

P-660RU-T v2 Series

ADSL 2+ USB / Ethernet Router

User's Guide

Version 3.40

12/2006

Edition 1



About This User's Guide

Intended Audience

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

Related Documentation

- Quick Start Guide
The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.
- Web Configurator Online Help
Embedded web help for descriptions of individual screens and supplementary information.



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

- Supporting Disk
Refer to the included CD for support documents.
- ZyXEL Web Site
Please refer to www.zyxel.com for additional support documentation and product certifications.

User Guide Feedback

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

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

E-mail: techwriters@zyxel.com.tw

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.








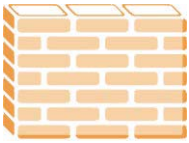



Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The P-660RU-T v2 may be referred to as the “ZyXEL Device”, the “device”, the “product” or the “system” in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the “enter” or “return” key on your keyboard.
- “Enter” means for you to type one or more characters and then press the [ENTER] key. “Select” or “choose” means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the “metric” value or the “scientific” value. For example, “k” for kilo may denote “1000” or “1024”, “M” for mega may denote “1000000” or “1048576” and so on.
- “e.g.” is a shorthand for “for instance”, and “i.e.” means “that is” or “in other words”.

Icons Used in Figures

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

ZyXEL Device 	Computer 	Notebook computer 
Server 	DSLAM 	Firewall 
Telephone 	Switch 	Router 

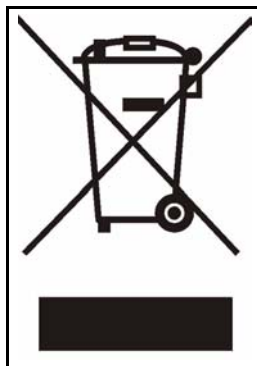
Safety Warnings



For your safety, be sure to read and follow all warning notices and instructions.

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

This product is recyclable. Dispose of it properly.



Contents Overview

Introduction	23
Introducing the ZyXEL Device	25
Introducing the Web Configurator	29
Wizard	35
Wizard Setup	37
Advanced	49
Password Setup	51
LAN Setup	53
WAN Setup	59
Security	69
Dynamic DNS Setup	71
Time and Date	73
Remote Management Configuration	75
Universal Plug-and-Play (UPnP)	79
Network Address Translation (NAT) Screens	91
Maintenance and Troubleshooting	101
Maintenance	103
Troubleshooting	115
Appendices and Index	119

Table of Contents

About This User's Guide	3
Document Conventions.....	4
Safety Warnings.....	6
Contents Overview	9
Table of Contents.....	11
List of Figures	17
List of Tables.....	21
Part I: Introduction.....	23
Chapter 1	
Introducing the ZyXEL Device	25
1.1 Overview	25
1.2 Ways to Manage the ZyXEL Device	26
1.3 Good Habits for Managing the ZyXEL Device	27
1.4 ZyXEL Device Hardware Installation and Connection	27
1.5 LEDs	27
Chapter 2	
Introducing the Web Configurator	29
2.1 Web Configurator Overview	29
2.1.1 Accessing the ZyXEL Device Web Configurator	29
2.2 Resetting the ZyXEL Device	30
2.3 Navigating the ZyXEL Device Web Configurator	31
2.4 The Site Map Screen	32
Part II: Wizard	35
Chapter 3	
Wizard Setup	37
3.1 Introduction	37

3.1.1 Encapsulation	37
3.1.2 Multiplexing	38
3.1.3 VPI and VCI	38
3.1.4 Internet Access Wizard Setup: First Screen	38
3.2 IP Address and Subnet Mask	39
3.2.1 IP Address Assignment	39
3.2.2 Nailed-Up Connection (PPP)	40
3.2.3 NAT	41
3.2.4 Internet Access Wizard Setup: Second Screen	41
3.2.5 DHCP Setup	45
3.2.6 Internet Access Wizard Setup: Third Screen	45
3.2.7 Internet Access Wizard Setup: Connection Test	46
Part III: Advanced.....	49
Chapter 4	
Password Setup.....	51
4.1 Password Overview	51
4.1.1 Configuring Password	51
Chapter 5	
LAN Setup.....	53
5.1 LAN Overview	53
5.1.1 LANs, WANs and the ZyXEL Device	53
5.2 DNS Server Addresses	54
5.3 LAN TCP/IP	54
5.3.1 Factory LAN Defaults	54
5.3.2 IP Address and Subnet Mask	54
5.3.3 RIP Setup	55
5.3.4 Multicast	55
5.4 Any IP	56
5.4.1 How Any IP Works	56
5.5 Configuring the LAN	57
Chapter 6	
WAN Setup.....	59
6.1 WAN Overview	59
6.2 Metric	59
6.3 PPPoE Encapsulation	60
6.4 Traffic Shaping	60
6.5 Zero Configuration Internet Access	61

6.6 Configuring WAN Setup	61
6.7 Traffic Redirect	64
6.8 Configuring WAN Backup	65
Chapter 7	
Security	69
7.1 Configuring Internet Security	69
Chapter 8	
Dynamic DNS Setup	71
8.1 Dynamic DNS	71
8.1.1 DYNDNS Wildcard	71
8.2 Configuring Dynamic DNS	71
Chapter 9	
Time and Date	73
9.1 Configuring Time and Date	73
Chapter 10	
Remote Management Configuration	75
10.1 Remote Management Overview	75
10.1.1 Remote Management Limitations	75
10.1.2 Remote Management and NAT	76
10.1.3 System Timeout	76
10.2 Telnet	76
10.3 FTP	76
10.4 Web	76
10.5 Configuring Remote Management	76
Chapter 11	
Universal Plug-and-Play (UPnP).....	79
11.1 Introducing Universal Plug and Play (UPnP)	79
11.1.1 How do I know if I'm using UPnP?	79
11.1.2 NAT Traversal	79
11.1.3 Cautions with UPnP	79
11.2 UPnP and ZyXEL	80
11.2.1 Configuring UPnP	80
11.3 Installing UPnP in Windows	80
11.3.1 Installing UPnP in Windows Me	81
11.3.2 Installing UPnP in Windows XP	82
11.4 Using UPnP in Windows XP: Example	84
11.4.1 Web Configurator Easy Access	87

Chapter 12
Network Address Translation (NAT) Screens..... 91

- 12.1 NAT Overview 91
 - 12.1.1 NAT Definitions 91
 - 12.1.2 What NAT Does 92
 - 12.1.3 How NAT Works 92
 - 12.1.4 NAT Application 93
 - 12.1.5 NAT Mapping Types 93
- 12.2 SUA (Single User Account) Versus NAT 94
- 12.3 SUA Server 95
 - 12.3.1 Default Server IP Address 95
 - 12.3.2 Port Forwarding: Services and Port Numbers 95
 - 12.3.3 Configuring Servers Behind SUA (Example) 96
- 12.4 Selecting the NAT Mode 96
- 12.5 Configuring SUA Server 97
- 12.6 Configuring Address Mapping 98
- 12.7 Editing an Address Mapping Rule 99

Part IV: Maintenance and Troubleshooting 101

Chapter 13
Maintenance 103

- 13.1 Maintenance Overview 103
- 13.2 System Status Screen 103
 - 13.2.1 System Statistics 105
- 13.3 DHCP Table Screen 106
- 13.4 Any IP Table Screen 107
- 13.5 Diagnostic Screens 108
 - 13.5.1 Diagnostic General Screen 108
 - 13.5.2 Diagnostic DSL Line Screen 109
- 13.6 Firmware Screen 110
- 13.7 Configuration Screen 111
 - 13.7.1 Backup Configuration 112
 - 13.7.2 Restore Configuration 112
 - 13.7.3 Reset to Factory Defaults 114

Chapter 14
Troubleshooting..... 115

- 14.1 Power, Hardware Connections, and LEDs 115
- 14.2 ZyXEL Device Access and Login 116
- 14.3 Internet Access 117

Part V: Appendices and Index	119
Appendix A Product Specifications.....	121
Appendix B Setting up Your Computer's IP Address.....	125
Appendix C IP Addresses and Subnetting	141
Appendix D Pop-up Windows, JavaScripts and Java Permissions.....	149
Appendix E Virtual Circuit Topology	155
Appendix F Legal Information	157
Appendix G Customer Support	161
Index.....	165

List of Figures

Figure 1 ZyXEL Device Internet Access Application	25
Figure 2 ZyXEL Device LAN-to-LAN Application	25
Figure 3 Password Screen	30
Figure 4 Change Password at Login	30
Figure 5 Web Configurator: Site Map Screen	32
Figure 6 Internet Access Wizard Setup: First Screen	39
Figure 7 Internet Connection with PPPoE	41
Figure 8 Internet Connection with RFC 1483	42
Figure 9 Internet Connection with ENET ENCAP	43
Figure 10 Internet Connection with PPPoA	44
Figure 11 Internet Access Wizard Setup: Third Screen	45
Figure 12 Internet Access Wizard Setup: LAN Configuration	46
Figure 13 Internet Access Wizard Setup: Connection Tests	47
Figure 14 Password	51
Figure 15 LAN and WAN IP Addresses	53
Figure 16 Any IP Example	56
Figure 17 LAN Setup	57
Figure 18 Example of Traffic Shaping	61
Figure 19 WAN Setup (PPPoE)	62
Figure 20 Traffic Redirect Example	64
Figure 21 Traffic Redirect LAN Setup	65
Figure 22 WAN Backup	66
Figure 23 Internet Security	69
Figure 24 Dynamic DNS	72
Figure 25 Time and Date	73
Figure 26 Remote Management	77
Figure 27 Configuring UPnP	80
Figure 28 Add/Remove Programs: Windows Setup: Communication	81
Figure 29 Add/Remove Programs: Windows Setup: Communication: Components	82
Figure 30 Network Connections	82
Figure 31 Windows Optional Networking Components Wizard	83
Figure 32 Networking Services	83
Figure 33 Network Connections	84
Figure 34 Internet Connection Properties	85
Figure 35 Internet Connection Properties: Advanced Settings	85
Figure 36 Internet Connection Properties: Advanced Settings: Add	86
Figure 37 System Tray Icon	86
Figure 38 Internet Connection Status	87

Figure 39 Network Connections	88
Figure 40 Network Connections: My Network Places	89
Figure 41 Network Connections: My Network Places: Properties: Example	89
Figure 42 How NAT Works	92
Figure 43 NAT Application With IP Alias	93
Figure 44 Multiple Servers Behind NAT Example	96
Figure 45 NAT Mode	96
Figure 46 Edit SUA/NAT Server Set	97
Figure 47 Address Mapping Rules	98
Figure 48 Address Mapping Rule Edit	99
Figure 49 System Status	104
Figure 50 System Status: Show Statistics	105
Figure 51 DHCP Table	107
Figure 52 Any IP Table	107
Figure 53 Diagnostic: General	108
Figure 54 Diagnostic: DSL Line	109
Figure 55 Firmware Upgrade	110
Figure 56 Network Temporarily Disconnected	111
Figure 57 Error Message	111
Figure 58 Configuration	112
Figure 59 Backup Configuration	112
Figure 60 Restore Configuration	113
Figure 61 Restore Configuration Successful	113
Figure 62 Network Temporarily Disconnected	114
Figure 63 Reset to Factory Default Settings	114
Figure 64 WIndows 95/98/Me: Network: Configuration	126
Figure 65 Windows 95/98/Me: TCP/IP Properties: IP Address	127
Figure 66 Windows 95/98/Me: TCP/IP Properties: DNS Configuration	128
Figure 67 Windows XP: Start Menu	129
Figure 68 Windows XP: Control Panel	129
Figure 69 Windows XP: Control Panel: Network Connections: Properties	130
Figure 70 Windows XP: Local Area Connection Properties	130
Figure 71 Windows XP: Internet Protocol (TCP/IP) Properties	131
Figure 72 Windows XP: Advanced TCP/IP Properties	132
Figure 73 Windows XP: Internet Protocol (TCP/IP) Properties	133
Figure 74 Macintosh OS 8/9: Apple Menu	134
Figure 75 Macintosh OS 8/9: TCP/IP	134
Figure 76 Macintosh OS X: Apple Menu	135
Figure 77 Macintosh OS X: Network	136
Figure 78 Red Hat 9.0: KDE: Network Configuration: Devices	137
Figure 79 Red Hat 9.0: KDE: Ethernet Device: General	137
Figure 80 Red Hat 9.0: KDE: Network Configuration: DNS	138
Figure 81 Red Hat 9.0: KDE: Network Configuration: Activate	138

Figure 82 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0	139
Figure 83 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0	139
Figure 84 Red Hat 9.0: DNS Settings in resolv.conf	139
Figure 85 Red Hat 9.0: Restart Ethernet Card	139
Figure 86 Red Hat 9.0: Checking TCP/IP Properties	140
Figure 87 Network Number and Host ID	142
Figure 88 Subnetting Example: Before Subnetting	144
Figure 89 Subnetting Example: After Subnetting	145
Figure 90 Pop-up Blocker	149
Figure 91 Internet Options: Privacy	150
Figure 92 Internet Options: Privacy	151
Figure 93 Pop-up Blocker Settings	151
Figure 94 Internet Options: Security	152
Figure 95 Security Settings - Java Scripting	153
Figure 96 Security Settings - Java	153
Figure 97 Java (Sun)	154
Figure 98 Virtual Circuit Topology	155

List of Tables

Table 1 ADSL Standards	26
Table 2 LED Description	27
Table 3 Web Configurator Screens Summary	32
Table 4 Internet Access Wizard Setup: First Screen	39
Table 5 Internet Connection with PPPoE	41
Table 6 Internet Connection with RFC 1483	42
Table 7 Internet Connection with ENET ENCAP	43
Table 8 Internet Connection with PPPoA	44
Table 9 Internet Access Wizard Setup: LAN Configuration	46
Table 10 Password	51
Table 11 LAN Setup	58
Table 12 WAN Setup	62
Table 13 WAN Backup	66
Table 14 Internet Security	70
Table 15 Dynamic DNS	72
Table 16 Time and Date	74
Table 17 Remote Management	77
Table 18 Configuring UPnP	80
Table 19 NAT Definitions	91
Table 20 NAT Mapping Types	94
Table 21 Services and Port Numbers	95
Table 22 NAT Mode	96
Table 23 Edit SUA/NAT Server Set	98
Table 24 Address Mapping Rules	99
Table 25 Address Mapping Rule Edit	100
Table 26 System Status	104
Table 27 System Status: Show Statistics	106
Table 28 DHCP Table	107
Table 29 Any IP Table	107
Table 30 Diagnostic: General	109
Table 31 Diagnostic: DSL Line	109
Table 32 Firmware Upgrade	110
Table 33 Backup Configuration	112
Table 34 Maintenance Restore Configuration	113
Table 35 Hardware Features	121
Table 36 Firmware Specifications	121
Table 37 Subnet Mask Example	142
Table 38 Subnet Masks	143

Table 39 Maximum Host Numbers	143
Table 40 Alternative Subnet Mask Notation	143
Table 41 Subnet 1	145
Table 42 Subnet 2	146
Table 43 Subnet 3	146
Table 44 Subnet 4	146
Table 45 Eight Subnets	146
Table 46 24-bit Network Number Subnet Planning	147
Table 47 16-bit Network Number Subnet Planning	147

PART I

Introduction

Introducing the ZyXEL Device (25)

Introducing the Web Configurator (29)

Introducing the ZyXEL Device

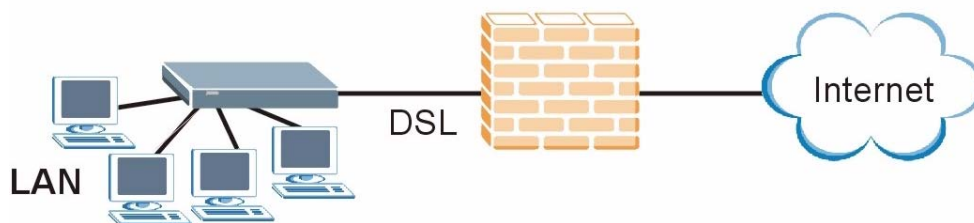
This chapter introduces the main applications and features of the ZyXEL Device. It also introduces the ways you can manage the ZyXEL Device.

1.1 Overview

Your ZyXEL Device integrates a high-speed 10/100Mbps auto-negotiating Ethernet LAN interface, a USB 1.1 LAN interface and a high-speed ADSL port into a single package. See [Appendix A on page 121](#) for a complete list of features.

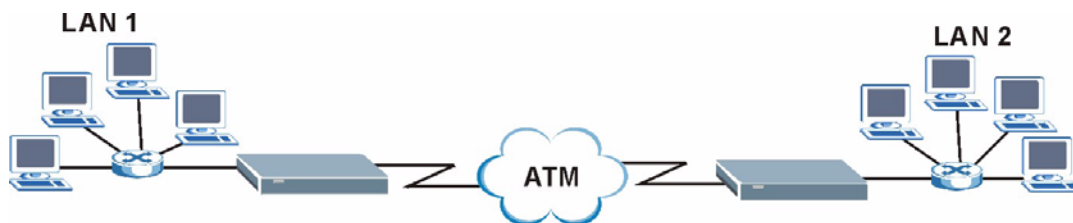
The ZyXEL Device is designed for high-speed Internet access at home. A typical Internet access application is shown below.

Figure 1 ZyXEL Device Internet Access Application



You can use the ZyXEL Device to connect two geographically dispersed networks over the ADSL line. A typical LAN-to-LAN application for your ZyXEL Device is shown as follows.

Figure 2 ZyXEL Device LAN-to-LAN Application



The ZyXEL Device is an ADSL router compatible with the ADSL/ADSL2/ADSL2+ standards. It allows super-fast, secure Internet access over the analog (POTS) or digital (ISDN) telephone line (depending on your model). Maximum data rates attainable for each standard are shown in the next table.

Table 1 ADSL Standards

DATA RATE STANDARD	UPSTREAM	DOWNSTREAM
ADSL	832 kbps	8Mbps
ADSL2	3.5Mbps	12Mbps
ADSL2+	3.5Mbps	24Mbps



If your ZyXEL Device does not support Annex M, the maximum ADSL2/2+ upstream data rate is 1.2 Mbps. ZyXEL Devices which work over ISDN do not support Annex M.



The standard your ISP supports determines the maximum upstream and downstream speeds attainable. Actual speeds attained also depend on the distance from your ISP, line quality, etc.

Models ending in "1", for example P-660RU-T1, denote a device that works over the analog telephone system, POTS (Plain Old Telephone Service). Models ending in "3" denote a device that works over ISDN (Integrated Synchronous Digital System). Models ending in "7" denote a device that works over T-ISDN (U-R2).

1.2 Ways to Manage the ZyXEL Device

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

- Web Configurator. This is recommended for everyday management of the ZyXEL Device using a (supported) web browser.
- Command Line Interface. Line commands are mostly used for troubleshooting by service engineers.
- FTP for firmware upgrades and configuration backup/restore.
- SNMP. The device can be monitored by an SNMP manager. See the SNMP chapter in this User's Guide.
- TR-069. TR-069 is a protocol that defines how your ZyXEL Device can be remotely managed via a management server.

1.3 Good Habits for Managing the ZyXEL Device

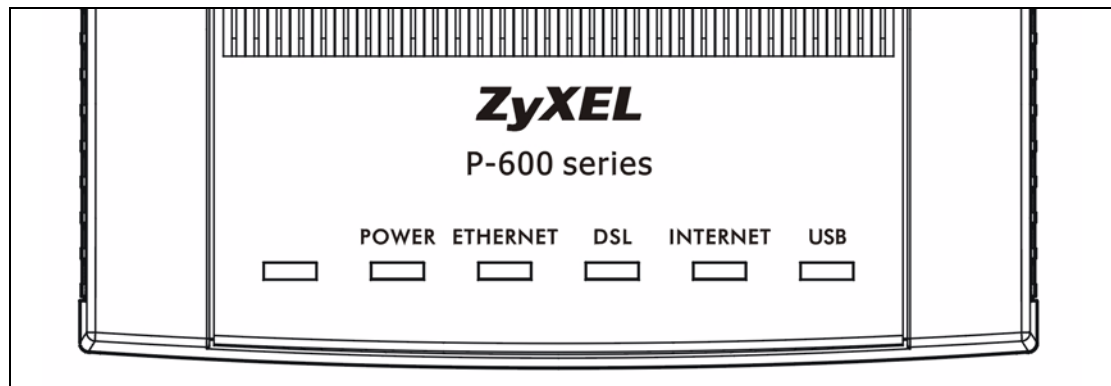
Do the following things regularly to make the ZyXEL Device more secure and to manage the ZyXEL Device more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes, or if you forget your password and have to reset the ZyXEL Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the ZyXEL Device. You could simply restore your last configuration.

1.4 ZyXEL Device Hardware Installation and Connection

Refer to the Quick Start Guide for information on hardware installation and connection.

1.5 LEDs



The following table describes the LEDs on the ZyXEL Device.

Table 2 LED Description

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The ZyXEL Device is receiving power and functioning properly.
		Blinking	The ZyXEL Device is rebooting.
	Red	On	The power to the ZyXEL Device is too low.
		Off	The ZyXEL Device is not ready or has malfunctioned.
ETHERNET	Green	On	The ZyXEL Device has a successful Ethernet connection.
		Blinking	The ZyXEL Device has a successful Ethernet connection and is receiving or sending data.
		Off	The ZyXEL Device does not have an Ethernet connection.

Table 2 LED Description

LED	COLOR	STATUS	DESCRIPTION
DSL	Green	On	The ZyXEL Device is linked successfully to a DSLAM.
		Blinking (Slow)	The ZyXEL Device is initializing the DSL line.
		Blinking (Fast)	The ZyXEL Device is sending or receiving non-PPP traffic.
		Off	The ZyXEL Device does not have a DSL link.
INTERNET	Amber	On	The ZyXEL Device has a PPP (PPPoA or PPPoE) connection.
		Blinking	The ZyXEL Device is sending or receiving PPPoA or PPPoE traffic.
		Off	The ZyXEL Device does not have a PPP (PPPoA or PPPoE) connection.
USB	Green	On	The ZyXEL Device has a successful USB connection.
		Blinking	The ZyXEL Device has a successful USB connection and is sending or receiving traffic.
		Off	The ZyXEL Device does not have a USB connection.

