79C971
MAC : 08:00:27:96:ed:3d

- Device Name: eth-eth0
- Started automatically at boot
- IP address assigned using DHCP

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

Figure 164 openSUSE 10.3: Network Card Setup



Address Setup

Select **No Address Setup** if you do not want any IP address for this device. This is particularly useful for bonding ethernet devices.

Select **Dynamic address** if you do not have a static IP address assigned by the system administrator or your cable or DSL provider.

You can choose one of the dynamic address assignment method. Select **DHCP** if you have a DHCP server running on your local network. Network addresses are then obtained automatically from the server.

To automatically search for free IP and then assign it statically, select **Zeroconf**. To use

Device Type: Ethernet
Configuration Name: eth0

○ No IP Address (for Bonding Devices)
○ Dynamic Address DHCP
● Statically assigned IP Address

IP Address:
Subnet Mask:
Hostname:

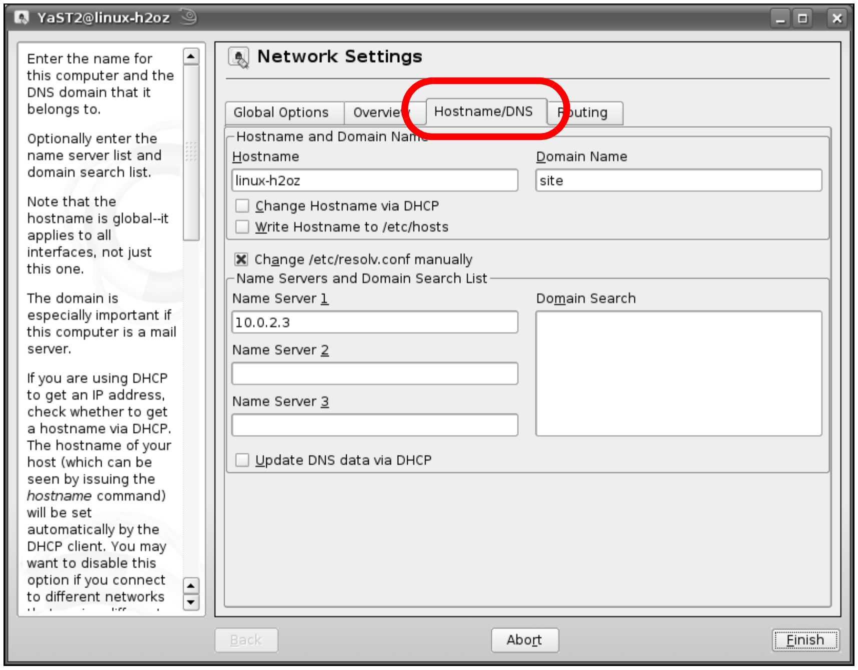
6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.

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 165 openSUSE 10.3: Network Settings



Enter the name for this computer and the DNS domain that it belongs to.

Optionally enter the name server list and domain search list.

Note that the hostname is global--it applies to all interfaces, not just this one.

The domain is especially important if this computer is a mail server.

If you are using DHCP to get an IP address, check whether to get a hostname via DHCP. The hostname of your host (which can be seen by issuing the *hostname* command) will be set automatically by the DHCP client. You may want to disable this option if you connect to different networks

Hostname and Domain Name

Hostname: linux-h2oz

Domain Name: site

☐ Change Hostname via DHCP

☐ Write Hostname to /etc/hosts

☒ Change /etc/resolv.conf manually

Name Servers and Domain Search List

Name Server 1: 10.0.2.3

Name Server 2:

Name Server 3:

Domain Search:

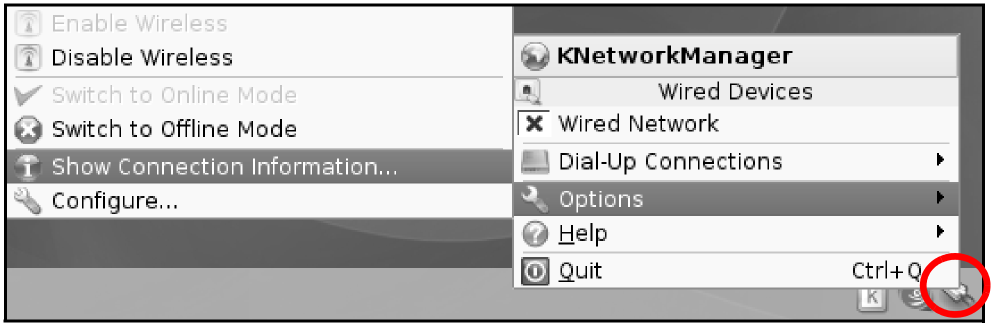
☐ Update DNS data via DHCP

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

Verifying Settings

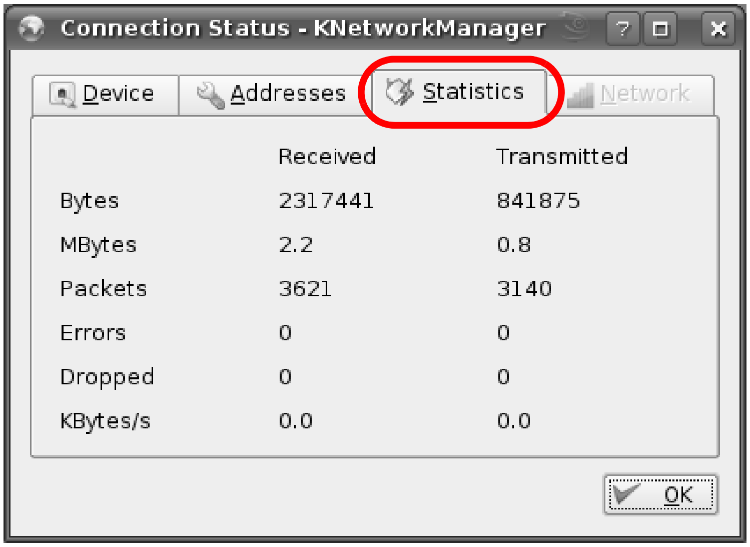
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 166 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 167 openSUSE: Connection Status - KNetwork Manager



	Received	Transmitted
Bytes	2317441	841875
MBytes	2.2	0.8
Packets	3621	3140
Errors	0	0
Dropped	0	0
KBytes/s	0.0	0.0

C

Pop-up Windows, JavaScript and Java Permissions

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

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

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

Internet Explorer Pop-up Blockers

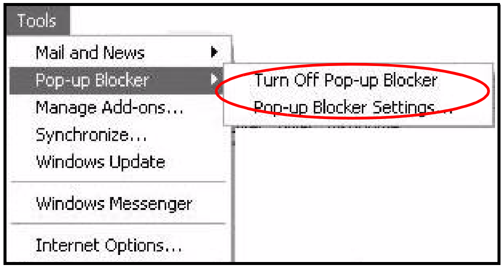
You may have to disable pop-up blocking to log into your device.

