

# P-660R-F1 Series

*ADSL2+ Router*

## *User's Guide*

### Default Login Details

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

Version 3.70  
Edition 1, 05/2011

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

The logo for ZyXEL, featuring the word "ZyXEL" in a bold, blue, sans-serif font. The "Zy" is in a smaller font size than "XEL".



---

# 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.

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

- Supporting Disc

Refer to the included CD for support documents.

- ZyXEL Web Site

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

## User Guide Feedback

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

The Technical Writing Team,

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

## Disclaimer

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

---

# Document Conventions

## Warnings and Notes

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

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

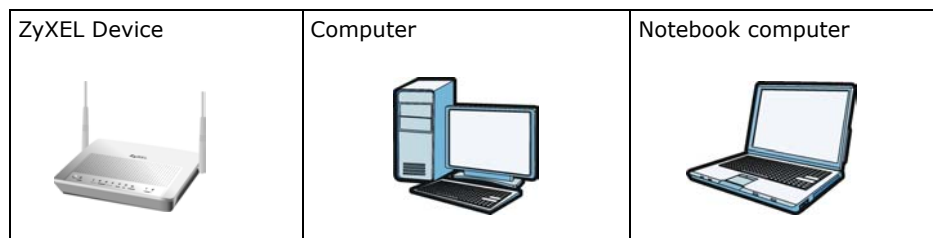
Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

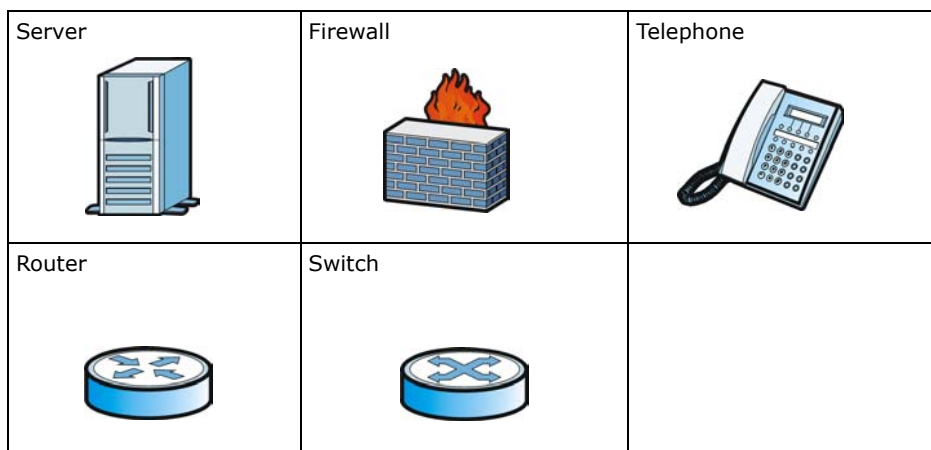
## Syntax Conventions

- The P-660R-F1 may be referred to as the "ZyXEL Device", the "device", the "system" or the "product" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket ( > ) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

## Icons Used in Figures

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





## Copyright

Copyright © 2011 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**

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

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

### **Notice 1**

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.

### **FCC Caution**

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

### **Viewing Certifications**

- 1 Go to [www.zyxel.com](http://www.zyxel.com)
- 2 Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.

Select the certification you wish to view from this page.

# 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 source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- This device is for indoor use only (utilisation intérieure exclusivement).

This product is recyclable. Dispose of it properly.







---

# Table of Contents

<b>About This User's Guide</b> .....	<b>3</b>
<b>Document Conventions</b> .....	<b>4</b>
<b>Copyright</b> .....	<b>5</b>
<b>Certifications</b> .....	<b>5</b>
<b>Safety Warnings</b> .....	<b>7</b>
<b>Table of Contents</b> .....	<b>9</b>
<b>Contents Overview</b> .....	<b>17</b>
<b>Chapter 1</b>	
<b>Getting To Know Your ZyXEL Device</b> .....	<b>19</b>
1.1 Introducing the ZyXEL Device .....	19
1.2 Features .....	20
1.3 Applications for the ZyXEL Device .....	21
1.3.1 Internet Access .....	22
1.3.2 LAN to LAN Application .....	22
1.4 Front Panel Lights .....	22
1.5 Hardware Connection .....	23
<b>Chapter 2</b>	
<b>Introducing the Web Configurator</b> .....	<b>24</b>
2.1 Web Configurator Overview .....	24
2.2 Accessing the Web Configurator .....	24
2.3 Resetting the ZyXEL Device .....	26
2.3.1 Using the Reset Button .....	26
2.4 Navigating the Web Configurator .....	26
2.4.1 Navigation Panel .....	26
2.4.2 Status Screen .....	28
2.4.3 Status: Any IP Table .....	30
2.4.4 Status: Packet Statistics .....	31
2.4.5 Changing Login Password .....	32
<b>Chapter 3</b>	
<b>Wizard Setup for Internet Access</b> .....	<b>34</b>
3.1 Introduction .....	34
3.2 Internet Access Wizard Setup .....	34
3.2.1 Automatic Detection .....	35