Introducing the Web Configurator

This chapter describes how to access and navigate the web configurator.

2.1 Web Configurator Overview

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

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

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

2.1.1 Accessing the ZyXEL Device Web Configurator

- 1 Make sure your ZyXEL Device hardware is properly connected (refer to the Quick Start Guide).
- 2 Prepare your computer or computer network to connect to the ZyXEL Device (refer to [Appendix B on page 125](#)).
- 3 Launch your web browser.
- 4 Type "192.168.1.1" as the URL.
- 5 An **Enter Network Password** window displays. Enter the password ("1234" is the default). Click **Login** to proceed to a screen asking you to change your password. Click **Cancel** to revert to the default password in the password field.

Figure 3 Password Screen

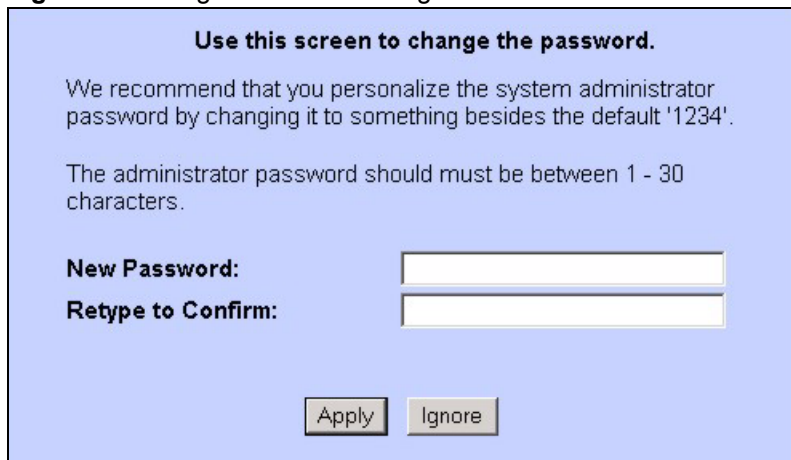


- 6** It is highly recommended you change the default password! Enter a new password, retype it to confirm and click **Apply**; alternatively click **Ignore** to proceed to the main menu if you do not want to change the password now.



If you do not change the password, the following screen appears every time you log in.

Figure 4 Change Password at Login



- 7** The **SITE MAP** screen displays.



The ZyXEL Device automatically times out after five minutes of inactivity. Simply log back into the ZyXEL Device if this happens.

2.2 Resetting the ZyXEL Device

Reset the ZyXEL Device in the following situations:

- You forgot your password.
- You cannot access the ZyXEL Device using the web configurator. Check **Troubleshooting** in the **Quick Start Guide** to make sure you cannot access the device anymore.

If you reset the ZyXEL Device, you lose all of the changes you have made. The ZyXEL Device re-loads its default settings, and the password resets to “1234”. You have to make all of your changes again.

Note: You will lose all of your changes when you push the **RESET** button.

To reset the ZyXEL Device,

- 1** Make sure the **POWER LED** is on and not blinking.
- 2** Press and hold the **RESET** button for five to ten seconds. Release the **RESET** button when the **POWER LED** begins to blink. The default settings have been restored.

If the ZyXEL Device restarts automatically, wait for the ZyXEL Device to finish restarting, and log in to the web configurator. The password is “1234”. You have finished.

If the ZyXEL Device does not restart automatically, disconnect and reconnect the ZyXEL Device’s power. Then, follow the directions above again.

2.3 Navigating the ZyXEL Device Web Configurator

The following summarizes how to navigate the web configurator from the **SITE MAP** screen.

- Click **Wizard Setup** to begin a series of screens to configure your ZyXEL Device for the first time.
- Click a link under **Advanced Setup** to configure advanced ZyXEL Device features.
- Click a link under **Maintenance** to see ZyXEL Device performance statistics, upload firmware and back up, restore or upload a configuration file.
- Click **SITE MAP** to go to the **Site Map** screen.
- Click Logout in the navigation panel when you have finished a ZyXEL Device management session.

2.4 The Site Map Screen

Figure 5 Web Configurator: Site Map Screen



Click the **HELP** icon (located in the top right corner of most screens) to view embedded help.

The following table describes the labels in this screen.

Table 3 Web Configurator Screens Summary

LINK	SUB-LINK	FUNCTION
Wizard Setup	Connection Setup	Use these screens for initial configuration including ISP parameters for Internet Access and WAN IP / DHCP server address assignment.
Advanced Setup		
Password		Use this screen to change your password.
LAN		Use this screen to configure LAN DHCP and TCP/IP settings.
WAN	WAN Setup	Use this screen to change the ZyXEL Device's WAN remote node settings.
	WAN Backup	Use this screen to configure your traffic redirect properties and WAN backup settings.
NAT	SUA Only	Use this screen to configure servers behind the ZyXEL Device.
	Full Feature	Use this screen to configure network address translation mapping rules.
Security		Use this screen to configure Internet security and apply the predefined filter rules.
Dynamic DNS		Use this screen to set up dynamic DNS.
Time and Date		Use this screen to change your ZyXEL Device's time and date.
Remote Management		Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet/FTP/Web to manage the ZyXEL Device.
UPnP		Use this screen to enable UPnP on the ZyXEL Device.
Maintenance		
System Status		This screen contains administrative and system-related information and is read-only.
DHCP Table		This screen displays DHCP (Dynamic Host Configuration Protocol) related information and is read-only.

Table 3 Web Configurator Screens Summary (continued)

LINK	SUB-LINK	FUNCTION
Any IP Table		This screen displays current read-only information of all network devices that use the Any IP feature to communicate with the ZyXEL Device.
Diagnostic	General	These screens display information to help you identify problems with the ZyXEL Device general connection.
	DSL Line	These screens display information to help you identify problems with the DSL line.
Firmware		Use this screen to upload firmware to your ZyXEL Device.
Configuration		Use these screens to backup, restore or reset the configuration of your ZyXEL Device.
LOGOUT		Click this label to exit the web configurator.

PART II

Wizard

Wizard Setup (37)

Wizard Setup

This chapter provides information on the Wizard Setup screens for Internet access in the web configurator.

3.1 Introduction

Use the **Wizard Setup** screens to configure your system for Internet access with the information provided by your ISP. Your ISP may have already configured some of the fields in the wizard screens for you.

3.1.1 Encapsulation

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

3.1.1.1 ENET ENCAP

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

3.1.1.2 PPP over Ethernet

PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP. The ZyXEL Device bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your computer to an ATM PVC (Permanent Virtual Circuit) which connects to ADSL Access Concentrator where the PPP session terminates. One PVC can support any number of PPP sessions from your LAN. For more information on PPPoE, see the appendices.

3.1.1.3 PPPoA

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

3.1.1.4 RFC 1483

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

3.1.2 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.

3.1.2.1 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.

3.1.2.2 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.

3.1.3 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.

3.1.4 Internet Access Wizard Setup: First Screen

In the **SITE MAP** screen click **Wizard Setup** to display the first wizard screen.

Figure 6 Internet Access Wizard Setup: First Screen

The following table describes the labels in this screen.

Table 4 Internet Access Wizard Setup: First Screen

LABEL	DESCRIPTION
Mode	From the Mode drop-down list box, select Routing (default) if your ISP allows multiple computers to share an Internet account. Otherwise select Bridge .
Encapsulation	Select the encapsulation type your ISP uses from the Encapsulation drop-down list box. Choices vary depending on what you select in the Mode field. If you select Bridge in the Mode field, select either PPPoA or RFC 1483 . If you select Routing in the Mode field, select PPPoA , RFC 1483 , ENET ENCAP or PPPoE .
Multiplex	Select the multiplexing method used by your ISP from the Multiplex drop-down list box either VC-based or LLC-based.
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.
VPI	Enter the VPI assigned to you. This field may already be configured.
VCI	Enter the VCI assigned to you. This field may already be configured.
Next	Click this button to go to the next wizard screen. The next wizard screen you see depends on what protocol you chose above. Click on the protocol link to see the next wizard screen for that protocol.

3.2 IP Address and Subnet Mask

See [Appendix C on page 141](#) for background information on IP addresses and subnetting.

3.2.1 IP Address Assignment

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

3.2.1.1 IP Assignment with PPPoA or PPPoE Encapsulation

If you have a dynamic IP, then the **IP Address** and **ENET ENCAP Gateway** 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 **ENET ENCAP Gateway** field.

3.2.1.2 IP Assignment with RFC 1483 Encapsulation

In this case the IP Address Assignment *must* be static with the same requirements for the **IP Address** and **ENET ENCAP Gateway** fields as stated above.

3.2.1.3 IP Assignment with ENET ENCAP Encapsulation

In this case you can have either a static or dynamic IP. For a static IP you must fill in all the **IP Address** and **ENET ENCAP Gateway** fields as supplied by your ISP. However for a dynamic IP, the ZyXEL Device acts as a DHCP client on the WAN port and so the **IP Address** and **ENET ENCAP Gateway** fields are not applicable (N/A) as the DHCP server assigns them to the ZyXEL Device.

3.2.1.4 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.



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*.

3.2.2 Nailed-Up Connection (PPP)

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

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

3.2.3 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.

3.2.4 Internet Access Wizard Setup: Second Screen

The second wizard screen varies depending on what mode and encapsulation type you use. All screens shown are with routing mode. Configure the fields and click **Next** to continue.

Figure 7 Internet Connection with PPPoE

The following table describes the labels in this screen.

Table 5 Internet Connection with PPPoE

LABEL	DESCRIPTION
Service Name	Type the name of your PPPoE service here.
User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
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 Obtain an IP Address Automatically if you have a dynamic IP address; otherwise select Static IP Address and type your ISP assigned IP address in the text box below.

Table 5 Internet Connection with PPPoE (continued)

LABEL	DESCRIPTION
Connection	Select Connect on Demand when you don't want the connection up all the time and specify an idle time-out (in seconds) in the Max. Idle Timeout field. The default setting selects Connection on Demand with 0 as the idle time-out, which means the Internet session will not timeout. Select Nailed-Up Connection when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
Network Address Translation	Select None , SUA Only or Full Feature from the drop-down list box. Refer to the NAT chapter for more details.
Back	Click Back to go back to the first wizard screen.
Next	Click Next to continue to the next wizard screen.

Figure 8 Internet Connection with RFC 1483

Connection Setup- ISP Parameters for Internet Access

IP Address

Network Address Translation
 ▾

The following table describes the labels in this screen.

Table 6 Internet Connection with RFC 1483

LABEL	DESCRIPTION
IP Address	This field is available if you select Routing in the Mode field. Type your ISP assigned IP address in this field.
Network Address Translation	Select None , SUA Only or Full Feature from the drop-down list box. Refer to Chapter 12 on page 91 for more details.
Back	Click Back to go back to the first wizard screen.
Next	Click Next to continue to the next wizard screen.

Figure 9 Internet Connection with ENET ENCAP

Connection Setup- ISP Parameters for Internet Access

IP Address

Obtain an IP Address Automatically

Static IP Address

IP Address

Subnet Mask

ENET ENCAP Gateway

Network Address Translation

The following table describes the labels in this screen.

Table 7 Internet Connection with ENET ENCAP

LABEL	DESCRIPTION
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 Obtain an IP Address Automatically if you have a dynamic IP address; otherwise select Static IP Address and type your ISP assigned IP address in the IP Address text box below.
Subnet Mask	Enter a subnet mask in dotted decimal notation. Refer to Appendix C on page 141 to calculate a subnet mask If you are implementing subnetting.
ENET ENCAP Gateway	You must specify a gateway IP address (supplied by your ISP) when you use ENET ENCAP in the Encapsulation field in the previous screen.
Network Address Translation	Select None , SUA Only or Full Feature from the drop-down list box. Refer to the NAT chapter for more details.
Back	Click Back to go back to the first wizard screen.
Next	Click Next to continue to the next wizard screen.

Figure 10 Internet Connection with PPPoA

Connection Setup- ISP Parameters for Internet Access

User Name

Password

IP Address

Obtain an IP Address Automatically

Static IP Address

Connection

Connect on Demand: Max Idle Timeout sec

Nailed-Up Connection

Network Address Translation

▼

The following table describes the labels in this screen.

Table 8 Internet Connection with PPPoA

LABEL	DESCRIPTION
User Name	Enter the login name that your ISP gives you.
Password	Enter the password associated with the user name above.
IP Address	This option is available if you select Routing in the Mode field. 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. Click Obtain an IP Address Automatically if you have a dynamic IP address; otherwise click Static IP Address and type your ISP assigned IP address in the IP Address text box below.
Connection	Select Connect on Demand when you don't want the connection up all the time and specify an idle time-out (in seconds) in the Max. Idle Timeout field. The default setting selects Connection on Demand with 0 as the idle time-out, which means the Internet session will not timeout. Select Nailed-Up Connection when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
Network Address Translation	This option is available if you select Routing in the Mode field. Select None , SUA Only or Full Feature from the drop-down list box. Refer to Chapter 12 on page 91 for more details.
Back	Click Back to go back to the first wizard screen.
Next	Click Next to continue to the next wizard screen.

3.2.5 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.

3.2.5.1 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.

3.2.6 Internet Access Wizard Setup: Third Screen

Verify the settings in the screen shown next.

Figure 11 Internet Access Wizard Setup: Third Screen

Wizard Setup - ISP Parameters for Internet Access

WAN Information:
 Mode: **Routing**
 Encapsulation: **PPPoE**
 Multiplexing: **LLC**
 VPI/VCI: **8/35**
 Service Name :
 User Name : **user@icp.ch**
 Password : *********
 IP Address : **Obtain an IP Address Automatically**
 Network Address Translation: **SUA Only**
 Connect on Demand: **Max Idle Timeout 0 sec.**

LAN Information:
 IP Address: **192.168.1.1**
 IP Mask: **255.255.255.0**
 DHCP: **ON**
 Client IP Pool Starting Address: **192.168.1.33**
 Size of Client IP Pool: **32**

If you want to change your ZyXEL Device LAN settings, click **Change LAN Configuration** to display the screen shown next. Otherwise, click **Log on to the Internet!** to save the configuration. Skip to [Section 3.2.7 on page 46](#).

Figure 12 Internet Access Wizard Setup: LAN Configuration

Connection Setup- ISP Parameters for Internet Access

LAN IP Address: 192.168.1.1

LAN Subnet Mask: 255.255.255.0

DHCP

DHCP Server: ON

Client IP Pool Starting Address: 192.168.1.33

Size of Client IP Pool: 32

Primary DNS Server: 0.0.0.0

Secondary DNS Server: 0.0.0.0

Back Finish

The following table describes the labels in this screen.

Table 9 Internet Access Wizard Setup: LAN Configuration

LABEL	DESCRIPTION
LAN IP Address	Enter the IP address of your ZyXEL Device in dotted decimal notation, for example, 192.168.1.1 (factory default). Note: If you changed the ZyXEL Device's LAN IP address, you must use the new IP address if you want to access the web configurator again.
LAN Subnet Mask	Enter a subnet mask in dotted decimal notation.
DHCP	
DHCP Server	From the DHCP Server drop-down list box, select On to allow your ZyXEL Device to assign IP addresses, an IP default gateway and DNS servers to computer systems that support the DHCP client. Select Off to disable DHCP server. When DHCP server is used, set the following items:
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	This field specifies the size or count of the IP address pool.
Primary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Secondary DNS Server	As above.
Back	Click Back to go back to the previous screen.
Finish	Click Finish to save the settings and proceed to the next wizard screen.

3.2.7 Internet Access Wizard Setup: Connection Test

The ZyXEL Device automatically tests the connection to the computer(s) connected to the LAN ports. To test the connection from the ZyXEL Device to the ISP, click **Start Diagnose**. Otherwise click **Return to Main Menu** to go back to the **Site Map** screen.

Figure 13 Internet Access Wizard Setup: Connection Tests

Wizard Setup - ISP Parameters for Internet Access

Your DSL Gateway is now configured. Your device is capable of testing your DSL service. The individual tests are listed below. Click "Start Diagnose" button if you want to test; otherwise, click "Return to Main Menu" button.

LAN connections	
Test your Ethernet Connection	PASS
WAN connections	
Test ADSL synchronization	PASS
Test ADSL(ATM OAM) loopback test	PASS
Test PPP/PPPoE server connection	PASS
Ping default gateway	PASS

Start Diagnose Return to Main Menu

3.2.7.1 Test Your Internet Connection

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

PART III

Advanced

- Password Setup (51)
- LAN Setup (53)
- WAN Setup (59)
- Security (69)
- Dynamic DNS Setup (71)
- Time and Date (73)
- Remote Management Configuration (75)
- Universal Plug-and-Play (UPnP) (79)
- Network Address Translation (NAT) Screens (91)

Password Setup

This chapter provides information on the **Password** screen.

4.1 Password Overview

It is strongly recommended that you change the password for accessing the ZyXEL Device.

4.1.1 Configuring Password

To change your ZyXEL Device's password (recommended), click **Password** in the **Site Map** screen. The screen appears as shown.

Figure 14 Password

The following table describes the labels in this screen.

Table 10 Password

LABEL	DESCRIPTION
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type the new password in this field.
Retype to Confirm	Type the new password again in this field.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

LAN Setup

This chapter describes how to configure LAN settings.

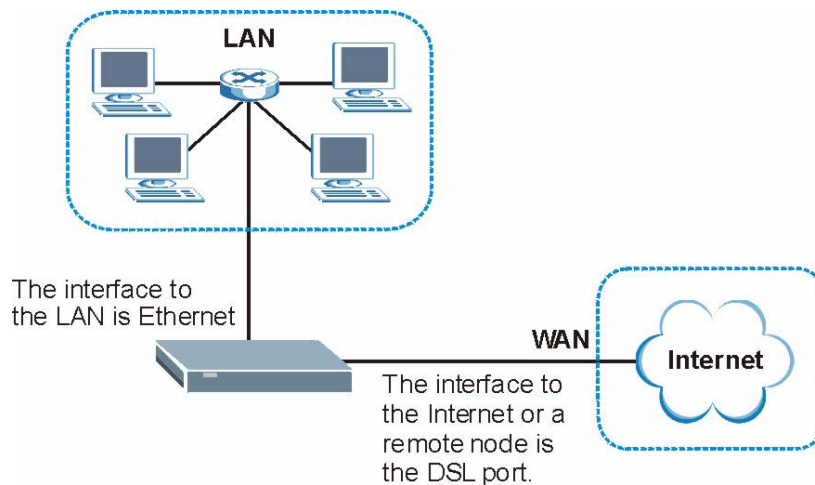
5.1 LAN Overview

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

5.1.1 LANs, WANs and the ZyXEL Device

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

Figure 15 LAN and WAN IP Addresses



5.2 DNS Server Addresses

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

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

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

The ZyXEL Device acts as a DNS proxy when the **Primary** and **Secondary DNS Server** fields are left blank in the **LAN Setup** screen.

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

5.3 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.

5.3.1 Factory LAN Defaults

The LAN parameters of the ZyXEL Device are preset in the factory with the following values:

- IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), read the embedded web configurator help regarding what fields need to be configured.

5.3.2 IP Address and Subnet Mask

Refer to [Section 3.2 on page 39](#) for this information.

5.3.3 RIP Setup

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

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

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

Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting.

5.3.4 Multicast

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

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The ZyXEL Device supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the ZyXEL Device queries all directly connected networks to gather group membership. After that, the ZyXEL Device periodically updates this information. IP multicasting can be enabled/disabled on the ZyXEL Device LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

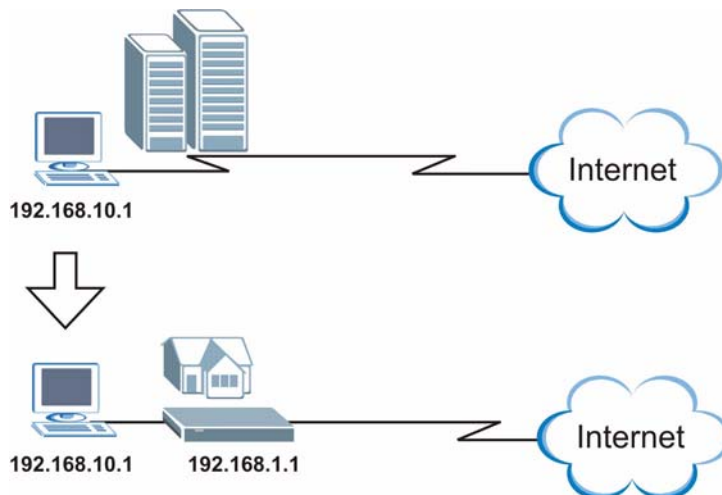
5.4 Any IP

Traditionally, you must set the IP addresses and the subnet masks of a computer and the ZyXEL Device to be in the same subnet to allow the computer to access the Internet (through the ZyXEL Device). In cases where your computer is required to use a static IP address in another network, you may need to manually configure the network settings of the computer every time you want to access the Internet via the ZyXEL Device.

With the Any IP feature and NAT enabled, the ZyXEL Device allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, when the IP addresses of the computer and the ZyXEL Device are not in the same subnet. Whether a computer is set to use a dynamic or static (fixed) IP address, you can simply connect the computer to the ZyXEL Device and access the Internet.

The following figure depicts a scenario where a computer is set to use a static private IP address in the corporate environment. In a residential house where a ZyXEL Device is installed, you can still use the computer to access the Internet without changing the network settings, even when the IP addresses of the computer and the ZyXEL Device are not in the same subnet.

Figure 16 Any IP Example



The Any IP feature does not apply to a computer using either a dynamic IP address or a static IP address that is in the same subnet as the ZyXEL Device's IP address.