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

Disable Pop-up Blockers

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

Figure 168 Pop-up Blocker

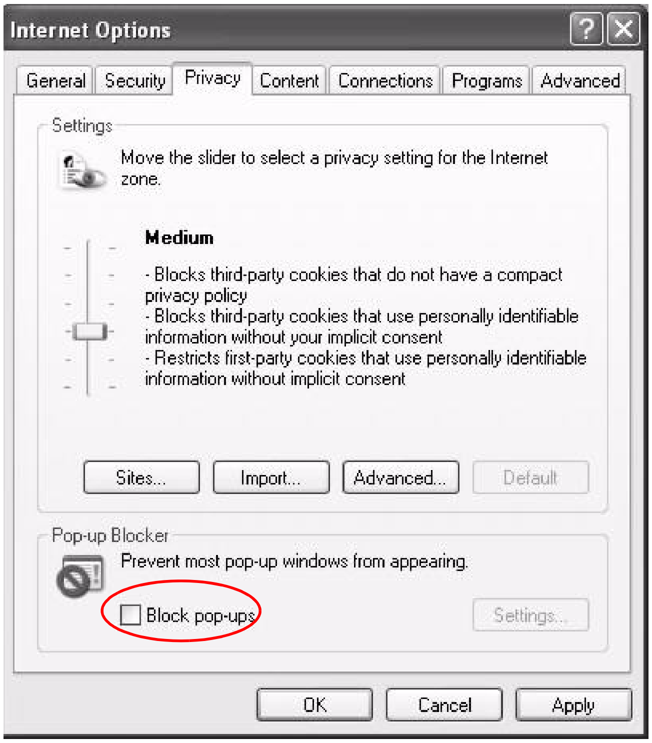


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

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 169 Internet Options: Privacy



Internet Options

Settings

Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

Pop-up Blocker

Prevent most pop-up windows from appearing.

☐ Block pop-ups

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

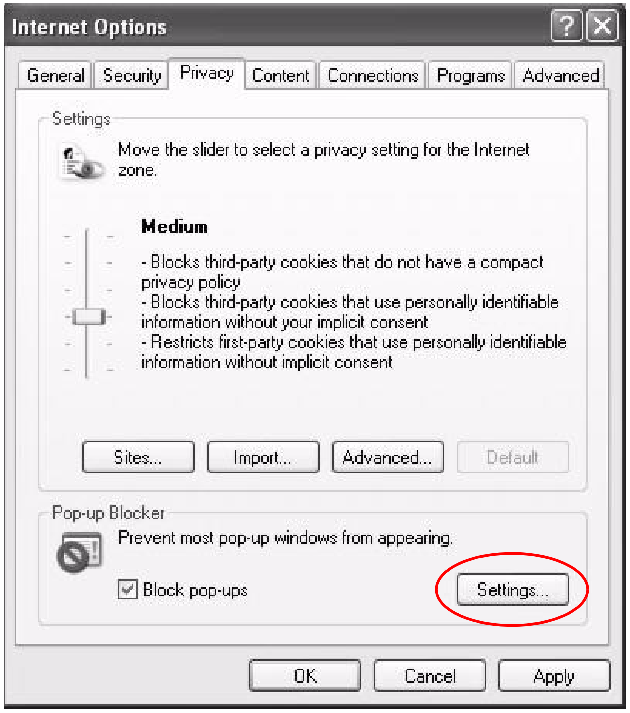
Enable Pop-up Blockers with Exceptions

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 170 Internet Options: Privacy



Settings

Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

Pop-up Blocker

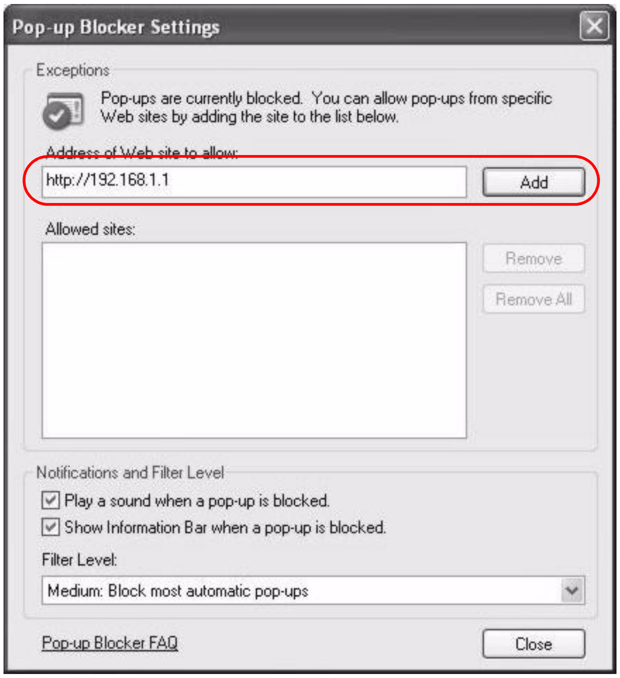
Prevent most pop-up windows from appearing.

☑ Block pop-ups

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 171 Pop-up Blocker Settings



Exceptions

Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.

Address of Web site to allow:

http://192.168.1.1

Allowed sites:

Notifications and Filter Level

☑ Play a sound when a pop-up is blocked.

☑ Show Information Bar when a pop-up is blocked.

Filter Level:

Medium: Block most automatic pop-ups

5 Click **Close** to return to the **Privacy** screen.

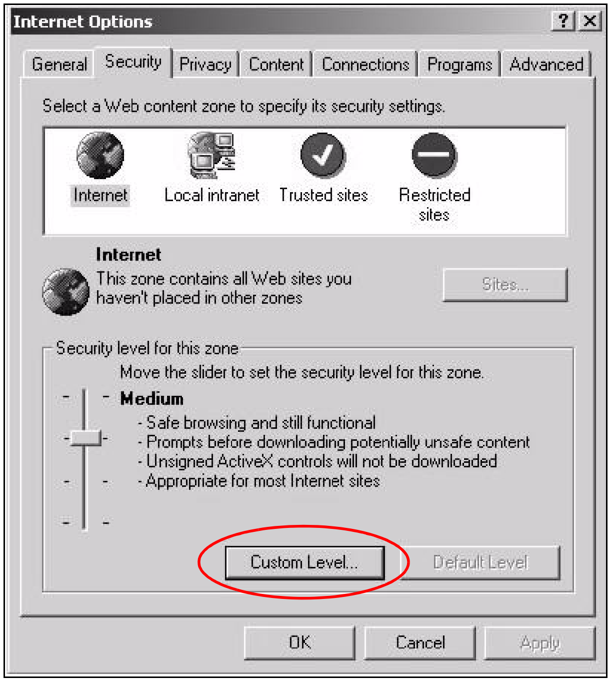
6 Click **Apply** to save this setting.

JavaScript

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

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

Figure 172 Internet Options: Security



Select a Web content zone to specify its security settings.

Internet

This zone contains all Web sites you haven't placed in other zones

Security level for this zone

Move the slider to set the security level for this zone.