---

3.2.2 Manual Configuration .....	36
----------------------------------	----

**Chapter 4**  
**WAN Setup .....** **43**

4.1 WAN Overview .....	43
4.1.1 Encapsulation .....	43
4.1.2 Multiplexing .....	44
4.1.3 Encapsulation and Multiplexing Scenarios .....	44
4.1.4 VPI and VCI .....	45
4.1.5 IP Address Assignment .....	45
4.1.6 Nailed-Up Connection (PPP) .....	45
4.1.7 NAT .....	46
4.2 Metric .....	46
4.3 Traffic Shaping .....	46
4.3.1 ATM Traffic Classes .....	47
4.4 Zero Configuration Internet Access .....	48
4.5 Internet Access Setup Screen .....	48
4.5.1 Configuring Advanced Internet Connection Setup .....	52
4.6 Configuring More Connections .....	54
4.6.1 More Connections Edit .....	55
4.6.2 Configuring More Connections Advanced Setup .....	57
4.7 Traffic Redirect .....	58
4.8 Configuring WAN Backup .....	60

**Chapter 5**  
**LAN Setup .....** **63**

5.1 LAN Overview .....	63
5.1.1 LANs, WANs and the ZyXEL Device .....	63
5.1.2 DHCP Setup .....	63
5.1.3 DNS Server Address .....	64
5.1.4 DNS Server Address Assignment .....	64
5.2 LAN TCP/IP .....	65
5.2.1 IP Address and Subnet Mask .....	65
5.2.2 RIP Setup .....	66
5.2.3 Multicast .....	66
5.2.4 Any IP .....	67
5.3 Configuring LAN IP .....	68
5.3.1 Configuring Advanced LAN Setup .....	69
5.4 DHCP Setup .....	70
5.5 LAN Client List .....	71
5.6 LAN IP Alias .....	72

**Chapter 6**  
**Network Address Translation (NAT) Screens.....** **75**

6.1 NAT Overview .....	75
6.1.1 NAT Definitions .....	75
6.1.2 What NAT Does .....	76
6.1.3 How NAT Works .....	76
6.1.4 NAT Application .....	77
6.1.5 NAT Mapping Types .....	77
6.2 SUA (Single User Account) Versus NAT .....	78
6.3 NAT General Setup .....	79
6.4 Port Forwarding .....	80
6.4.1 Default Server IP Address .....	80
6.4.2 Port Forwarding: Services and Port Numbers .....	80
6.4.3 Configuring Servers Behind Port Forwarding (Example) .....	81
6.5 Configuring Port Forwarding .....	81
6.5.1 Port Forwarding Rule Edit .....	82
6.6 The SIP ALG Screen .....	83
6.7 DMZ Hosting .....	84

**Chapter 7**  
**Firewalls ..... 85**

7.1 Overview .....	85
7.1.1 What You Can Do in the Firewall Screens .....	85
7.1.2 What You Need to Know About Firewall .....	85
7.1.3 Firewall Rule Setup Example .....	86
7.2 The Firewall General Screen .....	89
7.3 The Firewall Rule Screen .....	90
7.3.1 Configuring Firewall Rules .....	93
7.3.2 Customized Services .....	94
7.3.3 Configuring a Customized Service .....	95
7.4 The Firewall Threshold Screen .....	96
7.4.1 Threshold Values .....	97
7.4.2 Configuring Firewall Thresholds .....	97
7.5 Firewall Technical Reference .....	99
7.5.1 Firewall Rules Overview .....	99
7.5.2 Guidelines For Enhancing Security With Your Firewall .....	100
7.5.3 Security Considerations .....	100
7.5.4 Triangle Route .....	101

**Chapter 8**  
**Packet Filters ..... 105**

8.1 Overview .....	105
8.1.1 What You Can Do in the Packet Filter Screen .....	105
8.1.2 What You Need to Know About the Packet Filter .....	105
8.2 The Packet Filter Screen .....	105

8.2.1 Editing Protocol Filters .....	106
8.2.2 Configuring Protocol Filter Rules .....	107
8.2.3 Editing Generic Filters .....	109
8.2.4 Configuring Generic Packet Rules .....	111
8.3 Packet Filter Technical Reference .....	112
8.3.1 Filter Types and NAT .....	112
8.3.2 Firewall Versus Filters .....	112
<b>Chapter 9</b>	
<b>Certificates .....</b>	<b>115</b>
9.1 Overview .....	115
9.1.1 What You Can Do in the Certificates Screens .....	115
9.1.2 What You Need to Know About Certificates .....	115
9.2 The My Certificates Screen .....	117
9.2.1 My Certificate Import .....	118
9.2.2 My Certificate Create .....	120
9.2.3 My Certificate Details .....	122
9.3 The Trusted CAs Screen .....	125
9.3.1 Trusted CA Import .....	127
9.3.2 Trusted CA Details .....	128
9.4 The Trusted Remote Hosts Screens .....	130
9.4.1 Trusted Remote Hosts Import .....	131
9.4.2 Trusted Remote Host Certificate Details .....	132
9.5 The Directory Servers Screens .....	135
9.5.1 Directory Server Add and Edit .....	136
9.6 Certificates Technical Reference .....	137
9.6.1 Certificates Overview .....	137
9.6.2 Private-Public Certificates .....	138
9.6.3 Verifying a Trusted Remote Host's Certificate .....	138
<b>Chapter 10</b>	
<b>Static Route .....</b>	<b>141</b>
10.1 Static Route .....	141
10.2 Configuring Static Route .....	142
10.2.1 Static Route Edit .....	143
<b>Chapter 11</b>	
<b>Quality Of Service .....</b>	<b>145</b>
11.1 Overview .....	145
11.1.1 What You Can Do in the QoS Screens .....	145
11.1.2 What You Need to Know About QoS .....	145
11.1.3 QoS Class Setup Example .....	146
11.2 The QoS General Screen .....	149