You *must* enable NAT/SUA to use the Any IP feature on the ZyXEL Device.

5.4.1 How Any IP Works

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network. IP routing table is defined on IP Ethernet devices (the ZyXEL Device) to decide which hop to use, to help forward data along to its specified destination.

The following lists out the steps taken, when a computer tries to access the Internet for the first time through the ZyXEL Device.

- 1 When a computer (which is in a different subnet) first attempts to access the Internet, it sends packets to its default gateway (which is not the ZyXEL Device) by looking at the MAC address in its ARP table.
- 2 When the computer cannot locate the default gateway, an ARP request is broadcast on the LAN.
- 3 The ZyXEL Device receives the ARP request and replies to the computer with its own MAC address.
- 4 The computer updates the MAC address for the default gateway to the ARP table. Once the ARP table is updated, the computer is able to access the Internet through the ZyXEL Device.
- 5 When the ZyXEL Device receives packets from the computer, it creates an entry in the IP routing table so it can properly forward packets intended for the computer.

After all the routing information is updated, the computer can access the ZyXEL Device and the Internet as if it is in the same subnet as the ZyXEL Device.

5.5 Configuring the LAN

Click LAN to open the following screen.

Figure 17 LAN Setup

LAN - LAN Setup

DHCP

DHCP	Server ▾
Client IP Pool Starting Address	192.168.1.33
Size of Client IP Pool	32
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Remote DHCP Server	N/A

TCP/IP

IP Address	192.168.1.1
IP Subnet Mask	255.255.255.0
RIP Direction	Both ▾
RIP Version	RIP-2B ▾
Multicast	None ▾

Any IP Setup

Active

The following table describes the labels in this screen.

Table 11 LAN Setup

LABEL	DESCRIPTION
DHCP	
DHCP	<p>If set to Server, your ZyXEL Device can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client.</p> <p>If set to None, the DHCP server will be disabled.</p> <p>If set to Relay, the ZyXEL Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the Remote DHCP Server field in this case.</p> <p>When DHCP is used, the following items need to be set:</p>
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	This field specifies the size or count of the IP address pool.
Primary / Secondary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Remote DHCP Server	If Relay is selected in the DHCP field above then enter the IP address of the actual remote DHCP server here.
TCP/IP	
IP Address	Enter the IP address of your ZyXEL Device in dotted decimal notation, for example, 192.168.1.1 (factory default).
IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
RIP Direction	<p>RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. Use this field to control how much routing information the ZyXEL Device sends and receives on the subnet.</p> <p>Select the RIP direction from None, Both, In Only and Out Only.</p>
RIP Version	Select the RIP version from RIP-1 , RIP-2B and RIP-2M .
Multicast	<p>Select which version of IGMP the ZyXEL Device uses to support multicasting on the LAN. Multicast packets are sent to a group of computers on the LAN and are an alternative to unicast packets (packets sent to one computer) and broadcast packets (packets sent to every computer).</p> <p>IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports both IGMP version 1 (IGMP-v1) and IGMP-v2. Select None to disable it.</p>
Any IP Setup	<p>Select the Active checkbox to enable the Any IP feature. This allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, even when the IP addresses of the computer and the ZyXEL Device are not in the same subnet.</p> <p>When you disable the Any IP feature, only computers with dynamic IP addresses or static IP addresses in the same subnet as the ZyXEL Device's LAN IP address can connect to the ZyXEL Device or access the Internet through the ZyXEL Device.</p>
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring this screen afresh.

WAN Setup

This chapter describes how to configure WAN settings.

6.1 WAN Overview

A WAN (Wide Area Network) is an outside connection to another network or the Internet. See [Section on page 31](#) for more information on the fields in the WAN screens.

6.2 Metric

The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".

The metric sets the priority for the ZyXEL Device's routes to the Internet. If any two of the default routes have the same metric, the ZyXEL Device uses the following pre-defined priorities:

- Normal route: designated by the ISP (see [Section 6.5 on page 61](#))
- Traffic-redirect route (see [Section 6.7 on page 64](#))
- WAN-backup route, also called dial-backup (see [Section 6.8 on page 65](#))

For example, if the normal route has a metric of "1" and the traffic-redirect route has a metric of "2" and dial-backup route has a metric of "3", then the normal route acts as the primary default route. If the normal route fails to connect to the Internet, the ZyXEL Device tries the traffic-redirect route next. In the same manner, the ZyXEL Device uses the dial-backup route if the traffic-redirect route also fails.

If you want the dial-backup route to take first priority over the traffic-redirect route or even the normal route, all you need to do is set the dial-backup route's metric to "1" and the others to "2" (or greater).



IP Policy Routing overrides the default routing behavior and takes priority over all of the routes mentioned above.

6.3 PPPoE Encapsulation

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

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

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

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

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

6.4 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.

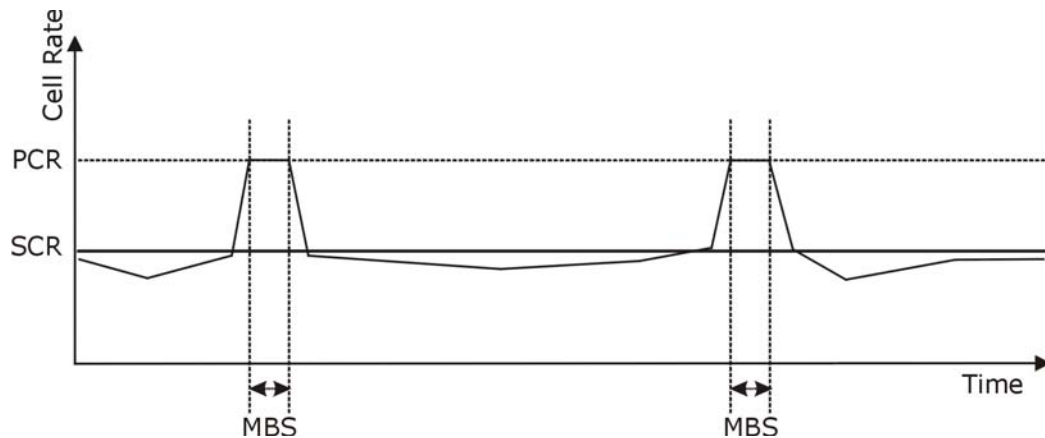
Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent 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 18 Example of Traffic Shaping

6.5 Zero Configuration Internet Access

Once you turn on and connect the ZyXEL Device to a telephone jack, it automatically detects the Internet connection settings (such as the VCI/VPI numbers and the encapsulation method) from the ISP and makes the necessary configuration changes. In cases where additional account information (such as an Internet account user name and password) is required or the ZyXEL Device cannot connect to the ISP, you will be redirected to web screen(s) for information input or troubleshooting.

Zero configuration for Internet access is disable when

- the ZyXEL Device is in bridge mode
- you set the ZyXEL Device to use a static (fixed) WAN IP address.

6.6 Configuring WAN Setup

To change your ZyXEL Device's WAN remote node settings, click **WAN > WAN Setup**. The screen differs by the encapsulation you select.

Figure 19 WAN Setup (PPPoE)

WAN - WAN Setup

Name

Mode

Encapsulation

Multiplex

Virtual Circuit ID

VPI

VCI

ATM QoS Type

Cell Rate

Peak Cell Rate cell/sec

Sustain Cell Rate cell/sec

Maximum Burst Size

Login Information

Service Name

User Name

Password

IP Address

Obtain an IP Address Automatically

Static IP Address

IP Address

Connection

Nailed-Up Connection

Connect on Demand

Max Idle Timeout sec

PPPoE Pass Through

Zero Configuration

The following table describes the labels in this screen.

Table 12 WAN Setup

LABEL	DESCRIPTION
Name	Enter the name of your Internet Service Provider, for example "MyISP". This information is for identification purposes only.
Mode	Select Routing (default) from the drop-down list box if your ISP allows multiple computers to share an Internet account. Otherwise select Bridge .
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the Mode field. If you select Bridge in the Mode field, select either PPPoA or RFC 1483 . If you select Routing in the Mode field, select PPPoA , RFC 1483 , ENET ENCAP or PPPoE .

Table 12 WAN Setup (continued)

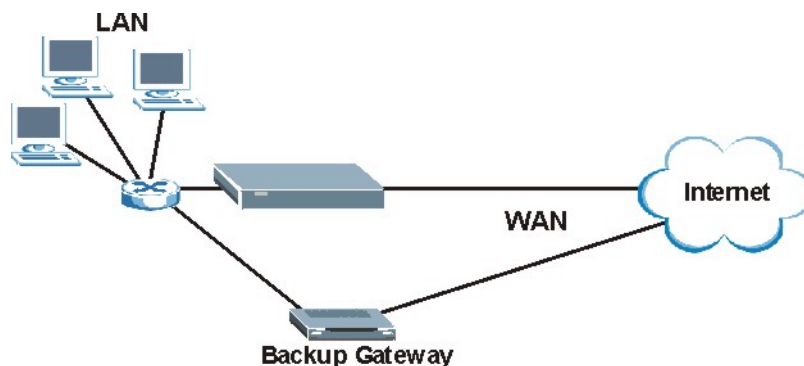
LABEL	DESCRIPTION
Multiplex	Select the method of multiplexing used by your ISP from the drop-down list. Choices are VC or LLC .
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
ATM QoS Type	Select CBR (Constant Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select UBR (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select VBR (Variable Bit Rate) for bursty traffic and bandwidth sharing with other applications.
Cell Rate	Cell rate configuration often helps eliminate traffic congestion that slows transmission of real time data such as audio and video connections.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustain Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
Login Information	(PPPoA and PPPoE encapsulation only)
Service Name	(PPPoE only) Type the name of your PPPoE service here.
User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
IP Address	This option is available if you select Routing in the Mode field. A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select Obtain an IP Address Automatically if you have a dynamic IP address; otherwise select Static IP Address and type your ISP assigned IP address in the IP Address field below.
Connection (PPPoA and PPPoE encapsulation only)	
Nailed-Up Connection	Select Nailed-Up Connection when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select Connect on Demand when you don't want the connection up all the time and specify an idle time-out in the Max Idle Timeout field.
Max Idle Timeout	Specify an idle time-out in the Max Idle Timeout field when you select Connect on Demand . The default setting is 0, which means the Internet session will not timeout.

Table 12 WAN Setup (continued)

LABEL	DESCRIPTION
PPPoE Passthrough (PPPoE encapsulation only)	This field is available when you select PPPoE encapsulation. 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.
Subnet Mask (ENET ENCAP encapsulation only)	Enter a subnet mask in dotted decimal notation. Refer to Appendix C on page 141 to calculate a subnet mask If you are implementing subnetting.
ENET ENCAP Gateway (ENET ENCAP encapsulation only)	You must specify a gateway IP address (supplied by your ISP) when you select ENET ENCAP in the Encapsulation field
Zero Configuration	This feature is not applicable/available when you configure the ZyXEL Device to use a static WAN IP address or in bridge mode. Select Yes to set the ZyXEL Device to automatically detect the Internet connection settings (such as the VCI/VPI numbers and the encapsulation method) from the ISP and make the necessary configuration changes. Select No to disable this feature. You must manually configure the ZyXEL Device for Internet access.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to begin configuring this screen afresh.

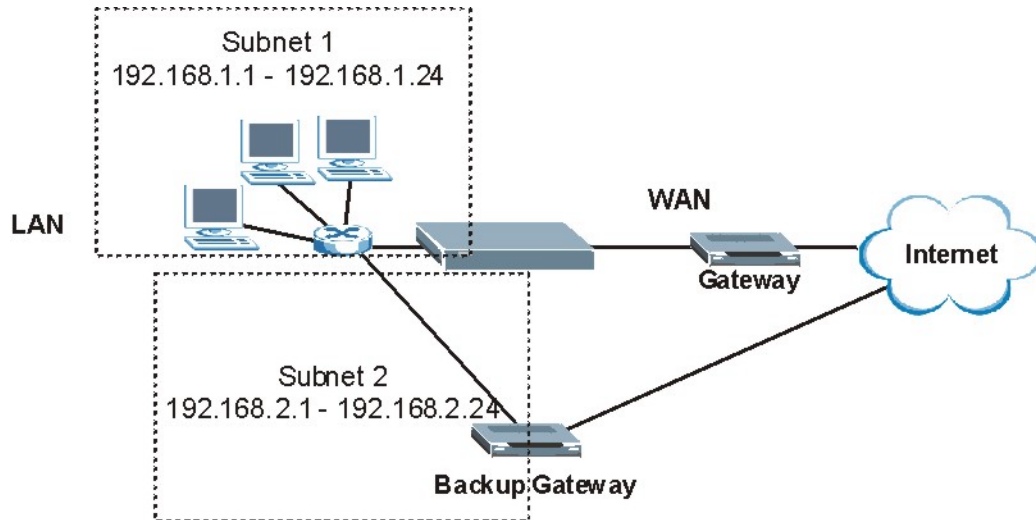
6.7 Traffic Redirect

Traffic redirect forwards traffic to a backup gateway when the ZyXEL Device cannot connect to the Internet. An example is shown in the figure below.

Figure 20 Traffic Redirect Example

The following network topology allows you to avoid triangle route security issues when the backup gateway is connected to the LAN. Use IP alias to configure the LAN into two or three logical networks with the ZyXEL Device itself as the gateway for each LAN network. Put the protected LAN in one subnet (Subnet 1 in the following figure) and the backup gateway in another subnet (Subnet 2). Configure filters that allow packets from the protected LAN (Subnet 1) to the backup gateway (Subnet 2).

Figure 21 Traffic Redirect LAN Setup



6.8 Configuring WAN Backup

To change your ZyXEL Device's WAN backup settings, click **WAN > WAN Backup**. The screen appears as shown.

Figure 22 WAN Backup

The following table describes the labels in this screen.

Table 13 WAN Backup

LABEL	DESCRIPTION
Backup Type	Select the method that the ZyXEL Device uses to check the DSL connection. Select DSL Link to have the ZyXEL Device check if the connection to the DSLAM is up. Select ICMP to have the ZyXEL Device periodically ping the IP addresses configured in the Check WAN IP Address fields.
Check WAN IP Address1-3	Configure this field to test your ZyXEL Device's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address). Note: If you activate either traffic redirect or dial backup, you must configure at least one IP address here. When using a WAN backup connection, the ZyXEL Device periodically pings the addresses configured here and uses the other WAN backup connection (if configured) if there is no response.
Fail Tolerance	Type the number of times (2 recommended) that your ZyXEL Device may ping the IP addresses configured in the Check WAN IP Address field without getting a response before switching to a WAN backup connection (or a different WAN backup connection).
Recovery Interval	When the ZyXEL Device is using a lower priority connection (usually a WAN backup connection), it periodically checks to whether or not it can use a higher priority connection. Type the number of seconds (30 recommended) for the ZyXEL Device to wait between checks. Allow more time if your destination IP address handles lots of traffic.

Table 13 WAN Backup (continued)

LABEL	DESCRIPTION
Timeout	Type the number of seconds (3 recommended) for your ZyXEL Device to wait for a ping response from one of the IP addresses in the Check WAN IP Address field before timing out the request. The WAN connection is considered "down" after the ZyXEL Device times out the number of times specified in the Fail Tolerance field. Use a higher value in this field if your network is busy or congested.
Traffic Redirect	
Active	Select this check box to have the ZyXEL Device use traffic redirect if the normal WAN connection goes down. Note: If you activate traffic redirect, you must configure at least one Check WAN IP Address.
Metric	This field sets this route's priority among the routes the ZyXEL Device uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
Backup Gateway	Type the IP address of your backup gateway in dotted decimal notation. The ZyXEL Device automatically forwards traffic to this IP address if the ZyXEL Device's Internet connection terminates.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to begin configuring this screen afresh.

Security

This chapter shows how to configure Internet security filters on your ZyXEL Device.

7.1 Configuring Internet Security

The ZyXEL Device can use predefined filters to stop packets of specified types from passing from the WAN to the LAN, or from the LAN to the WAN.



If you want to enable remote management of the ZyXEL Device from the WAN, ensure that the settings in this screen allow packets of the relevant type to pass from the WAN.

Click **Security** in the navigation panel to open the following screen.

Figure 23 Internet Security

Internet Security

Your device provides the following filter rules

<input type="checkbox"/> Telnet	Telnet traffic is blocked from the WAN to the LAN
<input type="checkbox"/> FTP	FTP traffic is blocked from the WAN to the LAN
<input type="checkbox"/> TFTP	TFTP traffic is blocked from the WAN to the LAN
<input type="checkbox"/> Web	Web traffic is blocked from the WAN to the LAN
<input type="checkbox"/> SNMP	SNMP traffic is blocked from the WAN
<input type="checkbox"/> Ping.	Ping traffic is blocked from the WAN/LAN

The following table describes the labels in this screen.

Table 14 Internet Security

LABEL	DESCRIPTION
Telnet	Select this to stop all telnet packets passing from the WAN to the LAN. Telnet traffic from the LAN can still pass through to the WAN.
FTP	Select this to stop all FTP traffic passing from the WAN to the LAN. FTP traffic from the LAN can still pass through to the WAN.
TFTP	Select this to stop all TFTP traffic passing from the WAN to the LAN. TFTP traffic from the LAN can still pass through to the WAN.
Web	Select this to stop all HTTP traffic passing from the WAN to the LAN.
SNMP	Select this to stop all SNMP traffic passing from the WAN to the ZyXEL Device. SNMP traffic from the LAN can still access the ZyXEL Device.
Ping	Select this to stop all ICMP Echo traffic passing from the WAN to the LAN, and from the LAN to the WAN. You can still ping devices on the LAN.
Apply	Click this button to save the settings in this screen.
Cancel	Click this button to return the fields in this screen to their previously-saved values.

Dynamic DNS Setup

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

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

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

8.1.1 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.

8.2 Configuring Dynamic DNS

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

Figure 24 Dynamic DNS

Dynamic DNS

Active

Service Provider: WWW.DynDNS.ORG

Host Name:

E-mail Address:

User:

Password:

Enable Wildcard

Apply Cancel

The following table describes the labels in this screen.

Table 15 Dynamic DNS

LABEL	DESCRIPTION
Active	Select this check box to use dynamic DNS.
Service Provider	This is the name of your Dynamic DNS service provider.
Host Names	Type the domain name assigned to your ZyXEL Device by your Dynamic DNS provider.
E-mail Address	Type your e-mail address.
User	Type your user name.
Password	Type the password assigned to you.
Enable Wildcard	Select the check box to enable DYNDNS Wildcard.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

Time and Date

This screen is not available on all models. Use this screen to configure the ZyXEL Device's time and date settings.

9.1 Configuring Time and Date

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

Figure 25 Time and Date

Time and Date

Time Server

Use Protocol when Bootup

IP Address or URL

Time and Date

Daylight Savings

Start Date month day

End Date month day

Synchronize system clock with Time Server now.
(This may take up to 60 seconds.)

Date

Current Date

New Date (yyy-mm-dd)

Time

Current Time : :

New Time : :

The following table describes the labels in this screen.

Table 16 Time and Date

LABEL	DESCRIPTION
Time Server	
Use Protocol when Bootup	<p>Select the time service protocol that your time server uses. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works.</p> <p>The main difference between them is the format.</p> <p>When you select the Daytime (RFC 867) format, the switch displays the day, month, year and time with no time zone adjustment. When you use this format it is recommended that you use a Daytime timeserver within your geographical time zone.</p> <p>Time (RFC 868) format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.</p> <p>NTP (RFC 1305) is similar to Time (RFC 868).</p> <p>Select None to enter the time and date manually.</p>
IP Address or URL	Enter the IP address or URL of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time and Date	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Select this option if you use daylight savings time. 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.
Start Date	Enter the month and day that your daylight-savings time starts on if you selected Daylight Savings .
End Date	Enter the month and day that your daylight-savings time ends on if you selected Daylight Savings .
Synchronize system clock with Time Server now.	<p>Select this option to have your ZyXEL Device use the time server (that you configured above) to set its internal system clock.</p> <p>Please wait for up to 60 seconds while the ZyXEL Device locates the time server. If the ZyXEL Device cannot find the time server, please check the time server protocol and its IP address. If the IP address was entered correctly, try pinging it for example to test the connection.</p>
Date	
Current Date	<p>This field displays the date set on your ZyXEL Device.</p> <p>Each time you reload this page, the ZyXEL Device synchronizes the time with the time server.</p>
New Date (yyyy-mm-dd)	<p>This field displays the last updated date from the time server.</p> <p>When you select None in the Use Protocol when Bootup field, enter the new date in this field and then click Apply.</p>
Time	
Current Time	<p>This field displays the time set on your ZyXEL Device.</p> <p>Each time you reload this page, the ZyXEL Device synchronizes the time with the time server.</p>
New Time	<p>This field displays the last updated time from the time server.</p> <p>When you select None in the Use Protocol when Bootup field, enter the new time in this field and then click Apply.</p>
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

Remote Management Configuration

This chapter provides information on configuring remote management.

10.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which ZyXEL Device interface (if any) from which computers.

You may manage your ZyXEL Device from a remote location via:

- Internet (WAN only)
- ALL (LAN and WAN)
- LAN only,
- Neither (Disable).

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

You may only have one remote management session running at a time. The ZyXEL Device automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows.

- 1 Telnet
- 2 HTTP

10.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

- You have not enabled that service on the interface in the corresponding remote management screen.
- The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the ZyXEL Device will disconnect the session immediately.
- There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
- A filter is applied (in the **Security** screen) to block a Telnet, FTP or Web service.

10.1.2 Remote Management and NAT

When NAT is enabled:

- Use the ZyXEL Device's WAN IP address when configuring from the WAN.
- Use the ZyXEL Device's LAN IP address when configuring from the LAN.

10.1.3 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The ZyXEL Device automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

10.2 Telnet

You can use Telnet to access the ZyXEL Device's command line interface. Specify which interfaces allow Telnet access and from which IP address the access can come.