Medium

- Safe browsing and still functional
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded
- Appropriate for most Internet sites

2 Click the **Custom Level...** button.

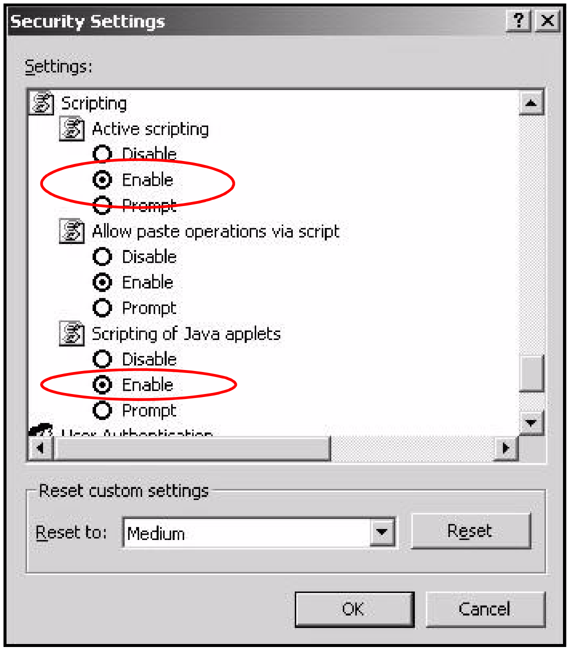
3 Scroll down to **Scripting**.

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 173 Security Settings - Java Scripting



Security Settings

Settings:

Scripting

Active scripting
- ○ Disable
- ● Enable
- ○ Prompt

Allow paste operations via script
- ○ Disable
- ● Enable
- ○ Prompt

Scripting of Java applets
- ○ Disable
- ● Enable
- ○ Prompt

User Authentication

Reset custom settings

Reset to: Medium

Java Permissions

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

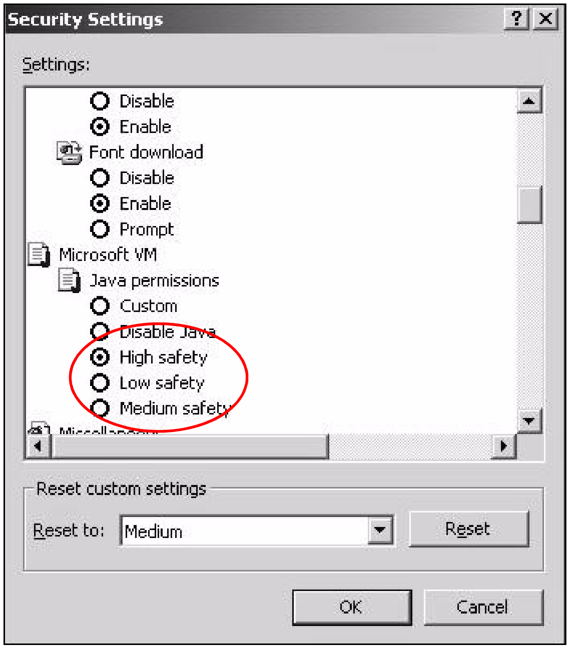
2 Click the **Custom Level...** button.

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 174 Security Settings - Java



Settings:

○ Disable
● Enable
Font download
○ Disable
● Enable
○ Prompt
Microsoft VM
Java permissions
○ Custom
○ Disable Java
● High safety
○ Low safety
○ Medium safety

Reset custom settings

Reset to: Medium

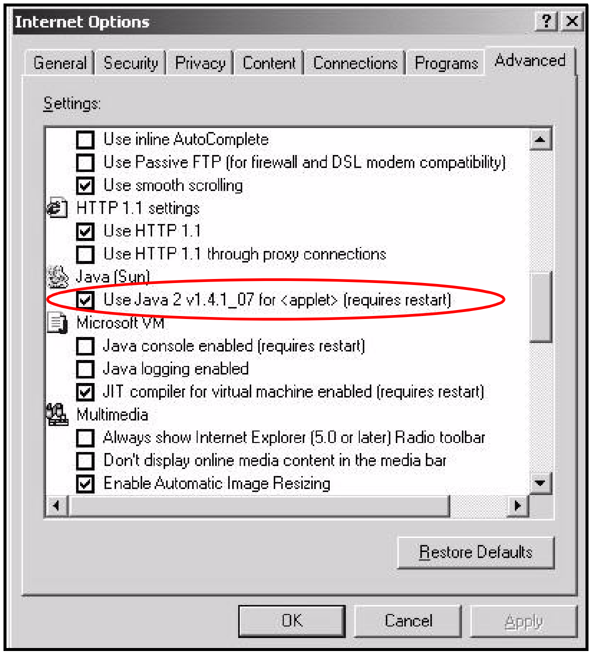
JAVA (Sun)

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 175 Java (Sun)



Settings:

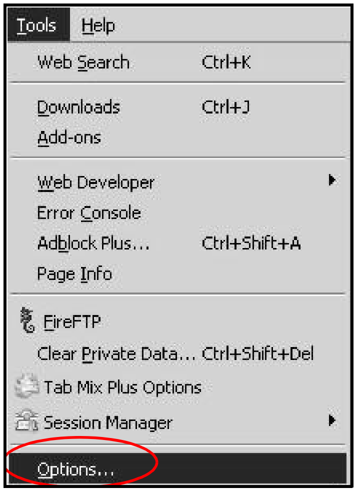
□ Use inline AutoComplete
□ Use Passive FTP (for firewall and DSL modem compatibility)
☑ Use smooth scrolling
HTTP 1.1 settings
☑ Use HTTP 1.1
□ Use HTTP 1.1 through proxy connections
Java (Sun)
☑ Use Java 2 v1.4.1_07 for <applet> (requires restart)
Microsoft VM
□ Java console enabled (requires restart)
□ Java logging enabled
☑ JIT compiler for virtual machine enabled (requires restart)
Multimedia
□ Always show Internet Explorer (5.0 or later) Radio toolbar
□ Don't display online media content in the media bar
☑ Enable Automatic Image Resizing

Mozilla Firefox

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

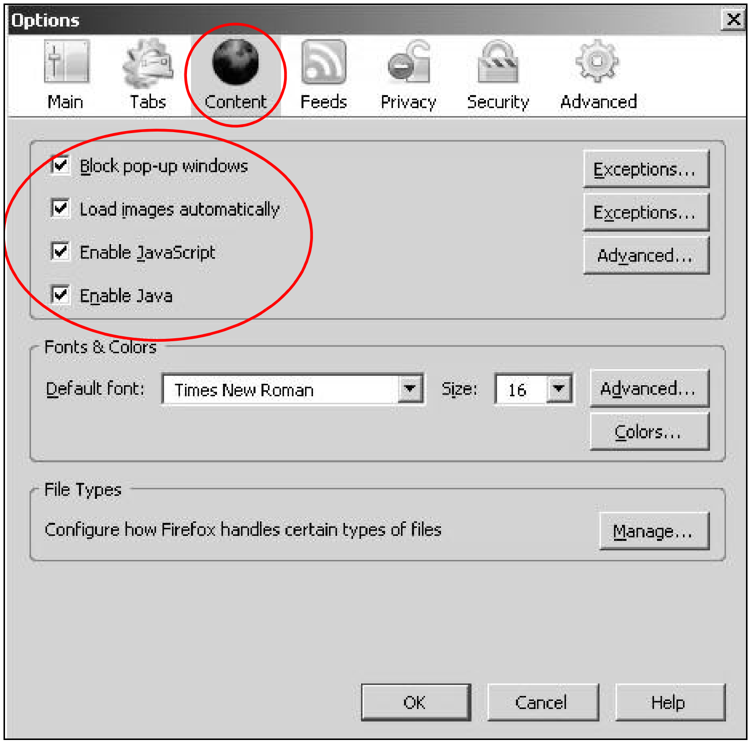
You can enable Java, Javascript and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