11.3 The Class Setup Screen .....	151
11.3.1 The Class Configuration Screen .....	152
11.4 The QoS Monitor Screen .....	155
11.5 QoS Technical Reference .....	156
11.5.1 IEEE 802.1Q Tag .....	156
11.5.2 IP Precedence .....	156
11.5.3 DiffServ .....	157
11.5.4 Automatic Priority Queue Assignment .....	157
<b>Chapter 12</b>	
<b>Dynamic DNS Setup .....</b>	<b>159</b>
12.1 Dynamic DNS Overview .....	159
12.1.1 DYNDNS Wildcard .....	159
12.2 Configuring Dynamic DNS .....	159
<b>Chapter 13</b>	
<b>Remote Management Configuration .....</b>	<b>163</b>
13.1 Remote Management Overview .....	163
13.1.1 Remote Management Limitations .....	163
13.1.2 Remote Management and NAT .....	163
13.1.3 System Timeout .....	164
13.2 The WWW Screen .....	164
13.2.1 WWW and HTTPS .....	164
13.3 Telnet .....	167
13.4 Configuring Telnet .....	167
13.5 Configuring FTP .....	168
13.6 SNMP .....	169
13.6.1 Supported MIBs .....	170
13.6.2 SNMP Traps .....	170
13.6.3 Configuring SNMP .....	171
13.7 Configuring DNS .....	172
13.8 Configuring ICMP .....	173
<b>Chapter 14</b>	
<b>Universal Plug-and-Play (UPnP).....</b>	<b>174</b>
14.1 Introducing Universal Plug and Play .....	174
14.1.1 How do I know if I'm using UPnP? .....	174
14.1.2 NAT Traversal .....	174
14.1.3 Cautions with UPnP .....	174
14.2 UPnP and ZyXEL .....	175
14.2.1 Configuring UPnP .....	175
14.3 Installing UPnP in Windows Example .....	176
14.3.1 Installing UPnP in Windows Me .....	176

14.3.2 Installing UPnP in Windows XP .....	177
14.4 Using UPnP in Windows XP Example .....	179
14.4.1 Auto-discover Your UPnP-enabled Network Device .....	179
14.4.2 Web Configurator Easy Access .....	182
<b>Chapter 15</b>	
<b>System .....</b>	<b>185</b>
15.1 General Setup .....	185
15.1.1 General Setup and System Name .....	185
15.1.2 General Setup .....	185
15.2 Time Setting .....	187
<b>Chapter 16</b>	
<b>Logs .....</b>	<b>191</b>
16.1 Overview .....	191
16.1.1 What You Can Do in the Log Screens .....	191
16.1.2 What You Need To Know About Logs .....	191
16.2 The View Log Screen .....	191
16.3 The Log Settings Screen .....	193
16.4 SMTP Error Messages .....	195
16.4.1 Example E-mail Log .....	195
16.5 Log Descriptions .....	197
<b>Chapter 17</b>	
<b>Tools .....</b>	<b>205</b>
17.1 Firmware Upgrade .....	205
17.2 Configuration Screen .....	207
17.2.1 Backup Configuration .....	207
17.2.2 Restore Configuration .....	207
17.2.3 Back to Factory Defaults .....	208
17.3 Restart .....	209
<b>Chapter 18</b>	
<b>Diagnostic .....</b>	<b>210</b>
18.1 General Diagnostic .....	210
18.2 DSL Line Diagnostic .....	211
<b>Chapter 19</b>	
<b>Troubleshooting.....</b>	<b>213</b>
19.1 Problems Starting Up the ZyXEL Device .....	213
19.2 Problems with the LAN .....	213
19.3 Problems with the WAN .....	214
19.4 Problems Accessing the ZyXEL Device .....	215

---

Appendix A .....	217
Appendix A Product Specifications .....	217
Appendix B Wall-mounting Instructions .....	221
Appendix C Setting up Your Computer's IP Address.....	223
Appendix D IP Addresses and Subnetting.....	239
Appendix E Splitters and Microfilters .....	247
Appendix F Pop-up Windows, JavaScripts and Java Permissions.....	251
<b>Index .....</b>	<b>259</b>