10.3 FTP

You can upload and download ZyXEL Device firmware and configuration files using FTP. To use this feature, your computer must have an FTP client.

10.4 Web

You can set the ZyXEL Device to use HTTP or HTTPS (HTTPS adds security) for web configurator sessions. Specify which interfaces allow web configurator access and from which IP address the access can come.

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

10.5 Configuring Remote Management

Click **Remote Management** to open the following screen.

Figure 26 Remote Management

Remote Management Control

Server Type	Access Status	Port	Secured Client IP
Telnet	All	23	0.0.0.0
FTP	All	21	0.0.0.0
Web	All	80	0.0.0.0

Apply Cancel

The following table describes the labels in this screen.

Table 17 Remote Management

LABEL	DESCRIPTION
Server Type	Each of these labels denotes a service that you may use to remotely manage the ZyXEL Device.
Access Status	Select the access interface. Choices are All , LAN Only , WAN Only and Disable .
Port	This field shows the port number for the remote management service. You may change the port number for a service in this field, but you must use the same port number to use that service for remote management.
Secured Client IP	The default 0.0.0.0 allows any client to use this service to remotely manage the ZyXEL Device. Type an IP address to restrict access to a client with a matching IP address.
Apply	Click Apply to save your settings back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

Universal Plug-and-Play (UPnP)

This chapter introduces the UPnP feature in the web configurator.

11.1 Introducing Universal Plug and Play (UPnP)

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 [Section 11.2.1 on page 80](#) for configuration instructions.

11.1.1 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.

11.1.2 NAT Traversal

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

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

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

See the NAT chapter for more information on NAT.

11.1.3 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.

11.2 UPnP and ZyXEL

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

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

11.2.1 Configuring UPnP

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

Figure 27 Configuring UPnP

The following table describes the labels in this screen.

Table 18 Configuring UPnP

LABEL	DESCRIPTION
Enable the Universal Plug and Play (UPnP) Service	Select this checkbox 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).
Allow users to make configuration changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the ZyXEL Device so that they can communicate through the ZyXEL Device, for example by using NAT traversal. UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.
Apply	Click Apply to save the setting to the ZyXEL Device.
Cancel	Click Cancel to return to the previously saved settings.

11.3 Installing UPnP in Windows

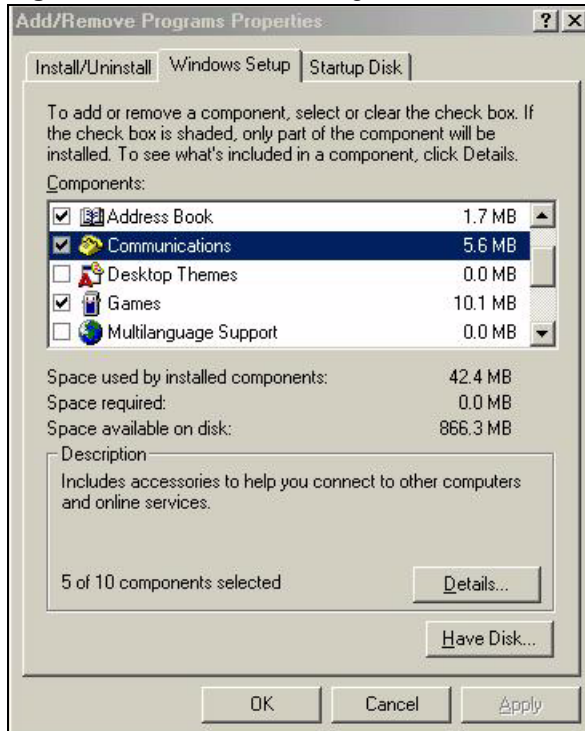
This section shows how to install UPnP in Windows Me and Windows XP.

11.3.1 Installing UPnP in Windows Me

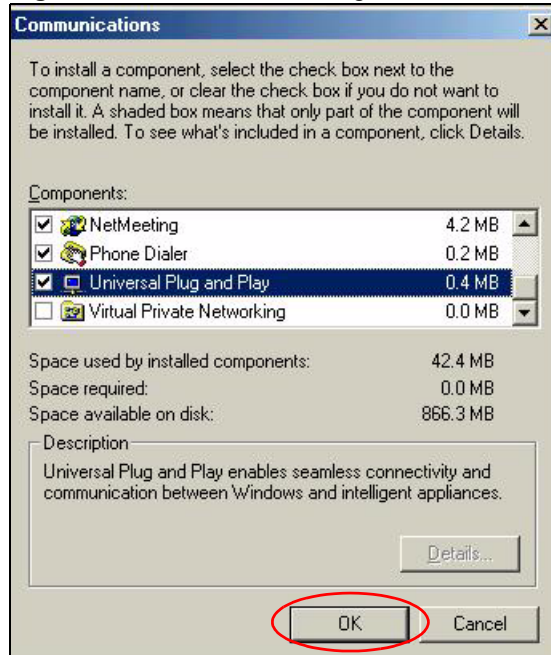
Follow the steps below to install the UPnP in Windows Me.

- 1 Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.
- 2 Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.

Figure 28 Add/Remove Programs: Windows Setup: Communication



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

Figure 29 Add/Remove Programs: Windows Setup: Communication: Components

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

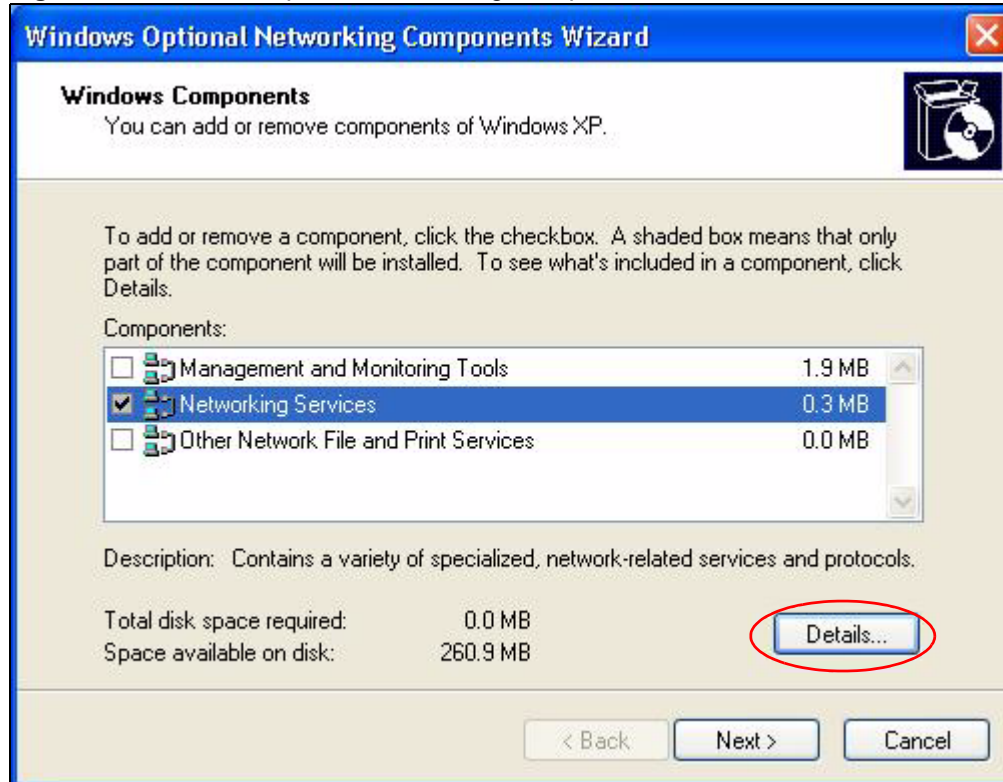
11.3.2 Installing UPnP in Windows XP

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

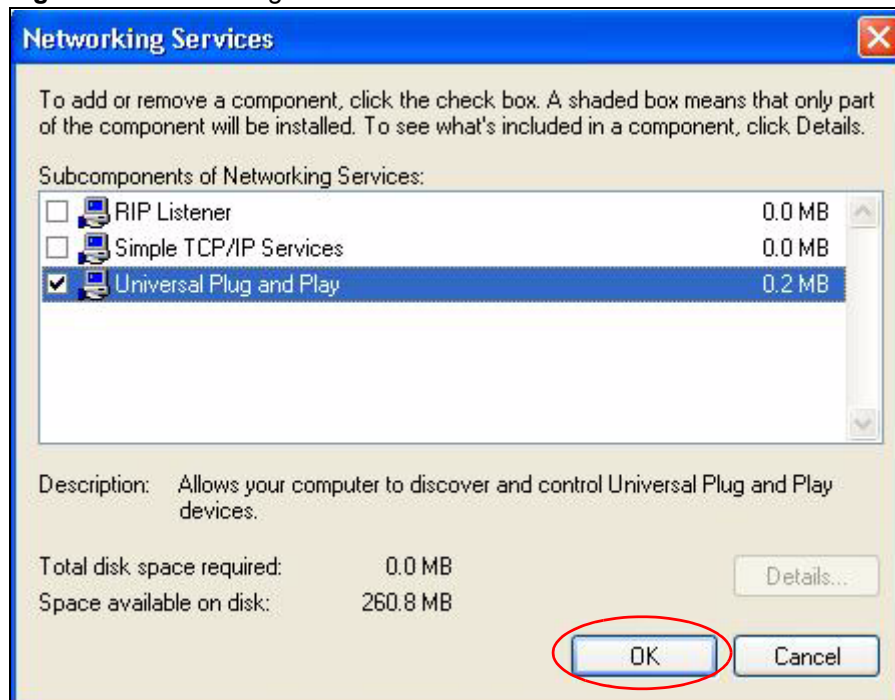
- 1 Click **Start** and **Control Panel**.
- 2 Double-click **Network Connections**.
- 3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ...**.

Figure 30 Network Connections

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

Figure 31 Windows Optional Networking Components Wizard

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

Figure 32 Networking Services

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

11.4 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.

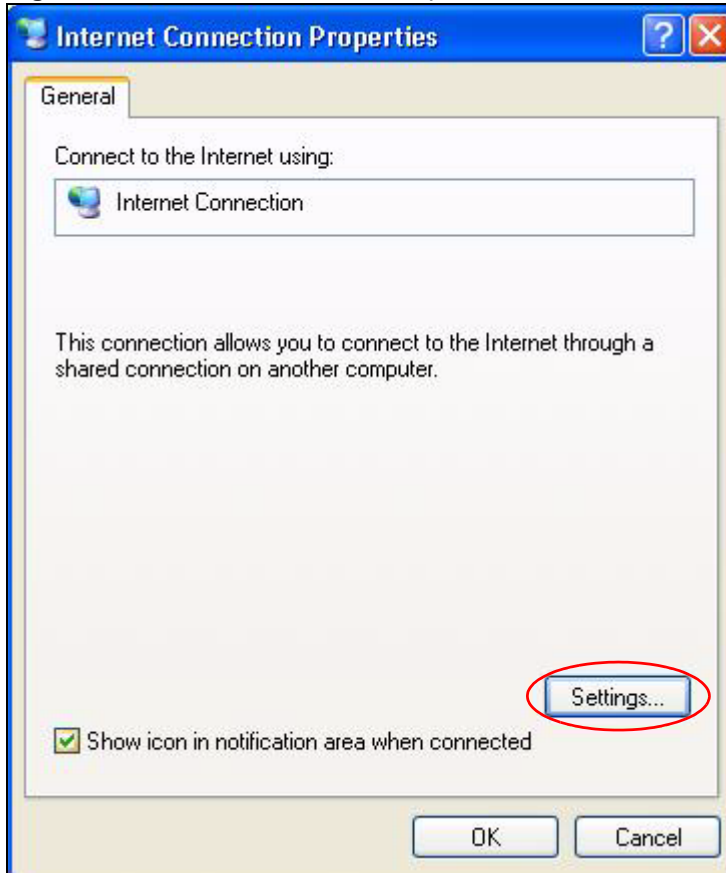
Auto-discover Your UPnP-enabled Network Device

- 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 33 Network Connections



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

Figure 34 Internet Connection Properties

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

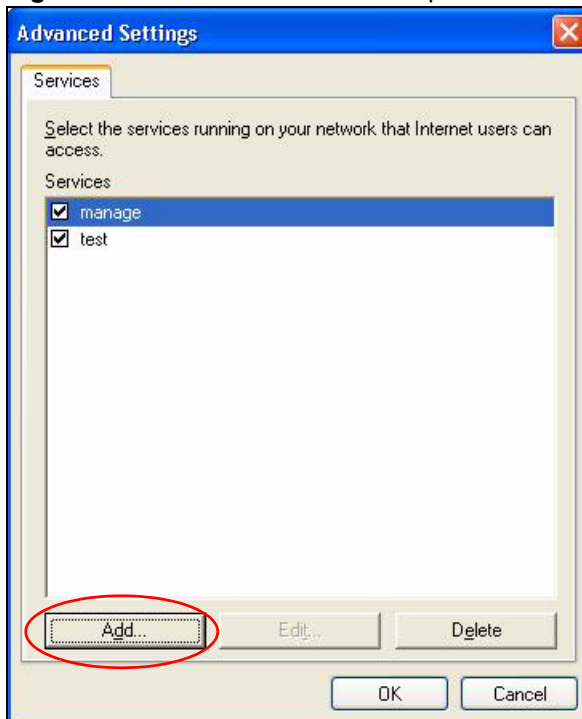
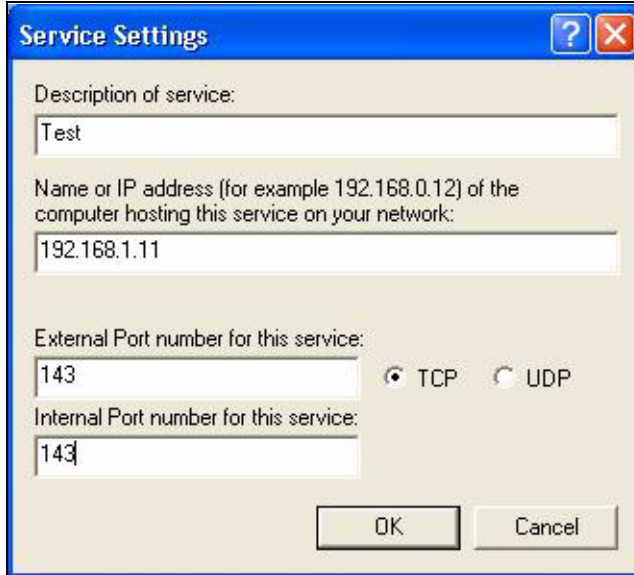
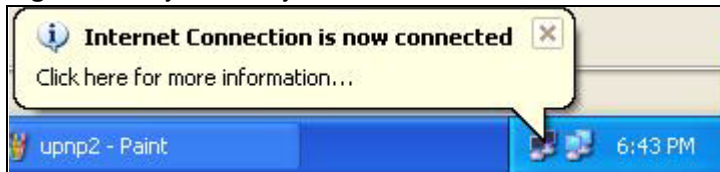
Figure 35 Internet Connection Properties: Advanced Settings

Figure 36 Internet Connection Properties: Advanced Settings: Add



- 5 When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.
- 6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

Figure 37 System Tray Icon



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

Figure 38 Internet Connection Status

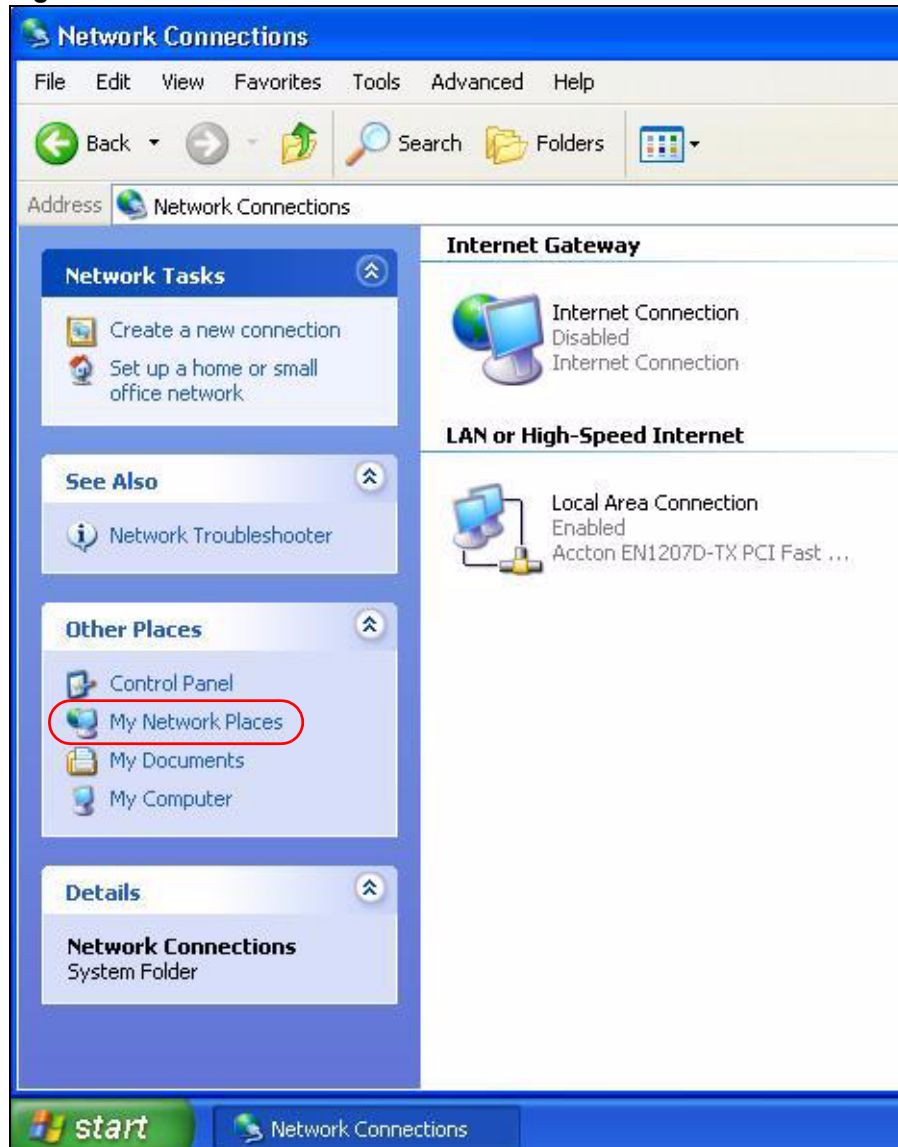
11.4.1 Web Configurator Easy Access

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 becomes helpful if you do not know the IP address of the ZyXEL Device.

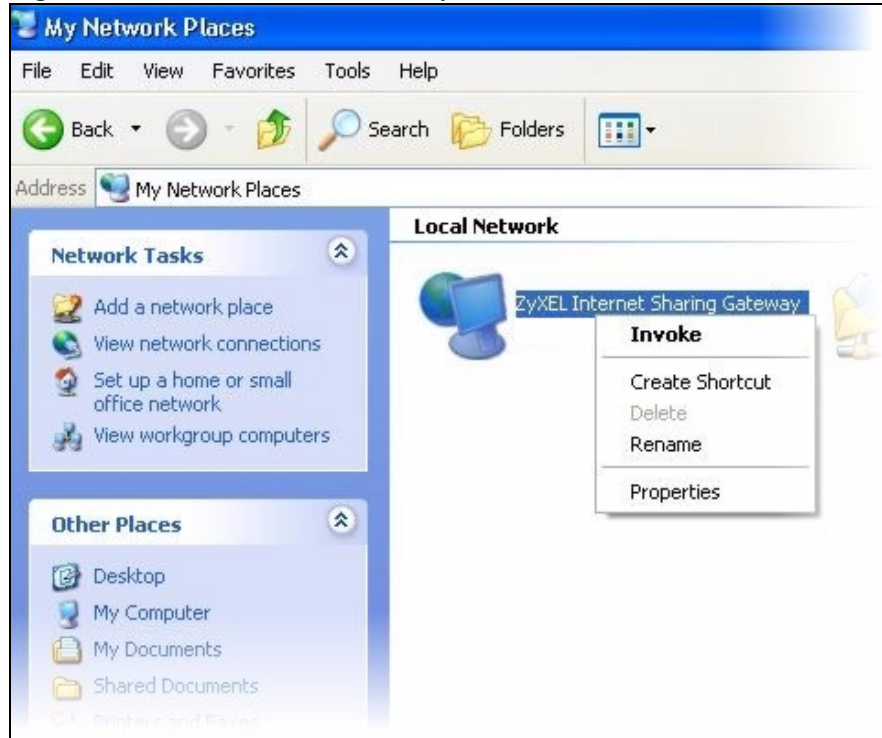
Follow the steps below to access the web configurator.

- 1 Click **Start** and then **Control Panel**.
- 2 Double-click **Network Connections**.
- 3 Select **My Network Places** under **Other Places**.

Figure 39 Network Connections



- 4 An icon with the description for each UPnP-enabled device displays under **Local Network**.
- 5 Right-click on the icon for your ZyXEL Device and select **Invoke**. The web configurator login screen displays.

Figure 40 Network Connections: My Network Places

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

Figure 41 Network Connections: My Network Places: Properties: Example

Network Address Translation (NAT) Screens

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

12.1 NAT 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.

12.1.1 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 on 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 19 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.