Figure 176 Mozilla Firefox: Tools > Options



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

Figure 177 Mozilla Firefox Content Security



☑ Block pop-up windows

☑ Load images automatically

☑ Enable JavaScript

☑ Enable Java

Fonts & Colors

Default font: Times New Roman Size: 16

File Types

Configure how Firefox handles certain types of files

D

Wireless LANs

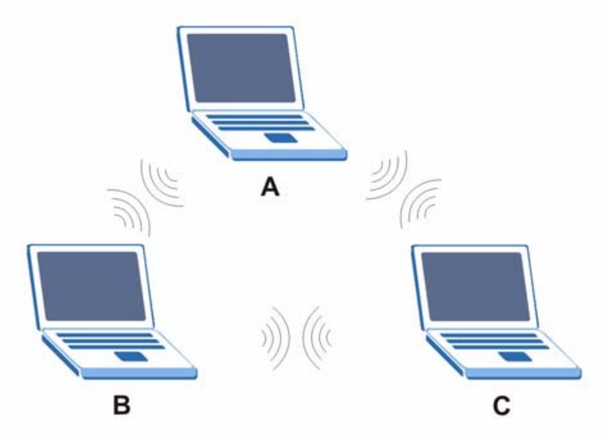
Wireless LAN Topologies

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 178 Peer-to-Peer Communication in an Ad-hoc Network

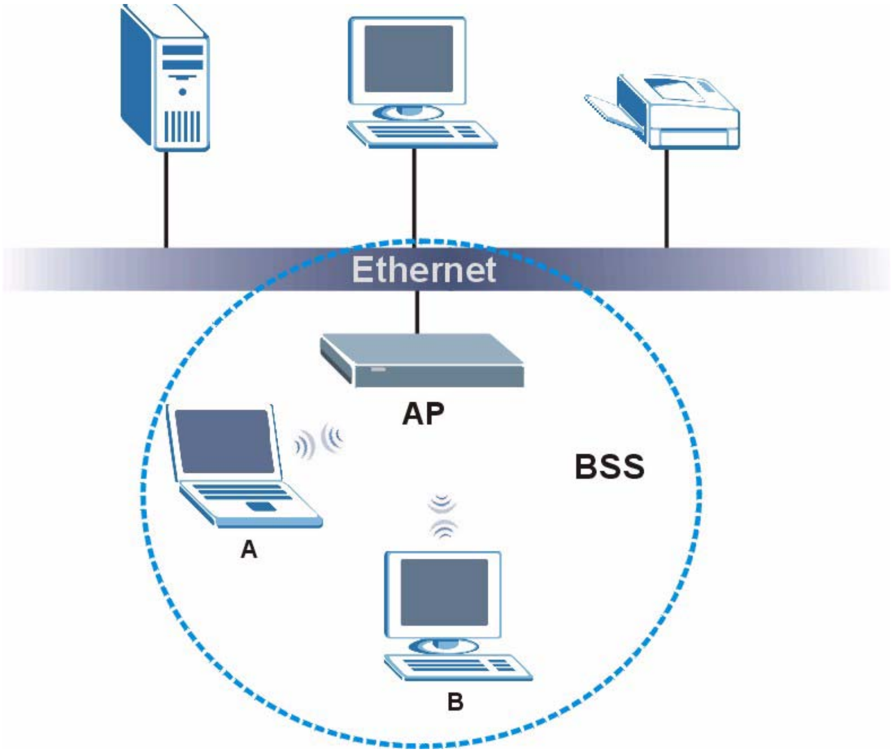


BSS

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 179 Basic Service Set



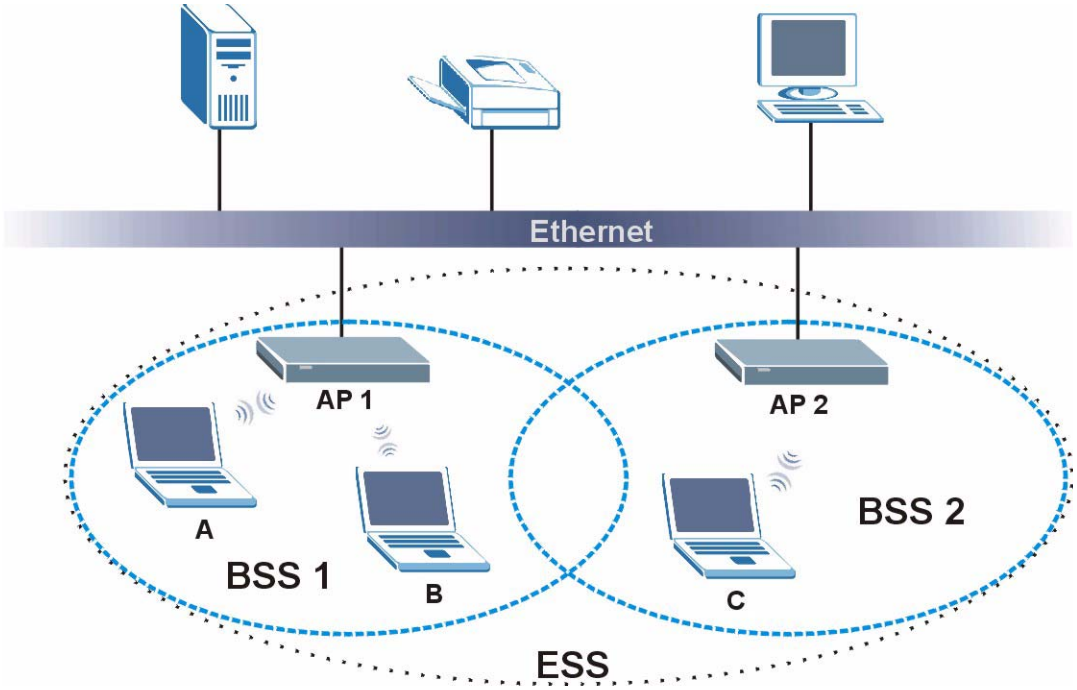
ESS

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 180 Infrastructure WLAN



Channel

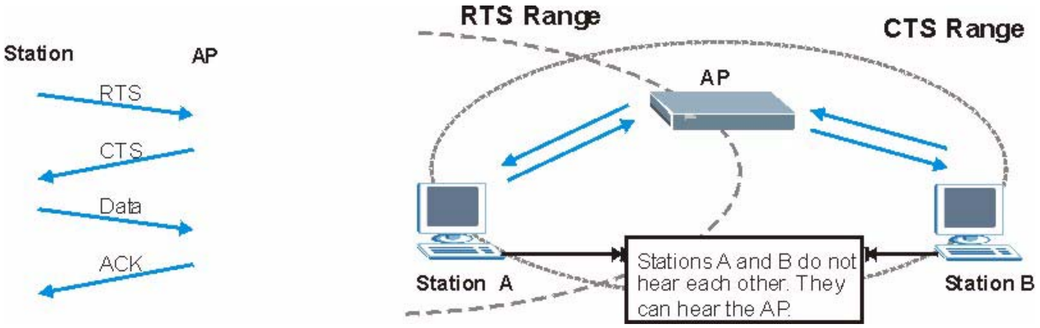
A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference 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 181 RTS/CTS


Station
AP
RTS
CTS
Data
ACK
RTS Range
CTS Range
AP
Station A
Station B
Stations A and B do not hear each other. They can hear the AP.