---



---

# Contents Overview

Copyright .....	5
Certifications .....	5
Getting To Know Your ZyXEL Device .....	19
Introducing the Web Configurator .....	24
Wizard Setup for Internet Access.....	34
WAN Setup .....	43
LAN Setup .....	63
Network Address Translation (NAT) Screens .....	75
Firewalls .....	85
Packet Filters .....	105
Certificates .....	115
Static Route .....	141
Quality Of Service .....	145
Dynamic DNS Setup .....	159
Remote Management Configuration .....	163
Universal Plug-and-Play (UPnP) .....	174
System .....	185
Logs .....	191
Tools .....	205
Diagnostic .....	210
Troubleshooting .....	213

---

# Getting To Know Your ZYXEL DEVICE

This chapter describes the key features and applications of your ZyXEL Device.

## 1.1 Introducing the ZyXEL Device

The ZyXEL Device is an ADSL2+ gateway that allows super-fast Internet access over analog (POTS) or digital (ISDN) telephone lines (depending on your model).

In the ZyXEL Device product name, "R" denotes an integrated router and "F" denotes a chip set standard.

Your ZyXEL Device product name ends with a number. Models ending in "1", for example P-660R-F1, denote a device that works over the analog telephone system, POTS (Plain Old Telephone Service). Models ending in "3" denote a device that works over ISDN (Integrated Services Digital Network). Models ending in "7" denote a device that works over T-ISDN (UR-2).

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

## 1.2 Features

### High Speed Internet Access

The DSL RJ-11 (ADSL over POTS models) or RJ-45 (ADSL over ISDN models) connects to your ADSL-enabled telephone line. The ZyXEL Device is compatible with the ADSL/ADSL2/ADSL2+ standards. 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

Note: 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.

### Zero Configuration Internet Access

Once you connect and turn on the ZyXEL Device, 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.

### Any IP

The Any IP feature allows a computer to access the Internet and the ZyXEL Device 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.

### Traffic Redirect

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.

### Universal Plug and Play (UPnP)

Using the standard TCP/IP protocol, the ZyXEL Device and other UPnP enabled devices can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.

## PPPoE (RFC2516)

PPPoE (Point-to-Point Protocol over Ethernet) emulates a dial-up connection. It allows your ISP to use their existing network configuration with newer broadband technologies such as ADSL. The PPPoE driver on the ZyXEL Device is transparent to the computers on the LAN, which see only Ethernet and are not aware of PPPoE thus saving you from having to manage PPPoE clients on individual computers. The ZyXEL Device also includes PPPoE idle time-out (the PPPoE connection terminates after a period of no traffic that you configure) and PPPoE Dial-on-Demand (the PPPoE connection is brought up only when an Internet access request is made).

## Network Address Translation (NAT)

Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).

## Dynamic DNS Support

With Dynamic DNS support, you can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessible from various locations on the Internet. You must register for this service with a Dynamic DNS service provider.

## DHCP

DHCP (Dynamic Host Configuration Protocol) allows the individual clients (computers) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The ZyXEL Device has built-in DHCP server capability enabled by default. It can assign IP addresses, an IP default gateway and DNS servers to DHCP clients. The ZyXEL Device can now also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients.

## IP Alias

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

## Housing

Your ZyXEL Device's compact and ventilated housing minimizes space requirements making it easy to position anywhere in your busy office.

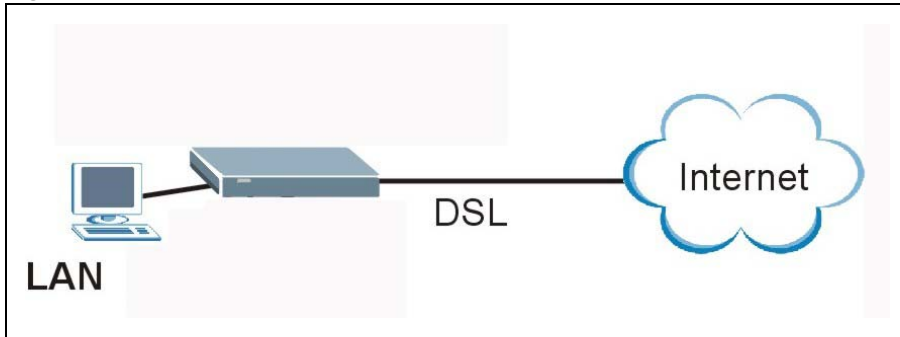
# 1.3 Applications for the ZyXEL Device

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

### 1.3.1 Internet Access

The ZyXEL Device is the ideal high-speed Internet access solution. It is compatible with all major ADSL DSLAM (Digital Subscriber Line Access Multiplexer) providers and supports the ADSL standards as shown in [Table 1 on page 20](#).