12.1.2 What NAT Does

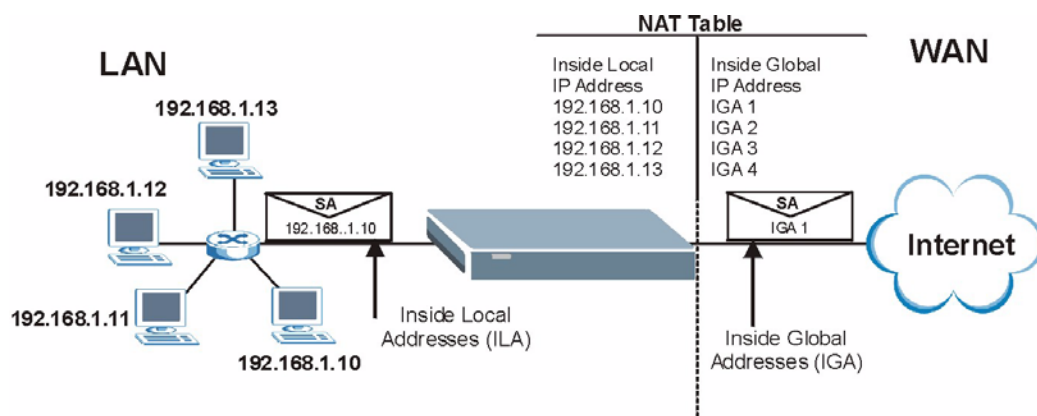
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) 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 (a web server and a telnet server, for example) on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see [Table 20 on page 94](#)), 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)*.

12.1.3 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.

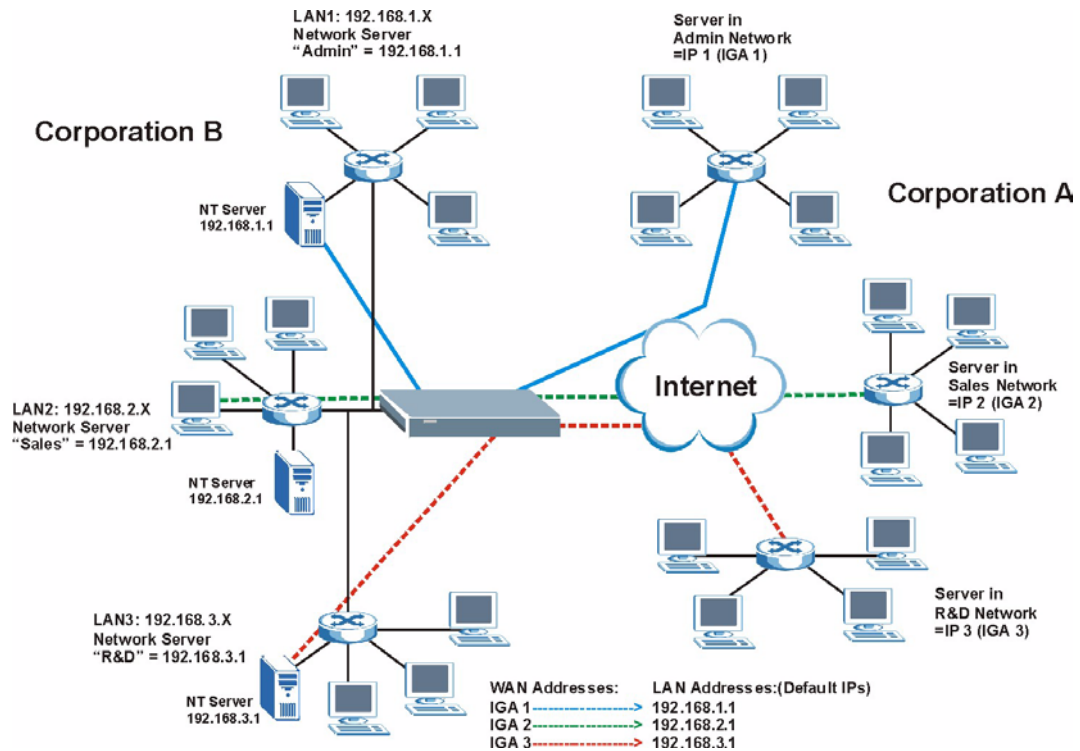
Figure 42 How NAT Works



12.1.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP Alias) behind the ZyXEL Device can communicate with three distinct WAN networks. More examples follow at the end of this chapter.

Figure 43 NAT Application With IP Alias



12.1.5 NAT Mapping Types

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

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



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

The following table summarizes these types.

Table 20 NAT Mapping Types

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

12.2 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The ZyXEL Device also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types as outlined in [Table 20 on page 94](#).



Choose SUA Only if you have just one public WAN IP address for your ZyXEL Device.



Choose Full Feature if you have multiple public WAN IP addresses for your ZyXEL Device.

12.3 SUA Server

A SUA server 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 SUA makes your whole inside network appear as a single computer to the outside world.

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.

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.

12.3.1 Default Server IP Address

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



If you do not assign an IP address in Server Set 1 (default server) the ZyXEL Device discards all packets received for ports that are not specified here or in the remote management setup.

12.3.2 Port Forwarding: Services and Port Numbers

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers.

Table 21 Services and Port Numbers

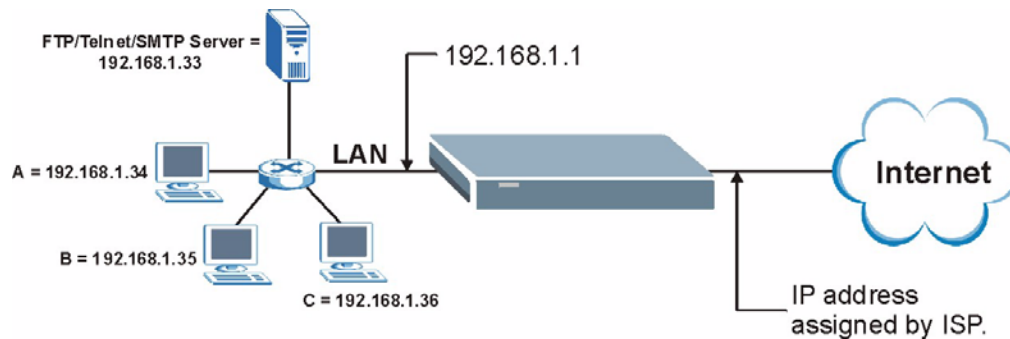
SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

12.3.3 Configuring Servers Behind SUA (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.

IP address assigned by ISP.

Figure 44 Multiple Servers Behind NAT Example



12.4 Selecting the NAT Mode

Click **NAT** to open the following screen.

Figure 45 NAT Mode

NAT - Mode

Network Address Translation

None
 SUA Only [Edit Details](#)
 Full Feature [Edit Details](#)

The following table describes the labels in this screen.

Table 22 NAT Mode

LABEL	DESCRIPTION
None	Select this radio button to disable NAT.
SUA Only	Select this radio button if you have just one public WAN IP address for your ZyXEL Device. The ZyXEL Device uses Address Mapping Set 1 in the NAT - Edit SUA/NAT Server Set screen.
Edit Details	Click this link to go to the NAT - Edit SUA/NAT Server Set screen.
Full Feature	Select this radio button if you have multiple public WAN IP addresses for your ZyXEL Device.

Table 22 NAT Mode (continued)

LABEL	DESCRIPTION
Edit Details	Click this link to go to the NAT - Address Mapping Rules screen.
Apply	Click Apply to save your configuration.

12.5 Configuring SUA Server



If you do not assign an IP address in Server Set 1 (default server), the ZyXEL Device discards all packets received for ports that are not specified here or in the remote management setup.

Click **NAT**, select **SUA Only** and click **Edit Details** to open the following screen.

Refer to [Table 21 on page 95](#) for port numbers commonly used for particular services.

Figure 46 Edit SUA/NAT Server Set

NAT - Edit SUA/NAT Server Set

	Start Port No.	End Port No.	IP Address
1	All ports	All ports	0.0.0.0
2	0	0	0.0.0.0
3	0	0	0.0.0.0
4	0	0	0.0.0.0
5	0	0	0.0.0.0
6	0	0	0.0.0.0
7	0	0	0.0.0.0
8	0	0	0.0.0.0
9	0	0	0.0.0.0
10	0	0	0.0.0.0
11	0	0	0.0.0.0
12	0	0	0.0.0.0

The following table describes the labels in this screen.

Table 23 Edit SUA/NAT Server Set

LABEL	DESCRIPTION
Start Port No.	Enter a port number in this field. To forward only one port, enter the port number again in the End Port No. field. To forward a series of ports, enter the start port number here and the end port number in the End Port No. field.
End Port No.	Enter a port number in this field. To forward only one port, enter the port number again in the Start Port No. field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the Start Port No. field above.
IP Address	Enter your server IP address in this field.
Save	Click Save to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to return to the previous configuration.

12.6 Configuring Address Mapping

Ordering your rules is important because the ZyXEL Device applies the rules in the order that you specify. When a rule matches the current packet, the ZyXEL Device takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9. Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so old rules 5, 6 and 7 become new rules 4, 5 and 6.

To change your ZyXEL Device's address mapping settings, click **NAT**, Select **Full Feature** and click **Edit Details** to open the following screen.

Figure 47 Address Mapping Rules

<i>NAT - Address Mapping Rules</i>					
	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
Rule 1	-
Rule 2	-
Rule 3	-
Rule 4	-
Rule 5	-
Rule 6	-
Rule 7	-
Rule 8	-
Rule 9	-
Rule 10	-

Back

The following table describes the labels in this screen.

Table 24 Address Mapping Rules

LABEL	DESCRIPTION
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are N/A for Server port mapping.
Local End IP	This is the end Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is N/A for One-to-one and Server mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for Many-to-One and Server mapping types.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is N/A for One-to-one , Many-to-One and Server mapping types.
Type	<p>1-1: One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type.</p> <p>M-1: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (in other words, PAT, port address translation), ZyXEL's Single User Account feature.</p> <p>M-M Ov (Overload): Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses.</p> <p>MM No (No Overload): Many-to-Many No Overload mode maps each local IP address to unique global IP addresses.</p> <p>Server: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.</p>
Back	Click Back to return to the NAT Mode screen.

12.7 Editing an Address Mapping Rule

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

Figure 48 Address Mapping Rule Edit

NAT - Edit Address Mapping Rule 1

Type: One-to-One

Local Start IP: 0.0.0.0

Local End IP: N/A

Global Start IP: 0.0.0.0

Global End IP: N/A

Server Mapping Set: N/A [Edit Details](#)

Apply Cancel Delete

The following table describes the labels in this screen.

Table 25 Address Mapping Rule Edit

LABEL	DESCRIPTION
Type	Choose the port mapping type from one of the following. <ul style="list-style-type: none"> • One-to-One: One-to-One mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type. • Many-to-One: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only. • Many-to-Many Overload: Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. • Many-to-Many No Overload: Many-to-Many No Overload mode maps each local IP address to unique global IP addresses. • Server: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	This is the starting local IP address (ILA). Local IP addresses are N/A for Server port mapping.
Local End IP	This is the end local IP address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is N/A for One-to-One and Server mapping types.
Global Start IP	This is the starting global IP address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending global IP address (IGA). This field is N/A for One-to-One , Many-to-One and Server mapping types.
Server Mapping Set	Only available when Type is set to Server . Select a number from the drop-down menu to choose a server set from the NAT - Address Mapping Rules screen.
Edit Details	Click this link to go to the NAT - Edit SUA/NAT Server Set screen to edit a server set that you have selected in the Server Mapping Set field.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to return to the previously saved settings.
Delete	Click Delete to exit this screen without saving.

PART IV

Maintenance and Troubleshooting

Maintenance (103)

Troubleshooting (115)

Maintenance

This chapter displays system information such as ZyNOS firmware, port IP addresses and port traffic statistics.

13.1 Maintenance Overview

The maintenance screens can help you view system information, upload new firmware, manage configuration and restart your ZyXEL Device.

13.2 System Status Screen

Click **System Status** to open the following screen. You can use this screen to monitor your ZyXEL Device. Note that these fields are READ-ONLY and are intended only for diagnostic purposes.

Figure 49 System Status

The screenshot displays the 'System Status' page with three main sections:

- System Status:**
 - System Name: P-660RU-T1_y2
 - ZyNOS FW Version: V3.40(ACM.0) | 08/23/2006
 - DSL FW Version: DMT FwVer: 3.1.0.4_B_TC, HwVer: T14F7_0.0
 - Standard: Multi-Mode
- WAN Information:**
 - IP Address: 0.0.0.0
 - IP Subnet Mask: 0.0.0.0
 - Default Gateway: 0.0.0.0
 - VPI/VCI: 8/ 35
- LAN Information:**
 - MAC Address: 00:13:49:00:00:01
 - IP Address: 192.168.1.1
 - IP Subnet Mask: 255.255.255.0
 - DHCP: Server
 - DHCP Start IP: 192.168.1.33
 - DHCP Pool Size: 32

At the bottom of the page, there is a button labeled 'Show Statistics'.

The following table describes the fields in this screen.

Table 26 System Status

LABEL	DESCRIPTION
System Status	
System Name	This is the name of your ZyXEL Device. It is for identification purposes.
ZyNOS Firmware Version	This is the ZyNOS firmware version and the date the firmware was created. ZyNOS is ZyXEL's proprietary Network Operating System design.
DSL FW Version	This is the DSL firmware version associated with your ZyXEL Device.
Standard	This is the standard that your ZyXEL Device is using.
WAN Information	
IP Address	This is the WAN port IP address.
IP Subnet Mask	This is the WAN port IP subnet mask.
Default Gateway	This is the IP address of the default gateway, if applicable.

Table 26 System Status (continued)

LABEL	DESCRIPTION
VPI/VCI	This is the Virtual Path Identifier and Virtual Channel Identifier that you entered in the first Wizard screen.
LAN Information	
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your ZyXEL Device.
IP Address	This is the LAN port IP address.
IP Subnet Mask	This is the LAN port IP subnet mask.
DHCP	This is the WAN port DHCP role - Server, Relay (not all ZyXEL Device models) or None .
DHCP Start IP	This is the first of the contiguous addresses in the IP address pool.
DHCP Pool Size	This is the number of IP addresses in the IP address pool.
Show Statistics	Click Show Statistics to see the performance statistics such as number of packets sent and number of packets received for each port.

13.2.1 System Statistics

Click **Show Statistics** in the **System Status** screen to open the following screen. Read-only information here includes port status and packet specific statistics. Also provided are "system up time" and "poll interval(s)". The **Poll Interval(s)** field is configurable.

Figure 50 System Status: Show Statistics

System up Time: 1:40:33
CPU Load: 5.60%

WAN Port Statistics:
Link Status: **Down**
Upstream Speed: **0 kbps**
Downstream Speed: **0 kbps**

Node-Link	Status	TxPkts	RxPkts	Errors	Tx B/s	Rx B/s	Up Time
1-ENET	N/A	0	0	0	0	0	0:00:00

LAN Port Statistics:

Interface:	Status	TxPkts	RxPkts	Collisions
Ethernet	100M/Full Duplex	3086	2727	0
USB	DOWN	0	0	0

Poll Interval(s) :

The following table describes the labels in this screen.

Table 27 System Status: Show Statistics

LABEL	DESCRIPTION
System up Time	This is the elapsed time the system has been up.
CPU Load	This field specifies the percentage of CPU utilization.
LAN or WAN Port Statistics	This is the WAN or LAN port.
Link Status	This is the status of your WAN link.
Upstream Speed	This is the upstream speed of your ZyXEL Device.
Downstream Speed	This is the downstream speed of your ZyXEL Device.
Node-Link	This field displays the remote node index number and link type. Link types are PPPoA, ENET, RFC 1483 and PPPoE.
Interface	This field displays the type of port.
Status	For the WAN port, this displays the port speed and duplex setting if you're using Ethernet encapsulation and Down (line is down), Idle (line (ppp) idle), Dial (starting to trigger a call) and Drop (dropping a call) if you're using PPPoE encapsulation. For a LAN port, this shows the port speed and duplex setting. Ethernet port connections can be in half-duplex or full-duplex mode. Full-duplex refers to a device's ability to send and receive simultaneously, while half-duplex indicates that traffic can flow in only one direction at a time. The Ethernet port must use the same speed or duplex mode setting as the peer Ethernet port in order to connect.
TxPkts	This field displays the number of packets transmitted on this port.
RxPkts	This field displays the number of packets received on this port.
Errors	This field displays the number of error packets on this port.
Tx B/s	This field displays the number of bytes transmitted in the last second.
Rx B/s	This field displays the number of bytes received in the last second.
Up Time	This field displays the elapsed time this port has been up.
Collisions	This is the number of collisions on this port.
Poll Interval(s)	Type the time interval for the browser to refresh system statistics.
Set Interval	Click this button to apply the new poll interval you entered in the Poll Interval field above.
Stop	Click this button to halt the refreshing of the system statistics.

13.3 DHCP Table Screen

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 set to **None**, DHCP service will be disabled and you must have another DHCP server on your LAN, or else the computer must be manually configured.

Click **Maintenance**, and then the **DHCP Table** tab. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP Client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the DHCP server.

Figure 51 DHCP Table

Host Name	IP Address	MAC Address
tw	192.168.1.33	00-00-E8-7C-14-80

The following table describes the fields in this screen.

Table 28 DHCP Table

LABEL	DESCRIPTION
Host Name	This is the name of the host computer.
IP Address	This field displays the IP address relative to the Host Name field.
MAC Address	This field displays the MAC (Media Access Control) address of the computer with the displayed host name. Every Ethernet device has a unique MAC 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.

13.4 Any IP Table Screen

Click **Maintenance**, **Any IP**. The Any IP table shows current read-only information (including the IP address and the MAC address) of all network devices that use the Any IP feature to communicate with the ZyXEL Device. Refer to [Section 5.4 on page 56](#) for more information.

Figure 52 Any IP Table

#	IP Address	MAC Address
1	192.168.10.1	00:50:ba:ad:4f:81

Refresh

The following table describes the labels in this screen.

Table 29 Any IP Table

LABEL	DESCRIPTION
#	This field displays the index number.
IP Address	This field displays the IP address of the network device.

Table 29 Any IP Table

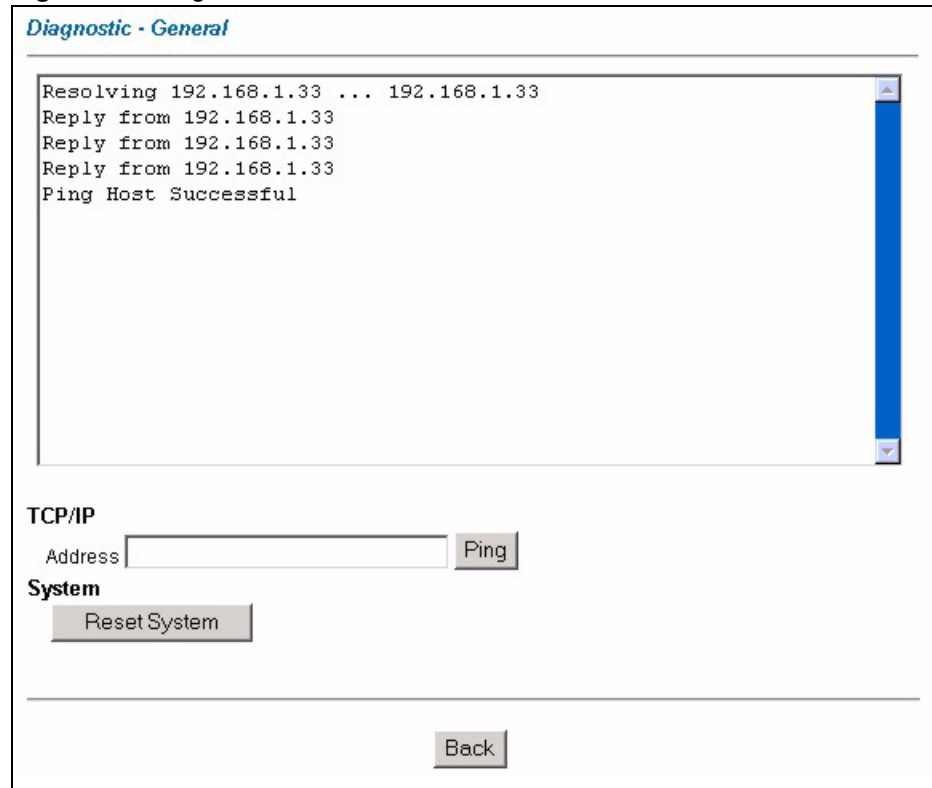
LABEL	DESCRIPTION
MAC Address	This field displays the MAC (Media Access Control) address of the computer with the displayed IP address. Every Ethernet device has a unique MAC address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Refresh	Click Refresh to update this screen.

13.5 Diagnostic Screens

These read-only screens display information to help you identify problems with the ZyXEL Device.

13.5.1 Diagnostic General Screen

Click **Diagnostic** and then **General** to open the screen shown next.

Figure 53 Diagnostic: General

The following table describes the labels in this screen.

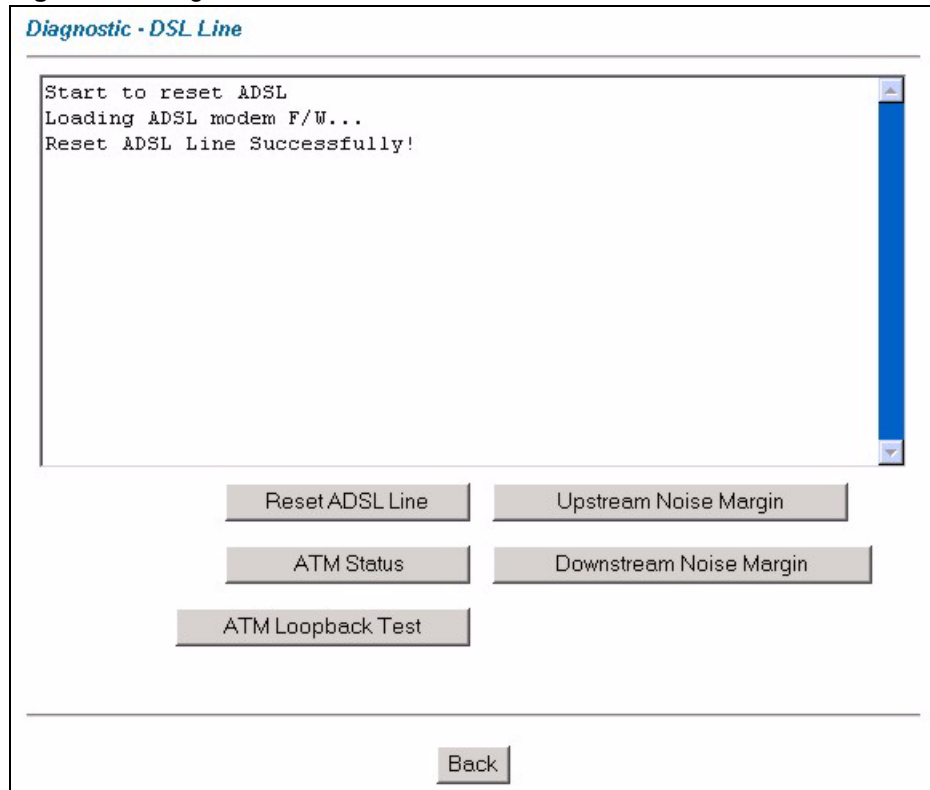
Table 30 Diagnostic: General

LABEL	DESCRIPTION
TCP/IP Address	Type the IP address of a computer that you want to ping in order to test a connection.
Ping	Click this button to ping the IP address that you entered.
Reset System	Click this button to reboot the ZyXEL Device. A warning dialog box is then displayed asking you if you're sure you want to reboot the system. Click OK to proceed.
Back	Click this button to go back to the main Diagnostic screen.