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 90 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 91 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)
Most Secure	WPA2

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 92 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

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA and WPA2 use Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP.

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.

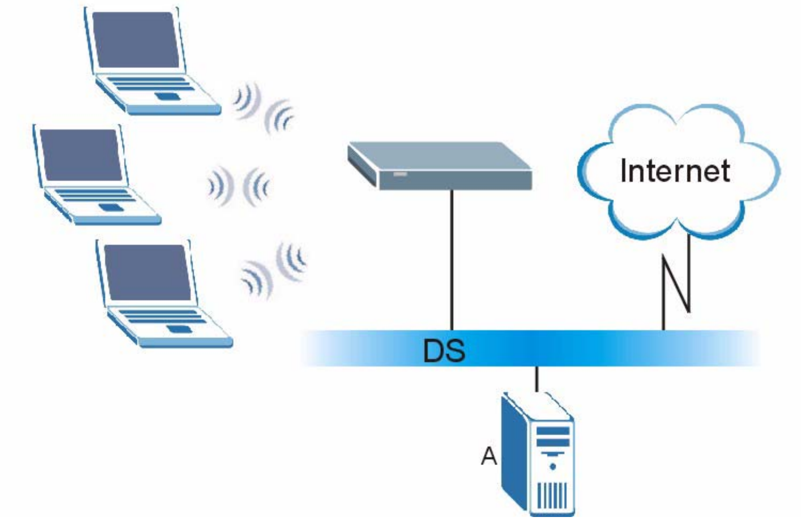
1 The AP passes the wireless client's authentication request to the RADIUS server.

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 182 WPA(2) with RADIUS Application Example



WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

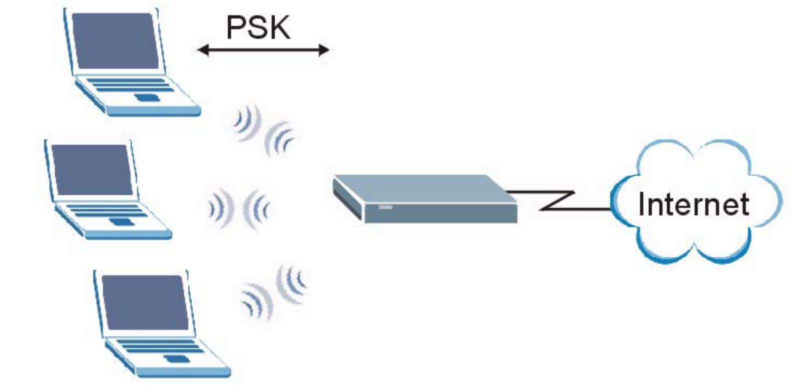
1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).

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 183 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 93 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.

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.

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 6.4 on page 93).

3 Press the button on one of the devices (it doesn't matter which).

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.

PIN Configuration

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

When you use the PIN method, you must enter the enrollee's PIN into the registrar. Then, when WPS is activated on the enrollee, it presents its PIN to the registrar. If the PIN matches, the registrar sends the network and security information to the enrollee, allowing it to join the network.

The advantage of using the PIN method rather than the PBC method is that you can ensure that the connection is established between the devices you specify, not just the first two devices to activate WPS in the area. However, you need to log into the configuration interfaces of both devices.

Take the following steps to set up WPS using the PIN method.

1 Decide which device you want to be the registrar (usually the AP) and which you want to be the enrollee (usually the client).

2 Look for the enrollee's WPS PIN; it may be displayed on the device. If you don't see it, log into the enrollee's configuration interface and locate the PIN. Select the PIN connection mode (not PBC connection mode). See the device's User's Guide for how to do this - for the ZyXEL Device, see Section 6.4 on page 93.

3 Log into the configuration utility of the registrar. Select the PIN connection mode (not the PBC connection mode). Locate the place where you can enter the enrollee's PIN (if you are using the ZyXEL Device, see Section 6.4 on page 93). Enter the PIN from the enrollee device.

4 Activate WPS on both devices within two minutes.

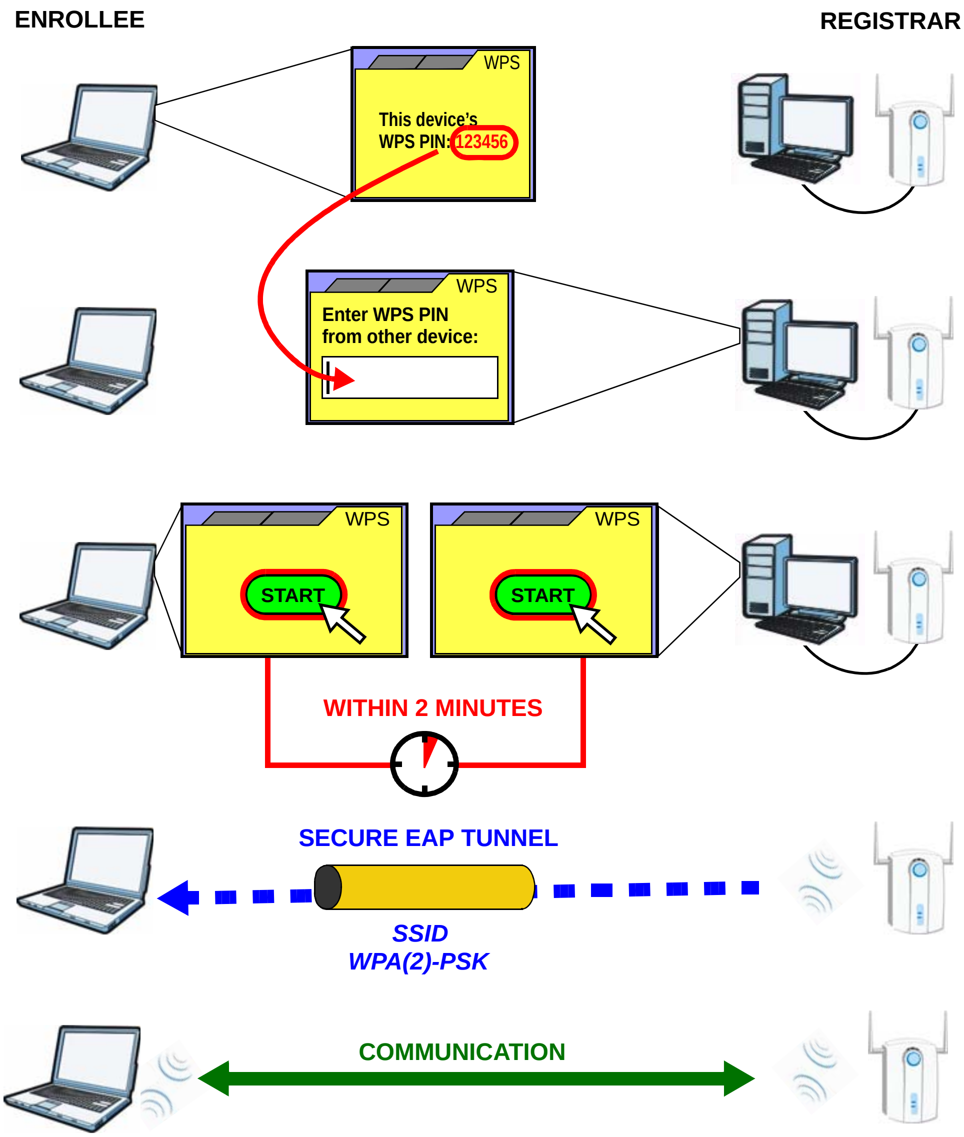
Note: Use the configuration utility to activate WPS, not the push-button on the device itself.