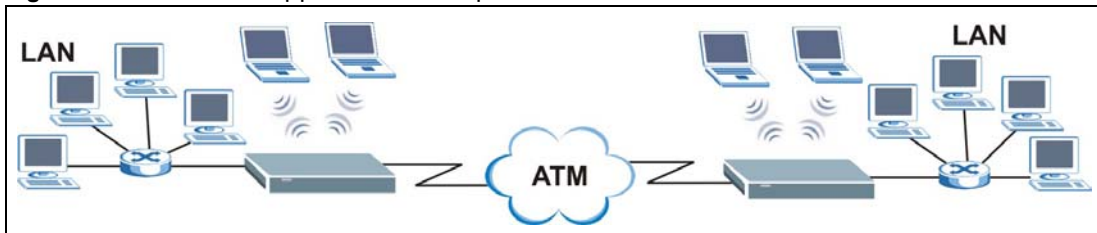
**Figure 1** Internet Access Applications



### 1.3.2 LAN to LAN Application

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

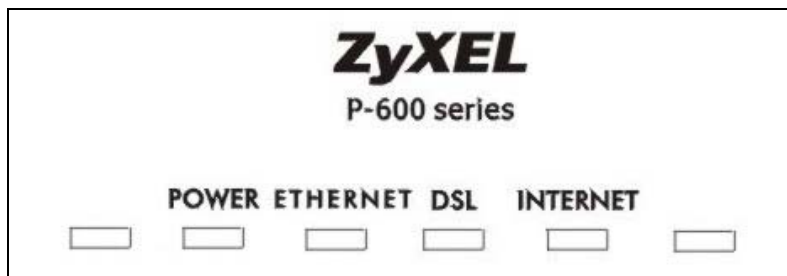
**Figure 2** LAN-to-LAN Application Example



## 1.4 Front Panel Lights

The following figure shows the front panel lights.

**Figure 3** Front Panel (P-660R-F1)



The following table describes the lights.

**Table 2** Front Panel Lights

LIGHT	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The ZyXEL Device is receiving power and functioning properly.
		Blinking	The ZyXEL Device is rebooting or performing diagnostics.
	Red	On	Power to the ZyXEL Device is too low.
		Off	The ZyXEL Device is turned off. The system is not receiving power.
ETHERNET	Green	On	The ZyXEL Device has a successful 10Mbps Ethernet connection.
		Blinking	The ZyXEL Device is receiving or sending data.
	Amber	On	The ZyXEL Device has a successful 100Mbps Ethernet connection.
		Blinking	The ZyXEL Device is receiving or sending data.
		Off	The ZyXEL Device is not connected to the LAN.
DSL	Green	On	The DSL line is up.
		Blinking	The ZyXEL Device is initializing the DSL line.
		Off	The DSL line is down.
INTERNET	Green	On	The Internet connection is up.
		Blinking	The ZyXEL Device is sending/receiving data.
		Off	The Internet connection is down.

## 1.5 Hardware Connection

Refer to the Quick Start Guide for information on hardware 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 ZyXEL Device setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

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

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

See the chapter on troubleshooting if you need to make sure these functions are allowed in Internet Explorer.

## 2.2 Accessing the Web Configurator

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



- 5 A window displays as shown. Enter the default admin password **1234** to configure the wizards and the advanced features or enter the default user password **user** to view the status only. Click **Login** to proceed to a screen asking you to change your password or click **Cancel** to revert to the default password.

**Figure 4** Password Screen



- 6 If you entered the user password, skip the next two steps and refer to [Section 2.4.2 on page 28](#) for more information about the **Status** screen.

If you entered the admin password, it is highly recommended you change the default admin password! Enter a new password between 1 and 30 characters, 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.

Note: If you do not change the password at least once, the following screen appears every time you log in with the admin password.

**Figure 5** Change Password at Login



Note: The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes). Simply log back into the ZyXEL Device if this happens to you.

## 2.3 Resetting the ZyXEL Device

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the ZyXEL Device to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the password will be reset to "1234".

### 2.3.1 Using the Reset Button

- 1 Make sure the **POWER** light is on (not blinking).
- 2 Press the **RESET** button for ten seconds or until the **POWER** light begins to blink and then release it. When the **POWER** light begins to blink, the defaults have been restored and the ZyXEL Device restarts.

## 2.4 Navigating the Web Configurator

We use the P-660R-F1 web screens in this guide as an example. Screens vary slightly for different ZyXEL Device models.

### 2.4.1 Navigation Panel

After you enter the admin password, use the sub-menus on the navigation panel to configure ZyXEL Device features. The following table describes the sub-menus.


**Figure 6** Web Configurator: Main Screen

The screenshot shows the ZyXEL Web Configurator main screen. On the left is a navigation panel with sub-menus: Network, Security, Advanced, and Maintenance. The main content area is divided into several sections:



- Device Information:** Host Name: r35, Model Number: P-660R-F1, MAC Address: 00:19:cb:02:56:69, ZyNOS Firmware Version: 3.70(VBE\_01b2 | 05/05/2011), DSL Firmware Version: Amazon\_se\_ADSL 3.4.4.10.0.1 26/2 5:9, WAN Information: - DSL Mode: NORMAL, - IP Address: 167.97.12.23, 0.0.0.0, N/A, 8/35, 192.168.1.1, 255.255.255.0, Server, Enabled.
- System Status:** System Uptime, Current Date, System Mode: Routing / Bridging, CPU Usage: 6.72%, Memory Usage: 53%.
- Interface Status:**

Interface	Status	Rate
DSL	Down	0 kbps / 0 kbps
LAN	Up	100M/Full Duplex
- Summary:** Client List, Packet Statistics, AnyIP Table.