13.5.2 Diagnostic DSL Line Screen

Click **Diagnostic** and then **DSL Line** to open the screen shown next.

Figure 54 Diagnostic: DSL Line



The following table describes the labels in this screen.

Table 31 Diagnostic: DSL Line

LABEL	DESCRIPTION
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!"
ATM Status	Click this button to view ATM status.

Table 31 Diagnostic: DSL Line (continued)

LABEL	DESCRIPTION
ATM Loopback Test	Click this button to start the ATM loopback test. Make sure you have configured at least one PVC with proper VPIs/VCI 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.
Upstream Noise Margin	Click this button to display the upstream noise margin.
Downstream Noise Margin	Click this button to display the downstream noise margin.
Back	Click this button to go back to the main Diagnostic screen.

13.6 Firmware Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a .bin extension, for example, "ZyXEL.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.



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

Click **Firmware** to open the following screen. Follow the instructions in this screen to upload firmware to your ZyXEL Device.

Figure 55 Firmware Upgrade

The following table describes the labels in this screen.

Table 32 Firmware Upgrade

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

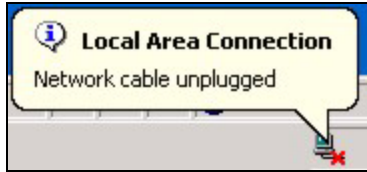


Do not turn off the ZyXEL Device while firmware upload is in progress!

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

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

Figure 56 Network Temporarily Disconnected



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

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

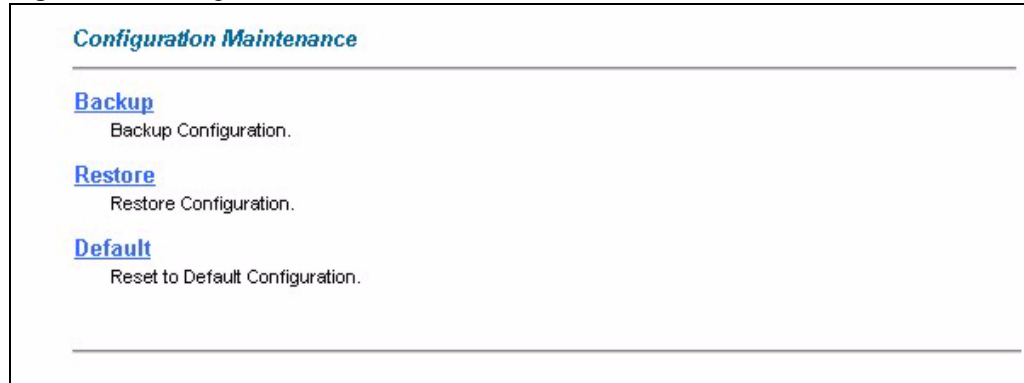
Figure 57 Error Message



13.7 Configuration Screen

Information related to backing up configuration, restoring configuration and resetting configuration to factory defaults appears as shown next. The following screens are not available on all models.

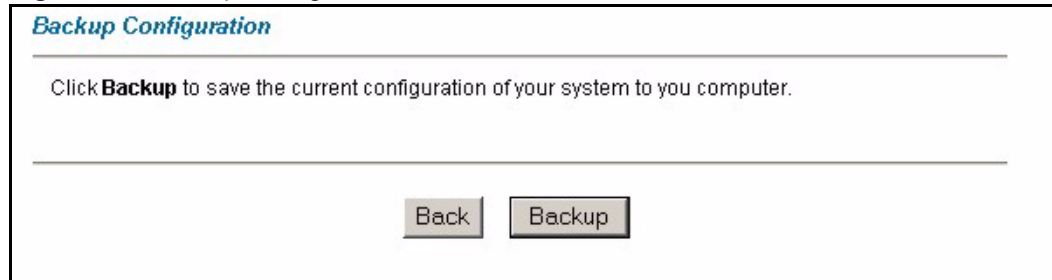
Click **Configuration** to see the following screen. You can choose to backup the configuration of your ZyXEL Device to a file on your computer, restore the configuration from a file on your computer or reset the configuration back to its factory defaults.

Figure 58 Configuration

13.7.1 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.

Figure 59 Backup Configuration

The following table describes the labels in this screen.

Table 33 Backup Configuration

LABEL	DESCRIPTION
Back	Click this button to go back to the main Configuration menu.
Backup	Click this button to save ZyXEL Device's current configuration to your computer.

13.7.2 Restore Configuration

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your ZyXEL Device. Click **Configuration** and then **Restore** to display the screen shown next.

Figure 60 Restore Configuration

The following table describes the labels in this screen.

Table 34 Maintenance Restore Configuration

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



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

After you see a “Restore Configuration Successful” screen, you must then wait one minute before logging into the ZyXEL Device again.

Figure 61 Restore Configuration Successful

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

Figure 62 Network Temporarily Disconnected

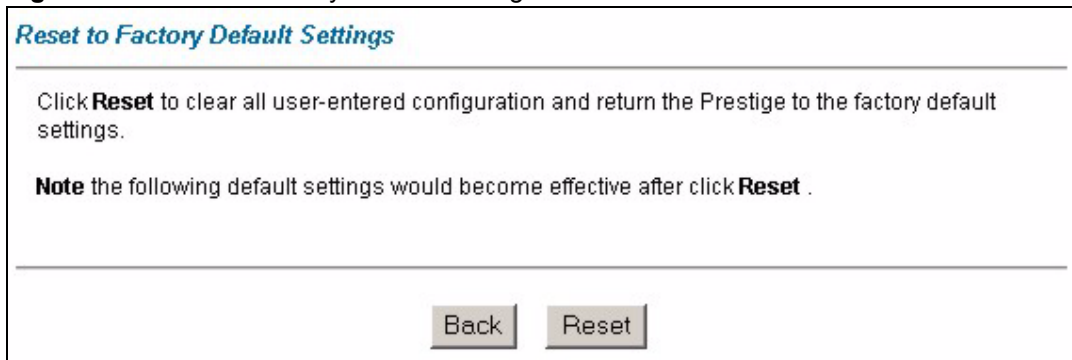


If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default ZyXEL Device IP address (192.168.1.1). See the appendix for details on how to set up your computer's IP address.

13.7.3 Reset to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the ZyXEL Device to its factory defaults.

Figure 63 Reset to Factory Default Settings



You can also press the **RESET** button on the rear panel to restore your ZyXEL Device to its factory default settings.

Troubleshooting

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

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

14.1 Power, Hardware Connections, and LEDs



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

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



One of the LEDs does not behave as expected.

- 1 Make sure you understand the normal behavior of the LED. See [Section 1.5 on page 27](#).
- 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.

14.2 ZyXEL Device Access and Login



I forgot the IP address for the ZyXEL Device.

- 1 The default IP address is **192.168.1.1**.
- 2 If you changed the IP address and have forgotten it, you might get the IP address of the ZyXEL Device by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the ZyXEL Device (it depends on the network), so enter this IP address in your Internet browser.
- 3 If this does not work, you have to reset the device to its factory defaults. See [Section 2.2 on page 30](#).



I forgot the password.

- 1 The default password is **1234**.
- 2 If this does not work, you have to reset the device to its factory defaults. See [Section 2.2 on page 30](#).



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 5.5 on page 57](#)), 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 and [Section 1.5 on page 27](#).
- 3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See [Appendix D on page 149](#).
- 4 If you disabled **Any IP** ([Section 5.4 on page 56](#)), make sure your computer is in the same subnet as the ZyXEL Device. (If you know that there are routers between your computer and the ZyXEL Device, skip this step.)
 - If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See [Section 5.5 on page 57](#). Your ZyXEL Device is a DHCP server by default.
 - If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the ZyXEL Device. See [Section 5.5 on page 57](#).

- 5 Reset the device to its factory defaults, and try to access the ZyXEL Device with the default IP address. See [Section 2.1.1 on page 29](#).
- 6 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 to find out why the ZyXEL Device does not respond to HTTP.
- If your computer is connected to the **WAN** port or is connected wirelessly, use a computer that is connected to an **ETHERNET** port.



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

- 1 Make sure you have entered the user name and password correctly. The default password is **1234**. This field is 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 2.2 on page 30](#).



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.

14.3 Internet Access



I cannot access the Internet.

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 1.5 on page 27](#).
- 2 Make sure you entered your ISP account information correctly in the wizard. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 3 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
- 4 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 27](#).
- 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 27](#). 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 Turn the ZyXEL Device off and on.

PART V

Appendices and Index

Product Specifications (121)
Setting up Your Computer's IP Address (125)
IP Addresses and Subnetting (141)
Pop-up Windows, JavaScripts and Java Permissions (149)
Virtual Circuit Topology (155)
Legal Information (157)
Customer Support (161)
Index (165)

Product Specifications

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

Table 35 Hardware Features

Dimensions	111 mm (L) × 106.5 mm (W) × 35 mm (H)
Weight	170g
Power Specification	9VAC 1A
Ethernet Port	One auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet Port.
USB Port	One USB v1.1 port
Operation Temperature	0° C ~ 40° C
Storage Temperature	-20° ~ 60° C
Operation Humidity	20% ~ 85% RH
Storage Humidity	20% ~ 90% RH

Table 36 Firmware Specifications

Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
DHCP Pool	192.168.1.33 to 192.168.1.64
ADSL Standards	Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt(G.992.1); G.lite(G.992.2)). ADSL2 G.dmt.bis (G.992.3) ADSL2 G.lite.bis (G.992.4) ADSL2+ (G.992.5) Reach-Extended ADSL (RE ADSL) SRA (Seamless Rate Adaptation) Auto-negotiating rate adaptation ADSL physical connection ATM AAL5 (ATM Adaptation Layer type 5) Multi-protocol over AAL5 (RFC2684/1483) PPP over ATM AAL5 (RFC 2364) PPP over Ethernet (RFC 2516) RFC 1483 encapsulation over ATM MAC encapsulated routing (ENET encapsulation) VC-based and LLC-based multiplexing Up to 8 PVCs (Permanent Virtual Circuits) I.610 F4/F5 OAM

Table 36 Firmware Specifications

Management	<p>Embedded Web Configurator CLI (Command Line Interpreter) Remote Management via Telnet or Web SNMP manageable FTP/TFTP for firmware downloading, configuration backup and restoration. Built-in Diagnostic Tools for FLASH memory, ADSL circuitry, RAM and LAN port Syslog</p>
Firmware Upgrade	<p>Download new firmware (when available) from the ZyXEL web site and use the web configurator, an FTP or a TFTP tool to put it on the ZyXEL Device.</p> <p>Note: Only upload firmware for your specific model!</p>
Configuration Backup & Restoration	<p>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.</p>
Network Address Translation (NAT)	<p>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.</p>
Multiple PVCs (Permanent Virtual Circuits)	<p>Your ZyXEL Device supports up to 8 PVCs.</p>
Packet Filters	<p>The ZyXEL Device's packet filtering functions allows added network security and management.</p>
Port Forwarding	<p>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.</p>
Traffic Redirect	<p>Traffic redirect forwards WAN traffic to a backup gateway when the ZyXEL Device cannot connect to the Internet, thus acting as an auxiliary if your regular WAN connection fails.</p>
DHCP (Dynamic Host Configuration Protocol)	<p>Use this feature to have the ZyXEL Device assign IP addresses, an IP default gateway and DNS servers to computers on your network.</p>
Dynamic DNS Support	<p>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.</p>
IP Multicast	<p>IP multicast is used to send traffic to a specific group of computers. The ZyXEL Device supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).</p>
IP Alias	<p>IP alias allows you to subdivide a physical network into logical networks over the same Ethernet interface with the ZyXEL Device itself as the gateway for each subnet.</p>
IP Policy Routing (IPPR)	<p>Traditionally, routing is based on the destination address only and the router takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator.</p>
Time and Date	<p>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.</p>
PPPoE	<p>PPPoE mimics a dial-up Internet access connection.</p>
PPTP Encapsulation	<p>Point-to-Point Tunneling Protocol (PPTP) enables secure transfer of data through a Virtual Private Network (VPN). The ZyXEL Device supports one PPTP connection at a time.</p>

Table 36 Firmware Specifications

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.
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.
Other Protocol Support	PPP (Point-to-Point Protocol) link layer protocol. Transparent bridging for unsupported network layer protocols. DHCP Server/Client/Relay RIP I/RIP II ICMP ATM QoS SNMP v1 and v2c with MIB II support (RFC 1213) IGMP Proxy

Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

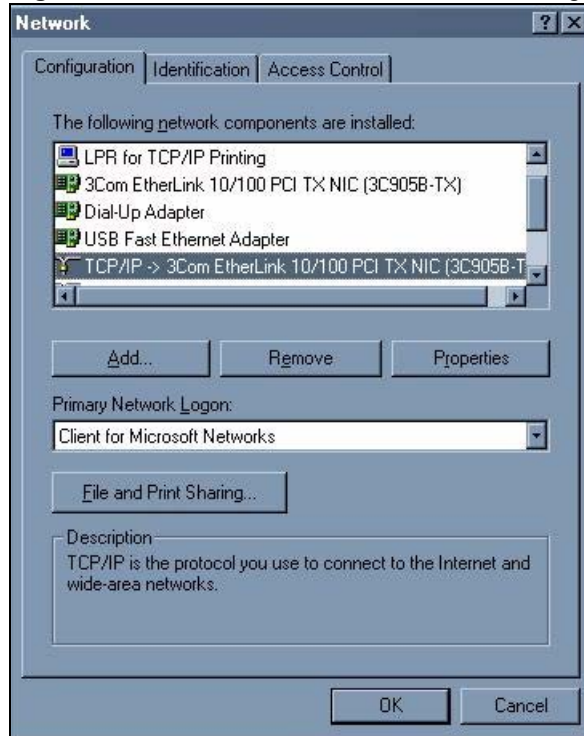
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the ZyXEL Device's LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

Figure 64 WIndows 95/98/Me: Network: Configuration

Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

- 1 In the **Network** window, click **Add**.
- 2 Select **Adapter** and then click **Add**.
- 3 Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

- 1 In the **Network** window, click **Add**.
- 2 Select **Protocol** and then click **Add**.
- 3 Select **Microsoft** from the list of **manufacturers**.
- 4 Select **TCP/IP** from the list of network protocols and then click **OK**.

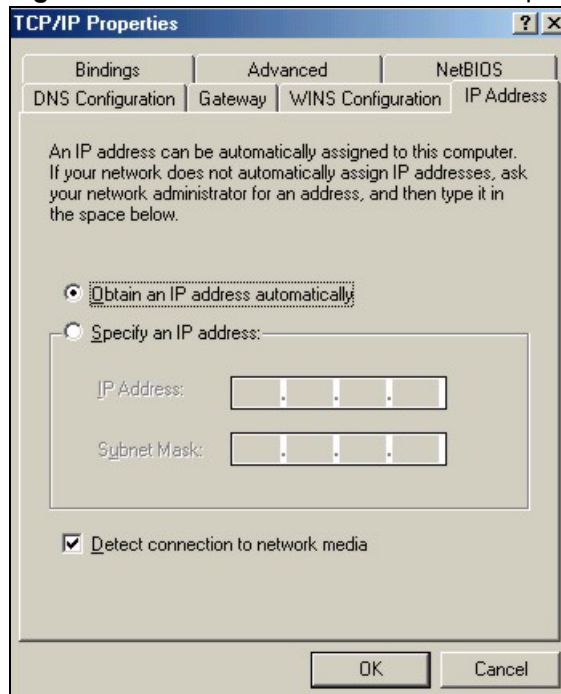
If you need Client for Microsoft Networks:

- 1 Click **Add**.
- 2 Select **Client** and then click **Add**.
- 3 Select **Microsoft** from the list of manufacturers.
- 4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
- 5 Restart your computer so the changes you made take effect.

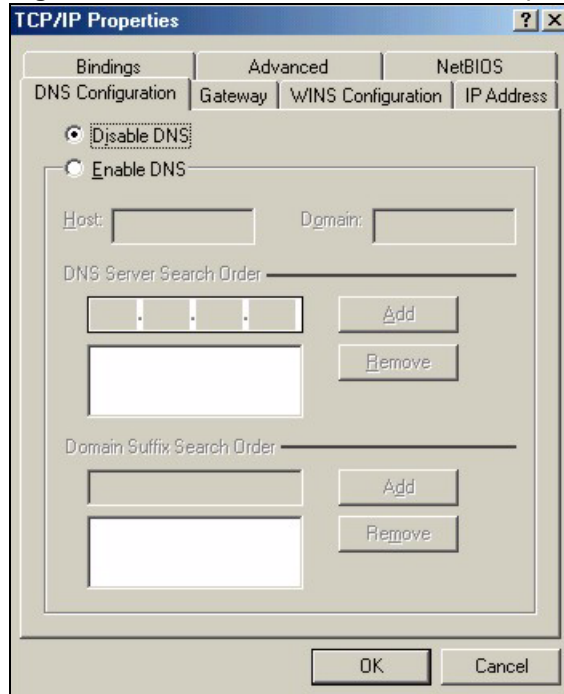
Configuring

- 1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**
- 2 Click the **IP Address** tab.
 - If your IP address is dynamic, select **Obtain an IP address automatically**.
 - If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

Figure 65 Windows 95/98/Me: TCP/IP Properties: IP Address



- 3 Click the **DNS Configuration** tab.
 - If you do not know your DNS information, select **Disable DNS**.
 - If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 66 Windows 95/98/Me: TCP/IP Properties: DNS Configuration

- 4 Click the **Gateway** tab.
 - If you do not know your gateway's IP address, remove previously installed gateways.
 - If you have a gateway IP address, type it in the **New gateway field** and click **Add**.
- 5 Click **OK** to save and close the **TCP/IP Properties** window.
- 6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
- 7 Turn on your ZyXEL Device and restart your computer when prompted.

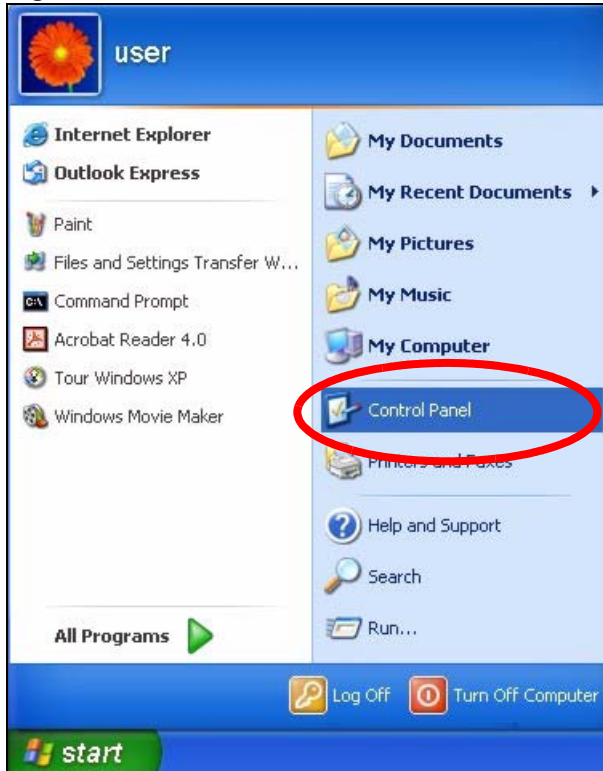
Verifying Settings

- 1 Click **Start** and then **Run**.
- 2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
- 3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

- 1 Click **start** (**Start** in Windows 2000/NT), **Settings, Control Panel**.

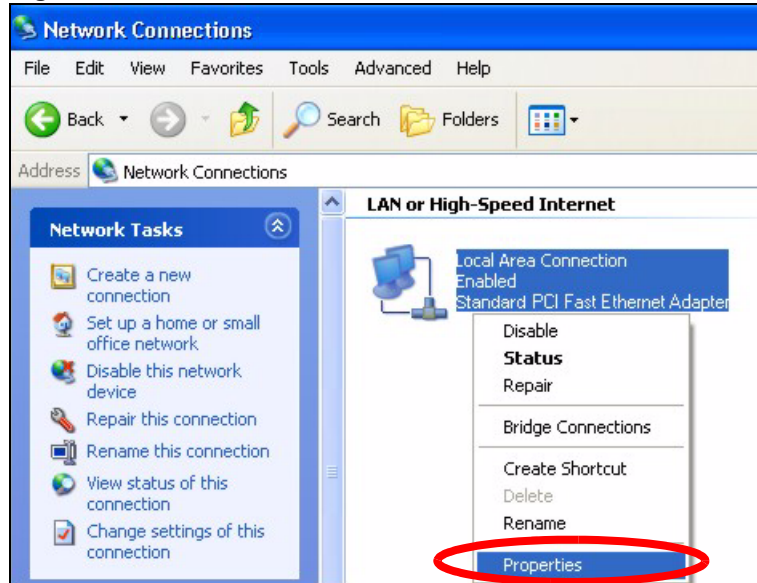
Figure 67 Windows XP: Start Menu

- 2 In the **Control Panel**, double-click **Network Connections (Network and Dial-up Connections)** in Windows 2000/NT).