5 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 184 Example WPS Process: PIN Method

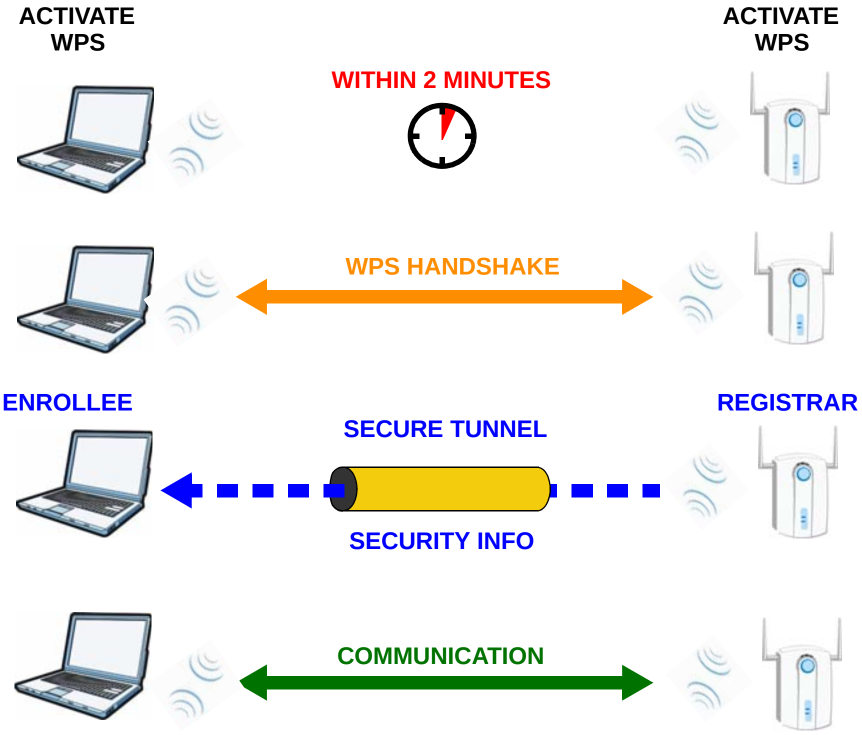


How WPS Works

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 185 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.

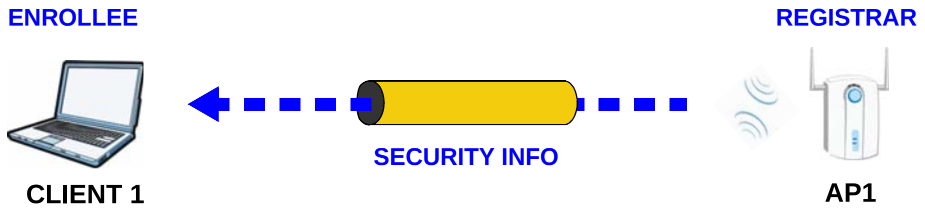
By default, a WPS devices is “unconfigured”. This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled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

Example WPS Network Setup

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

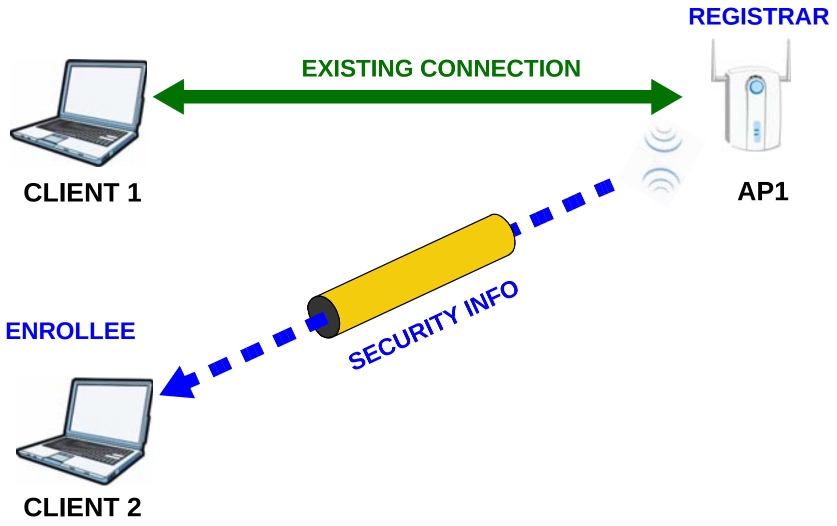
The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information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

Figure 186 WPS: Example Network Step 1



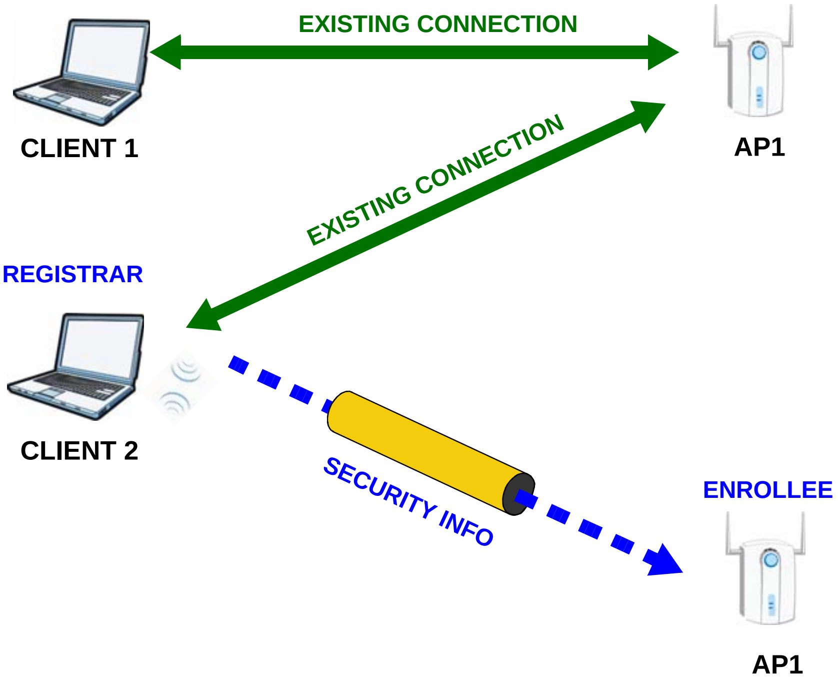
In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the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

Figure 187 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 188 WPS: Example Network Step 3



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.

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 94 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.

Table 94 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 94 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 94 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.

F

Open Software Announcements

End-User License Agreement for “P-2601HN(L)-F1”

Note: WARNING: ZyXEL Communications Corp. IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL, IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED OR ZyXEL, AND YOUR MONEY WILL BE REFUNDED.

1 Grant of License for Personal Use

ZyXEL Communications Corp. ("ZyXEL") grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the Software ("Documentation"), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

2 Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

3 Copyright

The Software and Documentation contain material that is protected by International Copyright Law and trade secret law, and by international treaty provisions. All rights not granted to you herein are expressly reserved by ZyXEL.

You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation.