Annotations in the image include a red circle around the navigation panel with the text "Use submenus to configure ZyXEL Device features." and a red arrow pointing to the Logout icon with the text "Click the Logout icon at any time to exit the web".

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

**Table 3** Web Configurator Screens Summary

LINK/ICON	SUB-LINK	FUNCTION
Wizard 	INTERNET SETUP	Use these screens for initial configuration including general setup, ISP parameters for Internet Access and WAN IP/DNS Server/MAC address assignment.
Logout 		Click this icon to exit the web configurator.
Status		This screen shows the ZyXEL Device's general device, system and interface status information. Use this screen to access the summary statistics tables.
Network		
WAN	Internet Connection	This screen allows you to configure ISP parameters, WAN IP address assignment, DNS servers and other advanced properties.
	More Connections	Use this screen to view and configure other connections for placing calls to another remote gateway.
	WAN Backup Setup	Use this screen to configure your traffic redirect properties and WAN backup settings.
LAN	IP	Use this screen to configure LAN TCP/IP settings, enable Any IP and other advanced properties.
	DHCP Setup	Use this screen to configure LAN DHCP settings.
	Client List	Use this screen to view current DHCP client information and to always assign an IP address to a MAC address (and host name).
	IP Alias	Use this screen to partition your LAN interface into subnets.
NAT	General	Use this screen to enable NAT.
	Port Forwarding	Use this screen to configure servers behind the ZyXEL Device.
Advanced		
Static Route		Use this screen to configure IP static routes.
Dynamic DNS		Use this screen to set up dynamic DNS.
Remote MGMT	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTPS or HTTP to manage the ZyXEL Device.
	Telnet	Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the ZyXEL Device.
	FTP	Use this screen to configure through which interface(s) and from which IP address(es) users can use FTP to access the ZyXEL Device.
	SNMP	Use this screen to configure your ZyXEL Device's settings for Simple Network Management Protocol management.
	DNS	Use this screen to configure through which interface(s) and from which IP address(es) users can send DNS queries to the ZyXEL Device.
	ICMP	Use this screen to change your anti-probing settings.
UPnP		Use this screen to enable UPnP on the ZyXEL Device.

**Table 3** Web Configurator Screens Summary (continued)

LINK/ICON	SUB-LINK	FUNCTION
Maintenance		
System	General	This screen contains administrative and system-related information and also allows you to change your password.
	Time Setting	Use this screen to change your ZyXEL Device's time and date.
Tools	Firmware	Use this screen to upload firmware to your ZyXEL Device.
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your ZyXEL Device.
	Restart	This screen allows you to reboot the ZyXEL Device without turning the power off.
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.

## 2.4.2 Status Screen

The following summarizes how to navigate the web configurator from the **Status** screen. Some fields or links are not available if you entered the user password in the login password screen (see [Figure 4 on page 25](#)). Not all fields are available on all models.

**Figure 7** Status Screen

Refresh Interval:

Device Information	
Host Name:	<a href="#">ras</a>
Model Number:	P-660R-F1
MAC Address:	00:19:cb:02:56:69
ZyNOS Firmware Version:	<a href="#">3.70(VBE.0)b2   05/05/2011</a>
DSL Firmware Version:	Amazon_se_ADSL 3.4.4.10.0.1 26/2 5:9
WAN Information	
- DSL Mode:	NORMAL
- IP Address:	<a href="#">0.0.0.0</a>
- IP Subnet Mask:	0.0.0.0
- Default Gateway:	0.0.0.0
- VPI/VCI:	8/35
LAN Information	
- IP Address:	<a href="#">192.168.1.1</a>
- IP Subnet Mask:	255.255.255.0
- DHCP:	<a href="#">N/A</a>
Security	
- Firewall:	<a href="#">Enabled</a>

System Status	
System Uptime:	0:43:04
Current Date/Time:	01/01/2000 18:32:58
System Mode:	<a href="#">Routing / Bridging</a>
CPU Usage:	<div style="width: 7.19%;"></div> 7.19%
Memory Usage:	<div style="width: 54%;"></div> 54%

Interface Status		
Interface	Status	Rate
DSL	Down	0 kbps / 0 kbps
LAN	Up	100M/Full Duplex

Summary	
<a href="#">Client List</a>	<a href="#">AnyIP Table</a>
<a href="#">Packet Statistics</a>	

The following table describes the labels shown in the **Status** screen.