Figure 68 Windows XP: Control Panel

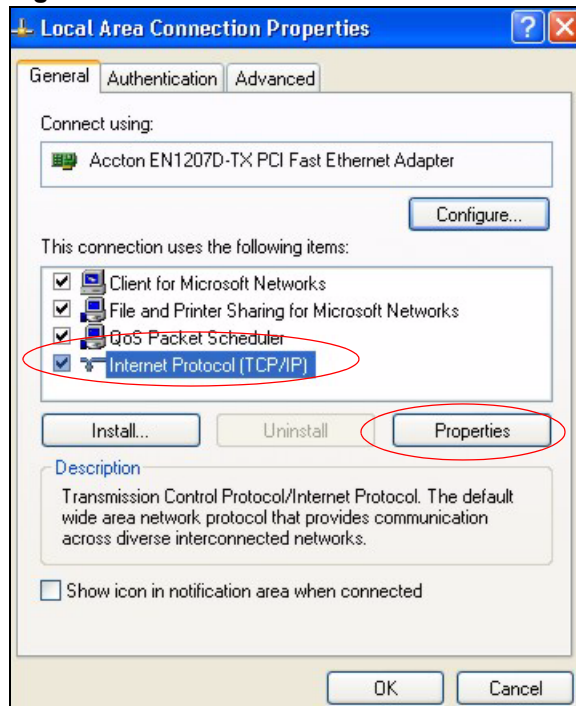
- 3 Right-click **Local Area Connection** and then click **Properties**.

Figure 69 Windows XP: Control Panel: Network Connections: Properties

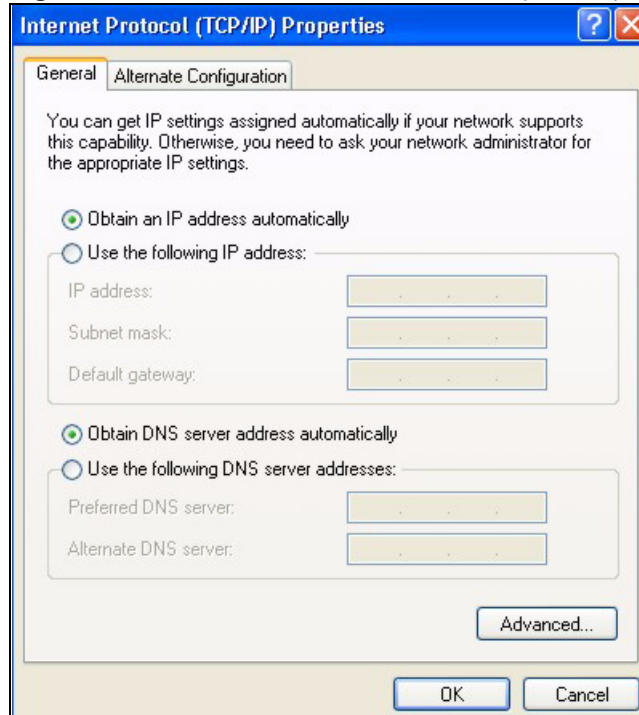


- 4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

Figure 70 Windows XP: Local Area Connection Properties



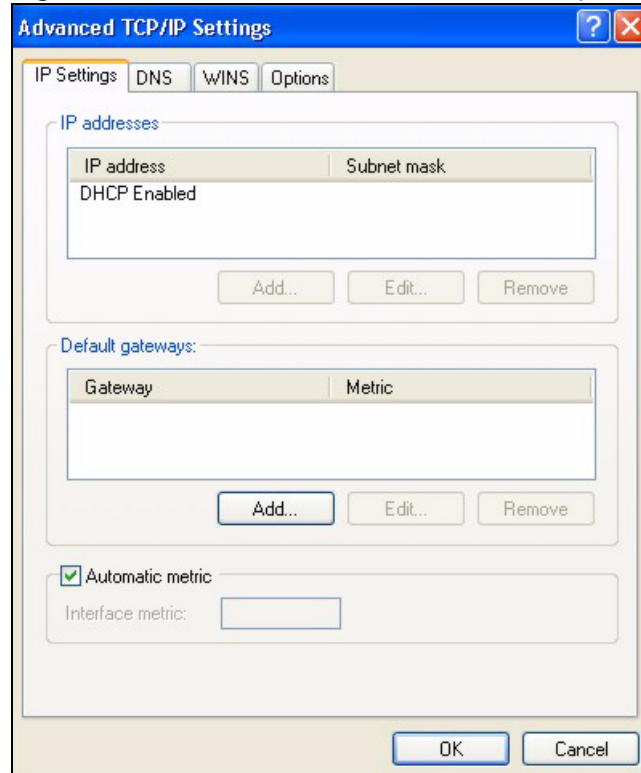
- 5 The **Internet Protocol TCP/IP Properties** window opens (the **General** tab in Windows XP).
 - If you have a dynamic IP address click **Obtain an IP address automatically**.
 - If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
 - Click **Advanced**.

Figure 71 Windows XP: Internet Protocol (TCP/IP) Properties

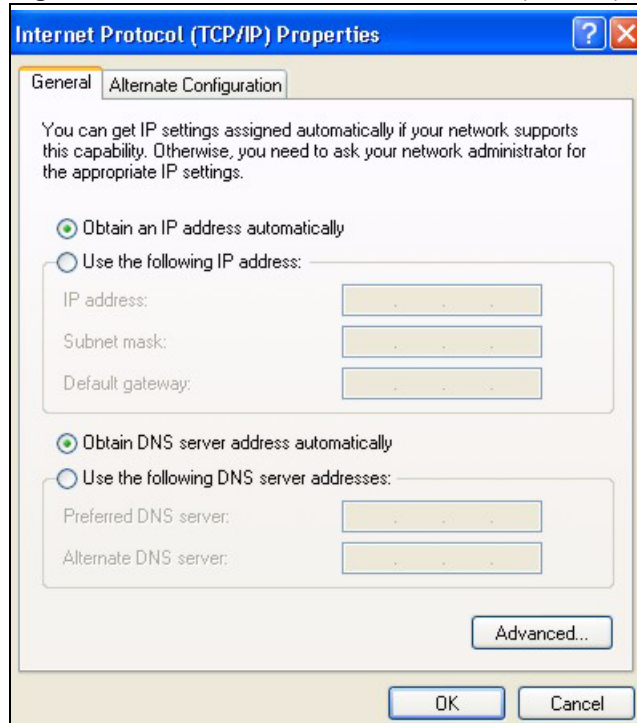
- 6** If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

Figure 72 Windows XP: Advanced TCP/IP Properties

- 7** In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):
- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
 - If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.
- If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 73 Windows XP: Internet Protocol (TCP/IP) Properties

- 8** Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 9** Click **Close (OK in Windows 2000/NT)** to close the **Local Area Connection Properties** window.
- 10** Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).
- 11** Turn on your ZyXEL Device and restart your computer (if prompted).

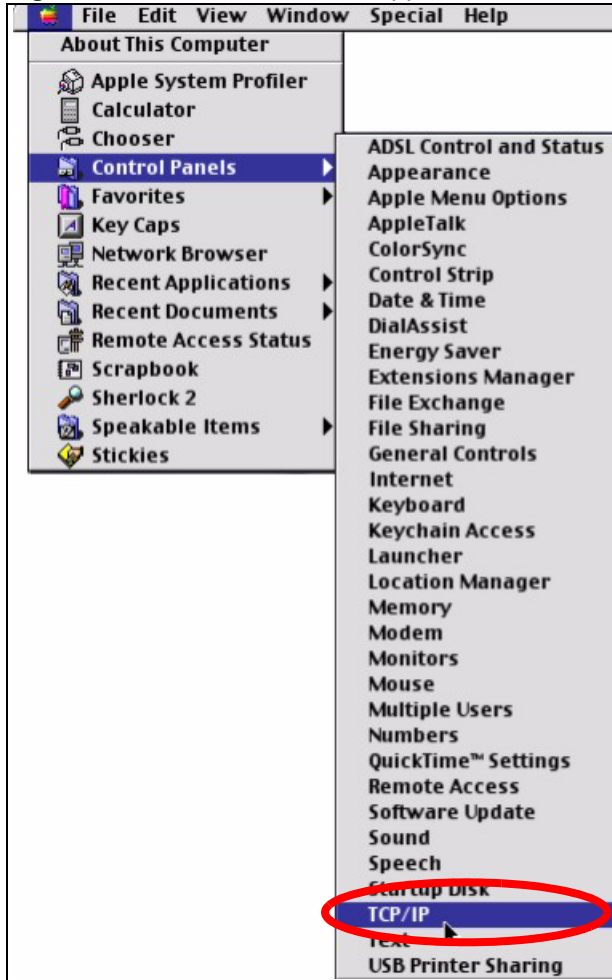
Verifying Settings

- 1** Click **Start, All Programs, Accessories** and then **Command Prompt**.
- 2** In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

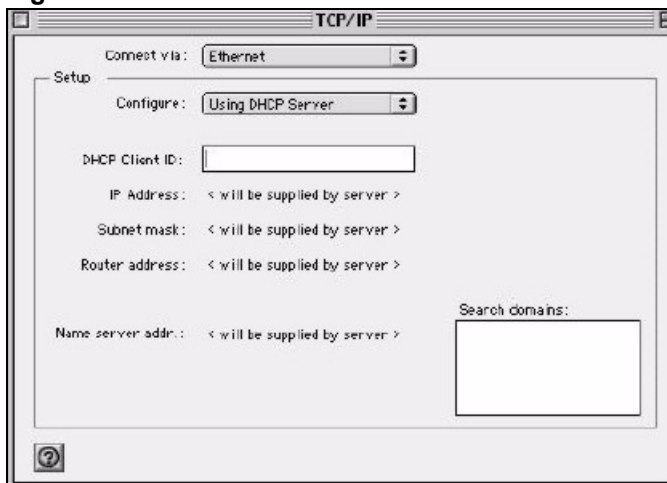
- 1** Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 74 Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

Figure 75 Macintosh OS 8/9: TCP/IP



3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.

- Type your IP address in the **IP Address** box.
 - Type your subnet mask in the **Subnet mask** box.
 - Type the IP address of your ZyXEL Device in the **Router address** box.
- 5** Close the **TCP/IP Control Panel**.
 - 6** Click **Save** if prompted, to save changes to your configuration.
 - 7** Turn on your ZyXEL Device and restart your computer (if prompted).

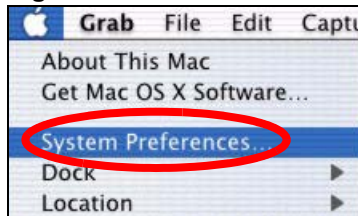
Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

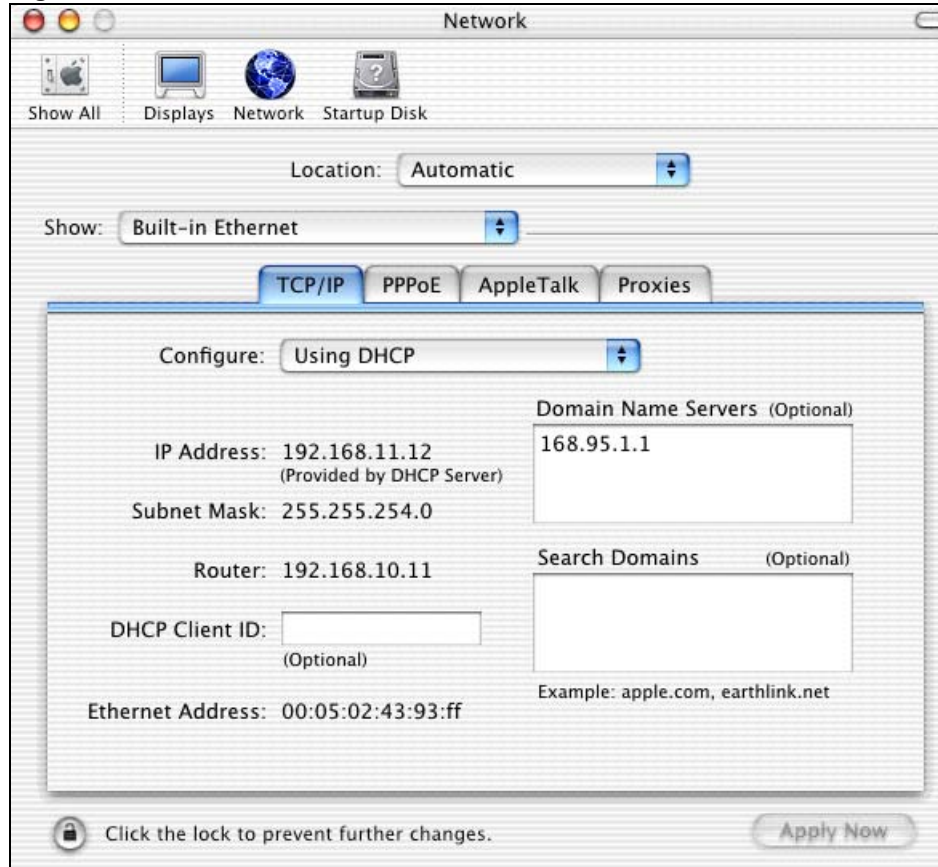
Macintosh OS X

- 1** Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 76 Macintosh OS X: Apple Menu



- 2** Click **Network** in the icon bar.
 - Select **Automatic** from the **Location** list.
 - Select **Built-in Ethernet** from the **Show** list.
 - Click the **TCP/IP** tab.
- 3** For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Figure 77 Macintosh OS X: Network

- 4 For statically assigned settings, do the following:
 - From the **Configure** box, select **Manually**.
 - Type your IP address in the **IP Address** box.
 - Type your subnet mask in the **Subnet mask** box.
 - Type the IP address of your ZyXEL Device in the **Router address** box.
- 5 Click **Apply Now** and close the window.
- 6 Turn on your ZyXEL Device and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Linux

This section shows you how to configure your computer's TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.



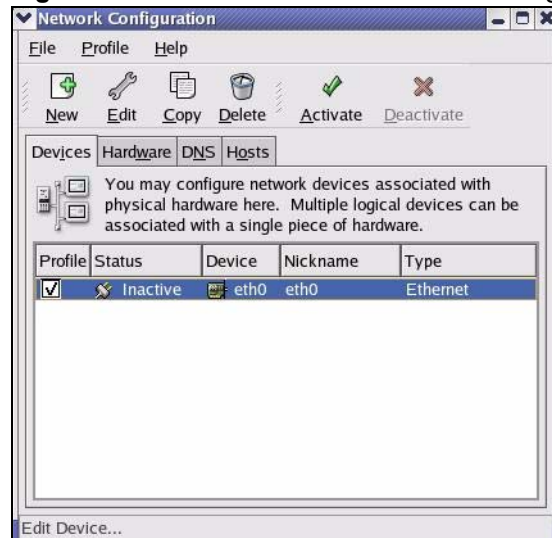
Make sure you are logged in as the root administrator.

Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

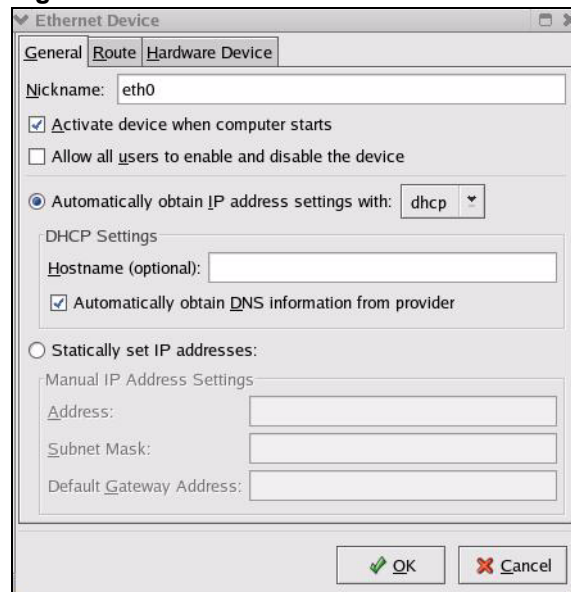
- 1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

Figure 78 Red Hat 9.0: KDE: Network Configuration: Devices



- 2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

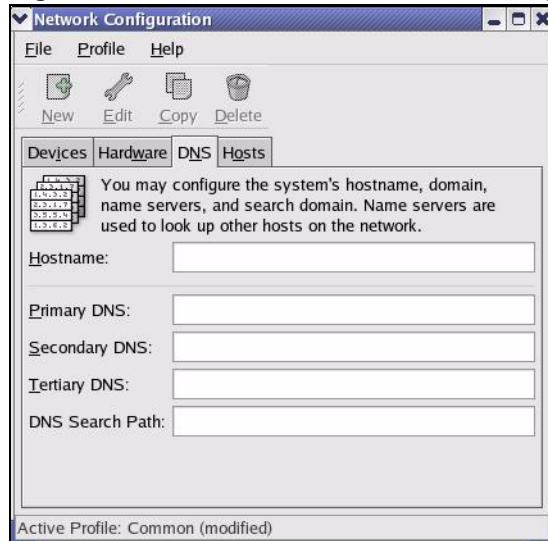
Figure 79 Red Hat 9.0: KDE: Ethernet Device: General



- If you have a dynamic IP address, click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
 - If you have a static IP address, click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.
- 3 Click **OK** to save the changes and close the **Ethernet Device General** screen.

- 4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

Figure 80 Red Hat 9.0: KDE: Network Configuration: DNS



- 5 Click the **Devices** tab.
- 6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes to save the changes in all screens.**

Figure 81 Red Hat 9.0: KDE: Network Configuration: Activate



- 7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

- 1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.
 - If you have a dynamic IP address, enter `dhcp` in the `BOOTPROTO=` field. The following figure shows an example.

Figure 82 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0

```

DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet

```

- If you have a static IP address, enter **static** in the `BOOTPROTO=` field. Type `IPADDR=` followed by the IP address (in dotted decimal notation) and type `NETMASK=` followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

Figure 83 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```

DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet

```

- 2 If you know your DNS server IP address(es), enter the DNS server information in the `resolv.conf` file in the `/etc` directory. The following figure shows an example where two DNS server IP addresses are specified.

Figure 84 Red Hat 9.0: DNS Settings in resolv.conf

```

nameserver 172.23.5.1
nameserver 172.23.5.2

```

- 3 After you edit and save the configuration files, you must restart the network card. Enter `./network restart` in the `/etc/rc.d/init.d` directory. The following figure shows an example.

Figure 85 Red Hat 9.0: Restart Ethernet Card