4 Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. Certain components of the Software, and third party open source programs included with the Software, have been or may be made available by ZyXEL listed in the below Table (collectively the “Open-Sourced Components”) You may modify or replace only these Open-Sourced Components; provided that you comply with the terms of this License and any applicable licensing terms governing use of the Open-Sourced Components, which have been provided on the online electronic documents for the Software (ftp://opensource.zyxel.com). ZyXEL is not obligated to provide any maintenance, technical or other support for the resultant modified Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. Except as and only to the extent expressly permitted in this License, by applicable licensing terms governing use of the Open-Sourced Components, or by applicable law, you may not market, co-brand, private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing. Portions of the Software utilize or include third party software and other copyright material. Acknowledgements, licensing terms and disclaimers for such material are contained in the online electronic documentation for the Software (ftp://opensource.zyxel.com), and your use of such material is governed by their respective terms. ZyXEL has provided, as part of the Software package, access to certain third party software as a convenience. To the extent that the Software contains third party software, ZyXEL has no express or implied obligation to provide any technical or other support for such software. Please contact the appropriate software vendor or manufacturer directly for technical support and customer service related to its software and products.

5 Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms and conditions of this License Agreement to those persons employed by you who come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

6 No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

7 Limitation of Liability

IN NO EVENT WILL ZyXEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyXEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyXEL's AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED THE PRODUCT’S PRICE. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

8 Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyXEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

9 Audit Rights

ZyXEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

10 Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyXEL all copies of the Software and Documentation in your possession or under your control. ZyXEL may terminate this License Agreement for any reason, including, but not limited to, if ZyXEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyXEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

11 General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in ROC, Taiwan. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyXEL. Any waiver or modification of this License Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.

Note: Some components of this product incorporate source code covered under the open source code licenses. To obtain the source code covered under those Licenses, please check ZyXEL Technical Support (support@zyxel.com.tw) to get it.

3RD PARTY SOFTWARE	VERSION	WEB ADDRESS OF THE SOFTWARE LICENSE TERM
MIPS Linux Kernel	2.6.20	http://www.linux-mips.org
bridge-utils	1.4	http://bridge.sourceforge.net
busybox	1.10.4	http://www.busybox.net
dnsmasq	2.49	http://www.thekelleys.org.uk/dnsmasq/
dropbear	0.52	http://matt.ucc.asn.au/dropbear/dropbear.html
ebtables	2.0.8-1	http://ebtables.sourceforge.net
iproute2	2.6.20	http://www.linuxgrill.com/anonymous/iproute2
iptables	1.3.8	http://www.netfilter.org
libbase64	0.0.1	http://www.gnu.org/software/gnulib
libedit	20080712-2.11	http://libedit.sourceforge.net
libupnp	1.4.2	http://www.libupnp.org/
libpcap	1.0.0	http://www.tcpdump.org/
linuxigd	1	http://linux-igd.sourceforge.net
logrotate	3.7.1	http://logrotate.darwinports.com/
mini_httpd		http://www.acme.com/software/mini_httpd/
mtd-utils	1.0.0	http://www.linux-mtd.infradead.org/
ncurses	5.7	http://www.gnu.org/software/ncurses/
openssh	5.2p1	http://www.openssh.com
ppp	2.4.4	http://www.roaringpenguin.com/pppoe
pure-ftpd	1.0.23	http://pureftpd.org
sntp		http://www.broadcom.com
syslog-ng	2.0.6	http://www.balabit.com/network-security/syslog-ng/
sysstat	8.1.8	http://pagesperso-orange.fr/sebastien.godard/
tcpdump	4.0.0	http://www.tcpdump.org/
updatedd	2.6	http://www.philipp-benner.de/updatedd/
wireless_tools	0.29	http://www.hpl.hp.com/

G

Legal Information

Copyright

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.

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 is designed for the WLAN 2.4 GHz and/or 5 GHz networks throughout the EC region and Switzerland, with restrictions in France.

Ce produit est conçu pour les bandes de fréquences 2,4 GHz et/ou 5 GHz conformément à la législation Européenne. En France métropolitaine, suivant les décisions n°03-908 et 03-909 de l'ARCEP, la puissance d'émission ne devra pas dépasser 10 mW (10 dB) dans le cadre d'une installation WiFi en extérieur pour les fréquences comprises entre 2454 MHz et 2483,5 MHz.

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

Note

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

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

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

Index

A

AAL5 247
ACK message 196
activation
- SSID 91
- wireless LAN
  - scheduling 97

administrator password 28
ADSL2 compliance 247
ADSL2+ compliance 247
Advanced Encryption Standard, see AES
AES 309
alternative subnet mask notation 256
antenna
- directional 314
- gain 313
- omni-directional 314

AP (Access Point) 301
applications
- Internet access 22
- VoIP 22

Asynchronous Transfer Mode 235
ATM
- QoS 79

ATM Adaptation Layer 5, see AAL5
audience 3
authentication 98, 100
- RADIUS server 100

automatic logout 28

B

backup
- configuration 229

bandwidth management 135
Basic Service Set, see BSS
blinking LEDs 24
broadcast 68
BSS 101, 299
- example 102

BYE request 196

C

CA 167, 307
call forwarding 248
call hold 200
call return 248
call rule 189, 190
call service mode 199
call transfer 200
call waiting 200, 248
caller ID 248
CBR 79
CBR (Constant Bit Rate) 72
certificate
- factory default 171

Certificate Authority, see CA
certificates 167
- CA 167
- replacing 171
- storage space 171
- thumbprint algorithms 170
- thumbprints 170
- trusted CAs 172, 173
- verifying fingerprints 169

Certification Authority, see CA
certifications 333
- notices 334
- viewing 335

channel 301
- interference 301

channel scan 85
channel, wireless LAN 83
Class of Service 197
Class of Service, see CoS
client list 114

client-server protocol 193
codecs 249
comfort noise generation 176, 248
command interface 24
configuration 117
  backup 229
  reset 231
  restoring 230
copyright 333
CoS 147, 197
country code 248
CTS (Clear to Send) 302
CTS threshold 98

D

data fragment threshold 98
default LAN IP address 27
Denial of Service, see DoS
device management
  command interface 24
  Telnet 24
DHCP 64, 112, 117, 118, 157
DHCP relay 244
DHCP server 244
diagnostic 233
differentiated services 198
Differentiated Services, see DiffServ
DiffServ (Differentiated Services) 197
  code points 197
  marking rule 148, 198
disclaimer 333
DNS 112, 131
domain name system, see DNS
DS (Differentiated Services) 148
DS field 148, 198
DSCP 147, 197
DSL line, reinitialize 236
DTMF 197
  detection and generation 249
Dual-Tone MultiFrequency, see DTMF
dynamic DNS 157
Dynamic Host Configuration Protocol, see DHCP
dynamic jitter buffer 248
dynamic WEP key exchange 308
DYNDNS wildcard 157

E

EAP Authentication 306
echo cancellation 176, 249
encapsulation 67
  PPPoA 77
  PPPoE 76
encryption 100, 309
ESS 300
Europe type call service mode 199
Extended Service Set IDentification 84, 93
Extended Service Set, see ESS

F

FCC interference statement 333
filters
  MAC address 99
firewalls 159
  configuration 161
  security 163
firmware 227
flash key 199
flashing 199
fragmentation threshold 98, 303
frequency range 250
FTP 150
FXO 190