**Table 4** Status Screen

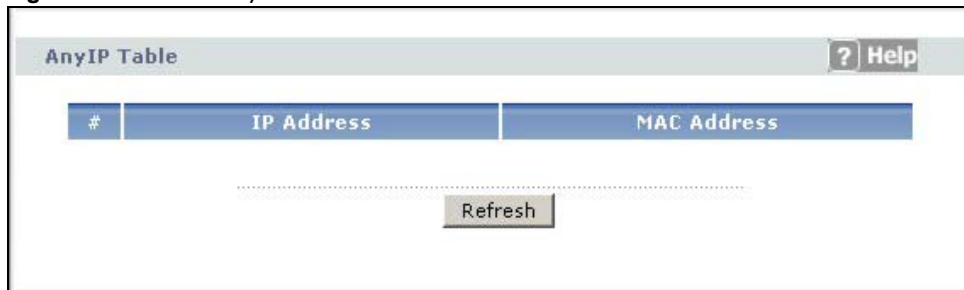
LABEL	DESCRIPTION
Refresh Interval	Select a number of seconds or <b>None</b> from the drop-down list box to refresh all screen statistics automatically at the end of every time interval or to not refresh the screen statistics.
Apply	Click this button to refresh the status screen statistics.
Device Information	
Host Name	This is the <b>System Name</b> you enter in the <b>Maintenance &gt; System &gt; General</b> screen. It is for identification purposes.
Model Number	This is your ZyXEL Device's model name.
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your ZyXEL Device.
ZyNOS Firmware Version	This is the ZyNOS Firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design.
WAN Information	
DSL Mode	This is the standard that your ZyXEL Device is using.
IP Address	This is the DSL port IP address.
IP Subnet Mask	This is the DSL port IP subnet mask.
Default Gateway	This is the IP address of the default gateway, if applicable.
VPI/VCI	This is the Virtual Path Identifier and Virtual Channel Identifier that you entered in the wizard or <b>WAN</b> screen.
LAN Information	
IP Address	This is the ETHERNET port IP address.
IP Subnet Mask	This is the ETHERNET port IP subnet mask.
DHCP	This is the ETHERNET port DHCP role - <b>Server, Relay</b> or <b>None</b> .
System Status	
System Uptime	This is the total time the ZyXEL Device has been on.
Current Date/Time	This field displays your ZyXEL Device's present date and time.
System Mode	This displays whether the ZyXEL Device is functioning as a router or a bridge.
CPU Usage	This number shows how many kilobytes of the heap memory the ZyXEL Device is using. Heap memory refers to the memory that is not used by ZyNOS (ZyXEL Network Operating System) and is thus available for running processes like NAT, VPN and the firewall.  The bar displays what percent of the ZyXEL Device's heap memory is in use. The bar turns from green to red when the maximum is being approached.
Memory Usage	This number shows the ZyXEL Device's total heap memory (in kilobytes).  The bar displays what percent of the ZyXEL Device's heap memory is in use. The bar turns from green to red when the maximum is being approached.
Interface Status	
Interface	This displays the ZyXEL Device port types.
Status	This field displays <b>Down</b> (line is down), <b>Up</b> (line is up or connected) if you're using Ethernet encapsulation and <b>Down</b> (line is down), <b>Up</b> (line is up or connected), <b>Idle</b> (line (ppp) idle), <b>Dial</b> (starting to trigger a call) and <b>Drop</b> (dropping a call) if you're using PPPoE encapsulation.

**Table 4** Status Screen

LABEL	DESCRIPTION
Rate	For the LAN ports, this displays the port speed and duplex setting. For the DSL port, it displays the downstream and upstream transmission rate.
Summary	
Any IP Table	Use this screen to view a list of IP addresses and MAC addresses of computers, which are not in the same subnet as the ZyXEL Device.
Packet Statistics	Use this screen to view port status and packet specific statistics.

### 2.4.3 Status: Any IP Table

Click the **Any IP Table** hyperlink in the **Status** screen. 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.

**Figure 8** Status: Any IP Table

The following table describes the labels in this screen.