```

[root@localhost init.d]# network restart

Shutting down interface eth0:                [OK]
Shutting down loopback interface:            [OK]
Setting network parameters:                  [OK]
Bringing up loopback interface:              [OK]
Bringing up interface eth0:                  [OK]

```

Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

Figure 86 Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

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

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

Introduction to IP Addresses

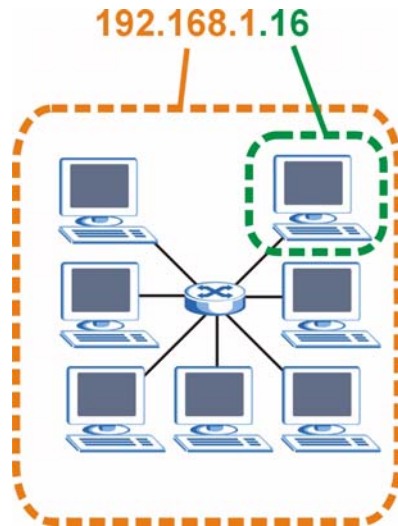
One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique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

Structure

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

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

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

Figure 87 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 37 Subnet Mask 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 38 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 39 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 40 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

Table 40 Alternative Subnet Mask Notation (continued)

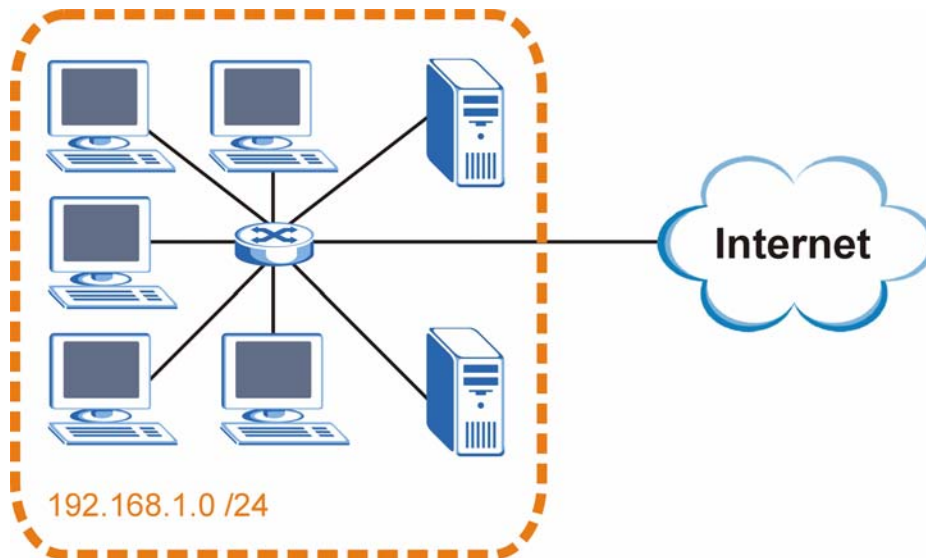
SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

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.

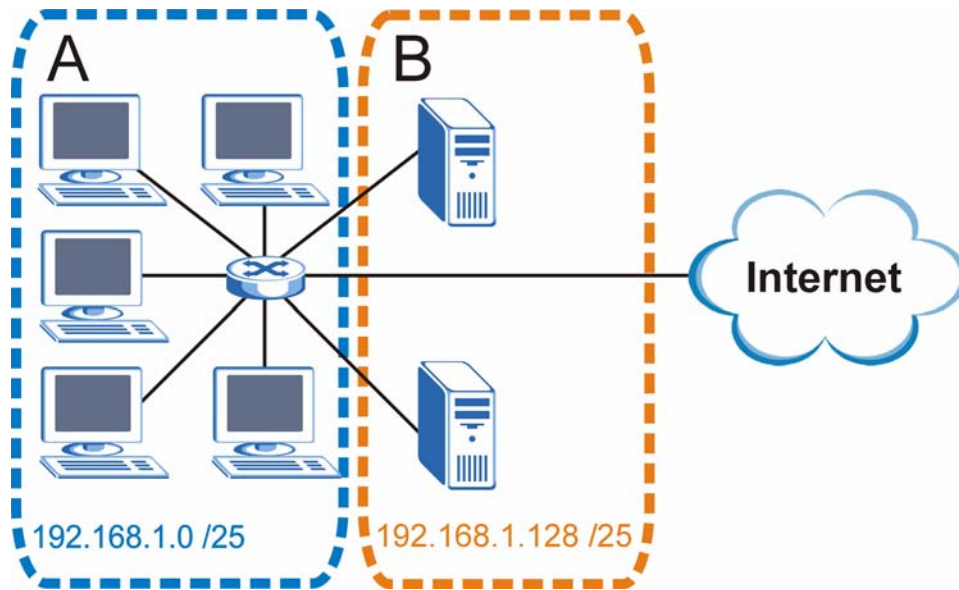
The following figure shows the company network before subnetting.

Figure 88 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 89 Subnetting Example: After Subnetting

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

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

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

Example: Four Subnets

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

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

Table 41 Subnet 1

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

Table 42 Subnet 2

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

Table 43 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 44 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	11000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
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 45 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

Table 45 Eight Subnets (continued)

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
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 46 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 47 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6

Table 47 16-bit Network Number Subnet Planning (continued)

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
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*.

Pop-up Windows, JavaScripts and Java Permissions

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

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



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

Internet Explorer Pop-up Blockers

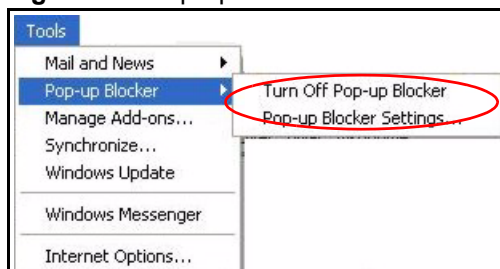
You may have to disable pop-up blocking to log into your device.

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 90 Pop-up Blocker

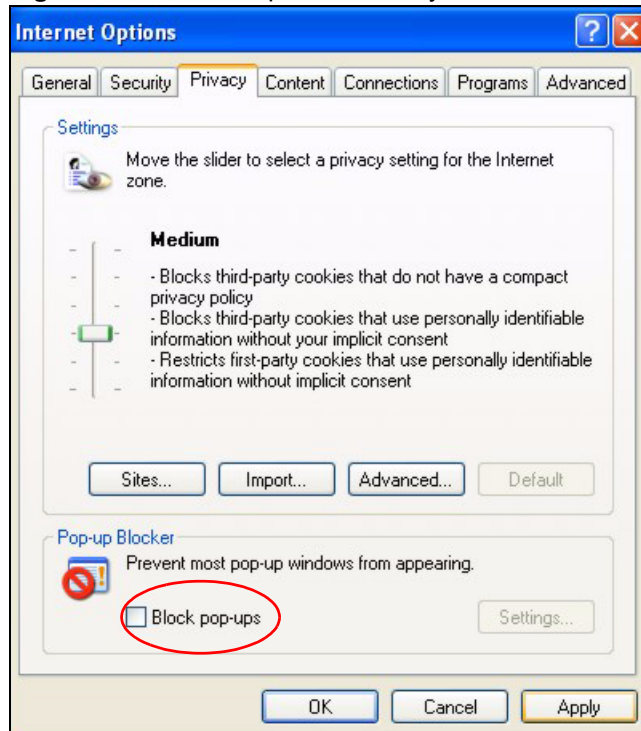


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

- 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 91 Internet Options: Privacy

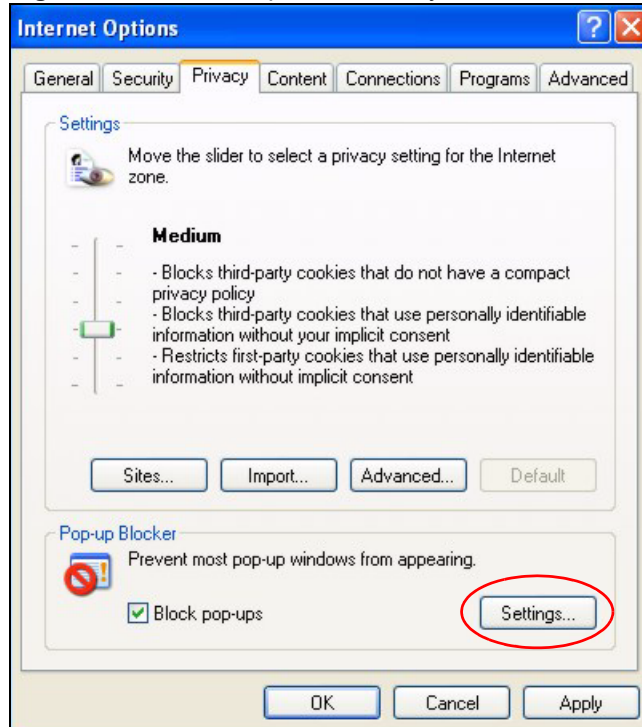


- 3 Click **Apply** to save this setting.

Enable pop-up Blockers with Exceptions

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

- 1 In Internet Explorer, select **Tools, Internet Options** and then the **Privacy** tab.
- 2 Select **Settings...** to open the **Pop-up Blocker Settings** screen.

Figure 92 Internet Options: Privacy

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

Figure 93 Pop-up Blocker Settings

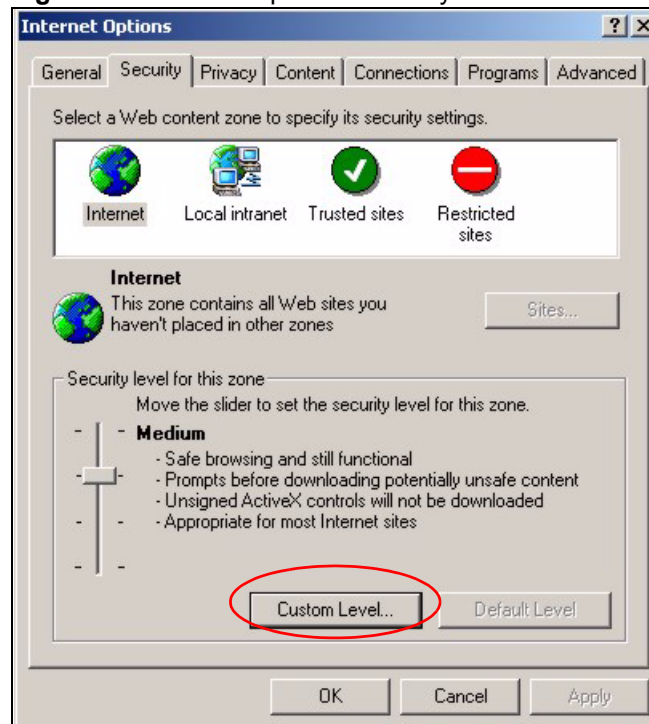
- 5 Click **Close** to return to the **Privacy** screen.
- 6 Click **Apply** to save this setting.

JavaScripts

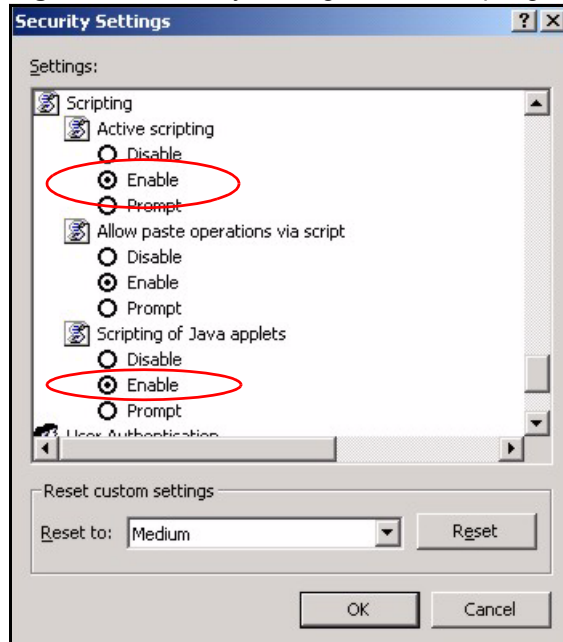
If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

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

Figure 94 Internet Options: Security

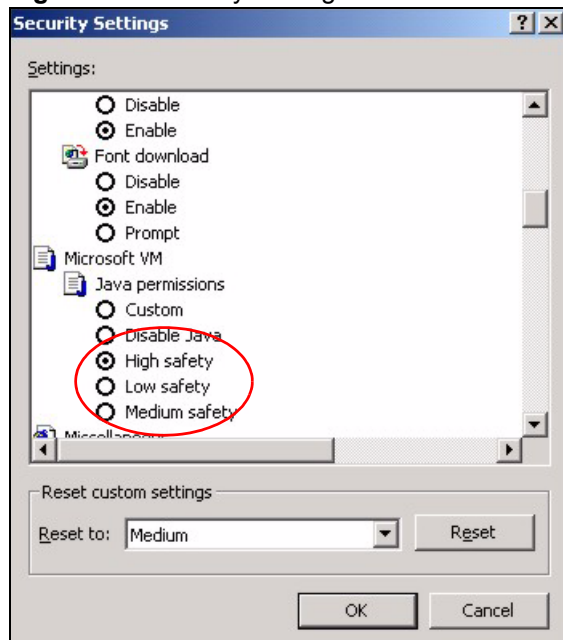


- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Scripting**.
- 4 Under **Active scripting** make sure that **Enable** is selected (the default).
- 5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).
- 6 Click **OK** to close the window.

Figure 95 Security Settings - Java Scripting

Java Permissions

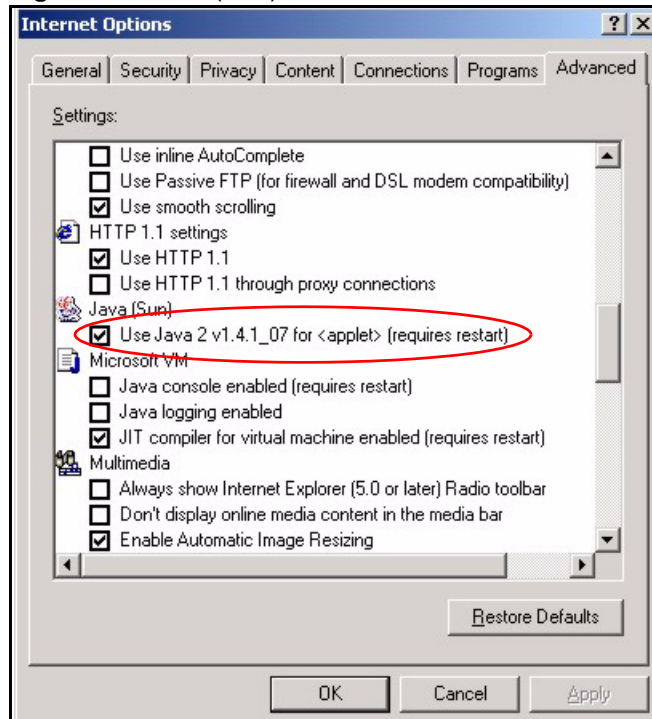
- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Microsoft VM**.
- 4 Under **Java permissions** make sure that a safety level is selected.
- 5 Click **OK** to close the window.

Figure 96 Security Settings - Java

JAVA (Sun)

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

Figure 97 Java (Sun)

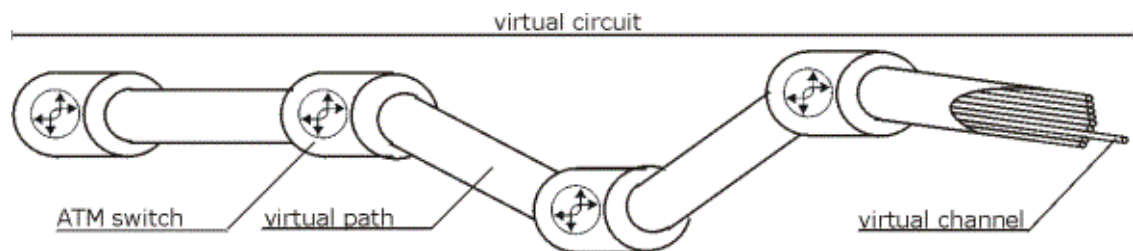


Virtual Circuit Topology

ATM is a connection-oriented technology, meaning that it sets up virtual circuits over which end systems communicate. The terminology for virtual circuits is as follows:

- Virtual Channel Logical connections between ATM switches
- Virtual Path A bundle of virtual channels
- Virtual Circuits A series of virtual paths between circuit end point

Figure 98 Virtual Circuit Topology



Think of a virtual path as a cable that contains a bundle of wires. The cable connects two points and wires within the cable provide individual circuits between the two points. In an ATM cell header, a VPI (Virtual Path Identifier) identifies a link formed by a virtual path; a VCI (Virtual Channel Identifier) identifies a channel within a virtual path.

The VPI and VCI identify a virtual path, that is, termination points between ATM switches. A series of virtual paths make up a virtual circuit.

Legal Information

Copyright

Copyright © 2006 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- 1 Reorient or relocate the receiving antenna.
- 2 Increase the separation between the equipment and the receiver.
- 3 Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- 4 Consult the dealer or an experienced radio/TV technician for help.

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Viewing Certifications

- 1 Go to <http://www.zyxel.com>.
- 2 Select your product on the ZyXEL home page to go to that product's page.
- 3 Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of

ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Customer Support

Please have the following information ready when you contact customer support.

Required Information

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

Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web Site: www.zyxel.com, www.europe.zyxel.com
- FTP Site: [ftp.zyxel.com](ftp://ftp.zyxel.com), [ftp.europe.zyxel.com](ftp://ftp.europe.zyxel.com)
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web Site: www.zyxel.co.cr
- FTP Site: [ftp.zyxel.co.cr](ftp://ftp.zyxel.co.cr)
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web Site: www.zyxel.cz
- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Česká Republika

Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web Site: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780 8448
- Web Site: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web Site: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-0
- Fax: +49-2405-6909-99
- Web Site: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web Site: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

Kazakhstan

- Support: <http://zyxel.kz/support>
- Sales E-mail: sales@zyxel.kz

- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web Site: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43, Dostyk ave., Office 414, Dostyk Business Centre, 050010, Almaty, Republic of Kazakhstan

North America

- Support E-mail: support@zyxel.com
- Sales E-mail: sales@zyxel.com
- Telephone: +1-800-255-4101, +1-714-632-0882
- Fax: +1-714-632-0858
- Web Site: www.us.zyxel.com
- FTP Site: <ftp.us.zyxel.com>
- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web Site: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48 (22) 333 8250
- Fax: +48 (22) 333 8251
- Web Site: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Russia

- Support: <http://zyxel.ru/support>
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web Site: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow, 117279, Russia

Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345

- Web Site: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web Site: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web Site: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev, 04050, Ukraine

United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344 303044, 08707 555779 (UK only)
- Fax: +44-1344 303034
- Web Site: www.zyxel.co.uk
- FTP Site: [ftp.zyxel.co.uk](ftp://ftp.zyxel.co.uk)
- Regular Mail: ZyXEL Communications UK, Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)

“+” is the (prefix) number you dial to make an international telephone call.

Index

A

address mapping [98](#)
Address Resolution Protocol (ARP) [56](#)
ADSL standards [26](#)
alternative subnet mask notation [143](#)
Any IP [56](#)
 How it works [56](#)
Any IP Setup [58](#)
Any IP table [107](#)
applications [25](#)
ATM Adaptation Layer 5 (AAL5) [37](#)

B

Backup [112](#)
Backup Type [66](#)

C

CBR (Constant Bit Rate) [63](#)
certifications [157](#)
 notices [158](#)
 viewing [158](#)
change password at login [30](#)
compact guide [29](#)
Configuration [45](#), [106](#)
contact information [161](#)
copyright [157](#)
customer support [161](#)

D

Default [114](#)
default LAN IP address [29](#)
default user name and password [29](#)
DHCP [45](#), [54](#), [71](#), [106](#), [107](#)
DHCP server [106](#)
DHCP table [107](#)

diagnostic [108](#)
disclaimer [157](#)
DNS [54](#)
Domain Name [95](#)
domain name system
 see DNS
DSL line, reinitialize [109](#)
Dynamic DNS [71](#)
DYNDNS Wildcard [71](#)

E

ECHO [95](#)
embedded help [32](#)
Encapsulated Routing Link Protocol (ENET ENCAP)
 [37](#)
Encapsulation [37](#)
 ENET ENCAP [37](#)
 PPP over Ethernet [37](#)
 PPPoA [37](#)
 RFC 1483 [38](#)
Ethernet [121](#)

F

Factory Defaults [114](#)
Factory LAN Defaults [54](#)
FCC interference statement [157](#)
Finger [95](#)
firmware [110](#)
 upload [110](#)
 upload error [111](#)
FTP [75](#), [95](#)
FTP Restrictions [75](#)

H

Host [51](#)
HTTP [95](#)
HTTP (Hypertext Transfer Protocol) [110](#)

I

IANA [40](#), [148](#)
IGMP [55](#)
Install UPnP [80](#)
 Windows Me [81](#)
 Windows XP [82](#)
Internet Access [25](#)
Internet access [37](#)
Internet access wizard setup [38](#)
Internet Assigned Numbers Authority
 See IANA
IP Address [39](#), [54](#), [95](#), [107](#)
IP Address Assignment [39](#)
 ENET ENCAP [40](#)
 PPPoA or PPPoE [40](#)
 RFC 1483 [40](#)
IP Policy Routing (IPPR) [122](#)
IP Pool Setup [45](#)

L

LAN Setup [53](#), [59](#)
LAN TCP/IP [54](#)

M

MAC (Media Access Control) [107](#)
maintenance [103](#)
management idle timeout period [30](#)
managing the device
 good habits [27](#)
 using FTP. See FTP.
 using Telnet. See command interface.
 using the command interface. See command interface.
Maximum Burst Size (MBS) [60](#), [63](#)
Metric [59](#)
Multicast [55](#)
Multiplexing [38](#)
multiplexing [38](#)
 LLC-based [38](#)
 VC-based [38](#)
Multiprotocol Encapsulation [38](#)

N

Nailed-Up Connection [40](#)
NAT [95](#), [96](#), [148](#)
 Address mapping rule [99](#)
 Application [93](#)
 Definitions [91](#)
 How it works [92](#)
 Mapping Types [93](#)
 What it does [92](#)
 What NAT does [92](#)
NAT (Network Address Translation) [91](#)
NAT mode [96](#)
NAT Traversal [79](#)
navigating the web configurator [31](#)
Network Management [95](#)
NNTP [95](#)

P

Password [51](#)
Peak Cell Rate (PCR) [60](#), [63](#)
Point to Point Protocol over ATM Adaptation Layer 5 (AAL5) [37](#)
Point-to-Point Tunneling Protocol [95](#)
POP3 [95](#)
Port Numbers [95](#)
PPP session over Ethernet (PPP over Ethernet, RFC 2516) [37](#)
PPPoE [60](#)
 Benefits [60](#)
PPPoE (Point-to-Point Protocol over Ethernet) [60](#)
PPTP [95](#)
product registration [159](#)
PVC (Permanent Virtual Circuit) [37](#)

R

registration
 product [159](#)
reinitialize the ADSL line [109](#)
related documentation [3](#)
remote management
 Telnet [76](#)
Remote Management and NAT [76](#)
Remote Management Limitations [75](#)
Restore [112](#)

RFC 1483 [38](#)
RFC 1631 [91](#)
RIP [55](#)
Routing Information Protocol [55](#)
 Direction [55](#)
 see RIP
 Version [55](#)

S

safety warnings [6](#)
Server [93, 94](#)
Services [95](#)
SMTP [95](#)
SNMP [95](#)
SUA [94, 96](#)
SUA (Single User Account) [94](#)
SUA server [95, 97](#)
 Default server set [95](#)
SUA vs NAT [94](#)
SUA/NAT Server Set [98](#)
subnet [141](#)
Subnet Mask [39, 54](#)
subnet mask [142](#)
subnetting [144](#)
Sustain Cell Rate (SCR) [63](#)
Sustained Cell Rate (SCR) [60](#)
syntax conventions [4](#)
System Timeout [76](#)

T

Telnet [76](#)
TFTP Restrictions [75](#)
trademarks [157](#)
Traffic Redirect [64, 65](#)
Traffic redirect [64](#)
traffic redirect [122](#)
Traffic shaping [60](#)

U

UBR (Unspecified Bit Rate) [63](#)
Universal Plug and Play [79](#)
 Application [79](#)

UPnP [79](#)
 Forum [80](#)
 security issues [79](#)
User Name [72](#)

V

VBR (Variable Bit Rate) [63](#)
Virtual Channel Identifier (VCI) [38](#)
virtual circuit (VC) [38](#)
Virtual Path Identifier (VPI) [38](#)
VPI & VCI [38](#)

W

WAN (Wide Area Network) [59](#)
WAN backup [65](#)
warranty [158](#)
 note [158](#)
Web Configurator [29, 31, 32](#)
web configurator screen summary [32](#)