G

G.168 176, 249
G.711 249
G.729 249

H

hidden node 301

host 213

host name 63

humidity 243

I

IAD 21

IANA 119, 262

IBSS 299

IEEE 802.11g 303

IEEE 802.11g wireless LAN 249

IEEE 802.11i 249

IEEE 802.1Q VLAN 198

IGMP 68

importing trusted CAs 173

Independent Basic Service Set, see IBSS

initialization vector (IV) 309

install UPnP 119
- Windows Me 119
- Windows XP 121

Integrated Access Device, see IAD

intended audience 3

Internet access 22

Internet Assigned Numbers Authority
- See IANA

Internet Assigned Numbers Authority, see IANA

IP address 64, 68, 77, 118
- default 27
- ping 233

IP pool 114

IP pool setup 118

ITU-T 176

ITU-T G.992.1 236

J

jitter buffer 248

L

LAN 111
- client list 114
- MAC address 115

LAN TCP/IP 118

limitations
- wireless LAN 101
- WPS 108

listening port 180

Local Area Network, see LAN

login
- passwords 28

logout 28
- automatic 28

logs 203, 207, 225

M

MAC 64

MAC address 115
- filter 99

Management Information Base (MIB) 218

managing the device
- command interface 24
- good habits 24
- Telnet 24
- using FTP. See FTP.

Maximum Burst Size (MBS) 72

MBS 78

MBSSID 102

Media Access Control, see MAC Address

Message Integrity Check, see MIC

MIC 309

model name 63

multicast 68
- IGMPInternet Group Multicast Protocol, see IGMP

multimedia 192

Multiple BSS, see MBSSID

multiple voice channels 248

multiplexing 77
- LLC-based 77, 247
- VC-based 77, 247

N

NAT 118, 151, 261
  definitions 154
  how it works 155
  what it does 155
Network Address Translation, see NAT
network map 31
non-proxy calls 189

O

OK response 196
operation humidity 243
operation temperature 243

P

Pairwise Master Key (PMK) 309, 311
passphrase 87
passwords 28
PBC 103
PCR 78
Peak Cell Rate (PCR) 72
peer-to-peer calls 23, 189
Per-Hop Behavior, see PHB
PHB 148, 198
phone book
  speed dial 189
phone config 248
PIN, WPS 104
  example 105
point-to-point calls 249
ports 24
power adaptor 250
power specifications 243
PPP (Point-to-Point Protocol) Link Layer Protocol 247
PPPoA 77
PPPoE 76, 246
preamble 98
preamble mode 303
product registration 336
profile 42
PSK 309
PSTN call setup signaling 197
Public Switched Telephone Network 21
pulse dialing 197
Push Button Configuration, see PBC
push button, WPS 103
PVC 247

Q

QoS 135, 136, 147, 197, 249
Quality of Service 249
Quality of Service, see QoS
quick dialing 249
Quick Start Guide 27

R

RADIUS 305
  message types 305
  messages 305
  shared secret key 306
RADIUS server 100
Real time Transport Protocol, see RTP
region 248
registration
  product 336
reinitialize the ADSL line 236
related documentation 3
Request To Send, see RTS
reset 231
RESET button 25
restart 231
restoring configuration 230
RFC 1631 149
RFC 1889 195, 249
RFC 1890 249
RFC 2327 249
RFC 2516 246
RFC 3261 249

RFC3262 support 186

router features 22

RTCP 249

RTP 195, 249

RTS (Request To Send) 302
- threshold 301, 302

RTS threshold 98

S

safety warnings 7

scan 85

scheduling
- wireless LAN 97

SCR 78

SDP 249

security
- wireless LAN 98

security, network 163

service access control 216

Service Set 84, 93

Session Description Protocol 249

Session Initiation Protocol, see SIP

shaping traffic 78, 79

silence suppression 176, 248

Simple Network Management Protocol, see SNMP

SIP 192
- account 192
- call progression 195
- client 193
- identities 192
- INVITE request 196
- number 192
- proxy server 194
- redirect server 194
- register server 195
- servers 193
- service domain 192
- URI 192
- user agent 193
- version 2 249

SNMP 217, 218
- agents 218
- Get 218
- GetNext 218
- Manager 218
- managers 218
- MIB 218
- network components 217
- Set 218
- Trap 218
- versions 217

speed dial 189

SSID 99
- activation 91
- MBSSID 102

stateful inspection 245

static route 127

status 61

status bar 34

status indicators 24

storage humidity 243

storage temperature 243

subnet 253

subnet mask 118, 254

subnetting 256

supplementary services 198

Sustain Cell Rate (SCR) 72

syntax conventions 5

system
- firmware 227
- passwords 28
- status 61

System Info 63

system name 63, 222

T

Telnet 24

temperature 243

Temporal Key Integrity Protocol, see TKIP

three-way conference 200

thresholds
- data fragment 98
- RTS/CTS 98

TKIP 309

ToS 197

traffic shaping 78

example 79
transparent bridging 247
trusted CAs, and certificates 172
tutorial
VoIP 47
wireless 38
Type of Service, see ToS

U

UBR 80
unicast 68
Uniform Resource Identifier 192
Universal Plug and Play, see UPnP
upgrading firmware 227
UPnP 116
forum 113
security issues 112

V

VAD 176, 248
VBR 79
VBR-nRT 79
VBR-RT 79
VCI 77
version
firmware
version 64
Virtual Local Area Network, see VLAN
VLAN 198
group 198
ID 198
ID tags 198
voice activity detection 176, 248
voice channels 248
voice coding 196
VoIP 191
features 22
peer-to-peer calls 189
tutorial 47
VoIP features 22, 23
VoIP status 210
VPI 77

W

WAN 67
ATM QoS 79
encapsulation 67
IGMP 68
IP address 68, 77
multicast 68
multiplexing 77
traffic shaping 78
example 79
VCI 77
VPI 77
warnings 7
warranty 335
note 335
Web Configurator 27
web configurator
passwords 28
WEP 87, 101
WEP Encryption 88
Wide Area Network, see WAN
Wi-Fi Protected Access, see WPA
wireless
client configuration 40
profile 42
security 304
tutorial 38
wireless client WPA supplicants 310
wireless LAN 81
authentication 98, 100
BSS 101
example 102
channel 83
encryption 100
example 82
fragmentation threshold 98
limitations 101
MAC address filter 99, 249
MBSSID 102
preamble 98
RADIUS server 100
RTS/CTS threshold 98
scheduling 97

security 98
SSID 99
activation 91
WEP 101
WPA 101
WPA-PSK 101
WPS 103, 105
example 107
limitations 108
PIN 104
push button 103

wireless network
example 81

wireless security 304

WLAN 81
auto-scan channel 85
button 26
interference 301
passphrase 87
scheduling 97
security parameters 312
see also wireless.
WEP 87

WPA 101, 249, 308
key caching 310
pre-authentication 310
user authentication 310
vs WPA-PSK 309
wireless client supplicant 310
with RADIUS application example 310

WPA2 308
user authentication 310
vs WPA2-PSK 309
wireless client supplicant 310
with RADIUS application example 310

WPA2-Pre-Shared Key, see WPA2-PSK

WPA2-PSK 308, 309
application example 311

WPA-PSK 101, 309
application example 311

WPS 103, 105
example 107
limitations 108
PIN 104
example 105
push button 103