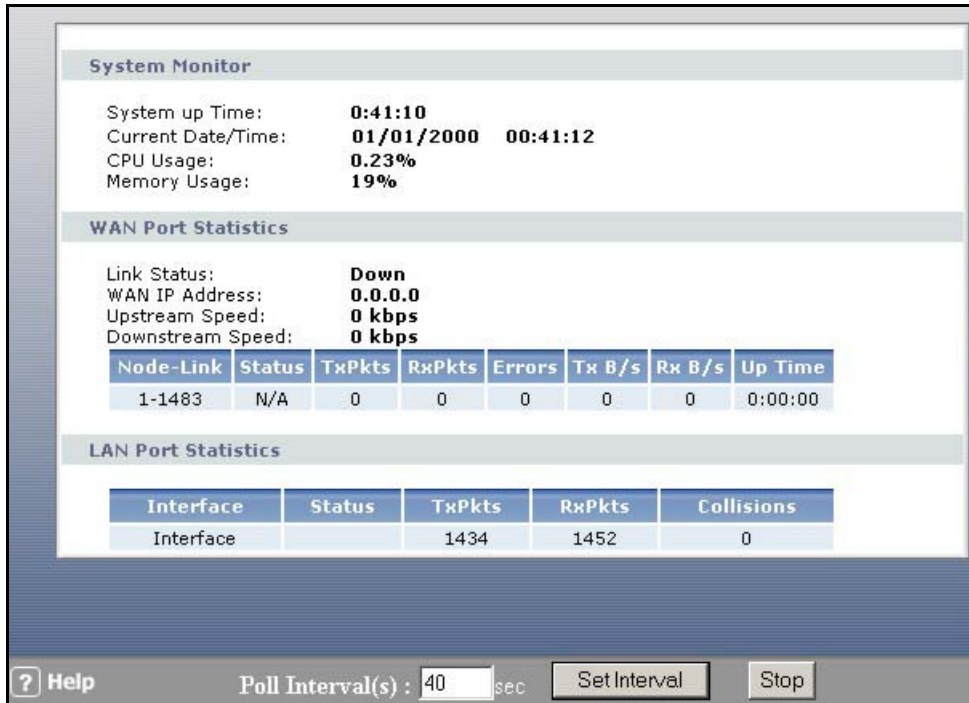
**Table 5** Status: Any IP Table

LABEL	DESCRIPTION
#	This is the index number of the host computer.
IP Address	This field displays the IP address of the network device.
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 <b>Refresh</b> to update this screen.

## 2.4.4 Status: Packet Statistics

Click the **Packet Statistics** hyperlink in the **Status** 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. Not all fields are available on all models

**Figure 9** Status: Packet Statistics



The following table describes the fields in this screen.

**Table 6** Status: Packet Statistics

LABEL	DESCRIPTION
System Monitor	
System up Time	This is the elapsed time the system has been up.
Current Date/Time	This field displays your ZyXEL Device's present date and time.
CPU Usage	This field specifies the percentage of CPU utilization.
Memory Usage	This field specifies the percentage of memory utilization.
LAN or WAN Port Statistics	
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.

**Table 6** Status: Packet Statistics (continued)

LABEL	DESCRIPTION
Status	This field displays <b>Down</b> (line is down), <b>Up</b> (line is up or connected) if you're using Ethernet encapsulation and <b>Down</b> (line is down), <b>Up</b> (line is up or connected), <b>Idle</b> (line (ppp) idle), <b>Dial</b> (starting to trigger a call) and <b>Drop</b> (dropping a call) if you're using PPPoE encapsulation.  For the WLAN port, it displays the transmission rate when WLAN is enabled or <b>N/A</b> when WLAN is disabled.
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.
Help	Click this button to bring the help screen.
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 <b>Poll Interval</b> field above.
Stop	Click this button to halt the refreshing of the system statistics.

## 2.4.5 Changing Login Password

It is highly recommended that you periodically change the password for accessing the ZyXEL Device. If you didn't change the default one after you logged in or you want to change to a new



password again, then click **Maintenance > System** to display the screen as shown next. See [Table 69 on page 186](#) for detailed field descriptions.

**Figure 10** System General

The screenshot shows a web configuration interface with two tabs: "General" (selected) and "Time Setting". The main content area is divided into two sections: "System Setup" and "Password".

**System Setup**

- System Name:
- Domain Name:
- Administrator Inactivity Timer:  (minutes, 0 means no timeout)

**Password**

The "Password" section contains two groups of fields, each enclosed in a red rounded rectangle:

- User Password:**
  - New Password:
  - Retype to confirm:
- Admin Password:**
  - Old Password:
  - New Password:
  - Retype to confirm:

**Caution:**  
Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.

At the bottom of the form are two buttons: "Apply" and "Cancel".

# Wizard Setup for Internet Access

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 given to you by your ISP.

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

## 3.2 Internet Access Wizard Setup


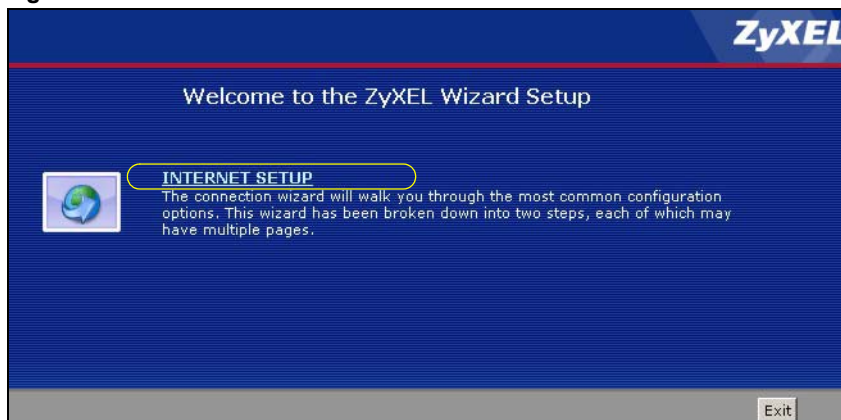
- 1 After you enter the admin password to access the web configurator, select **Go to Wizard setup** and click **Apply**. Otherwise, click the wizard icon (  ) in the top right corner of the web configurator to display the wizard main screen.
- 2 Click **INTERNET SETUP** to configure the system for Internet access.

Figure 11 Wizard: Welcome

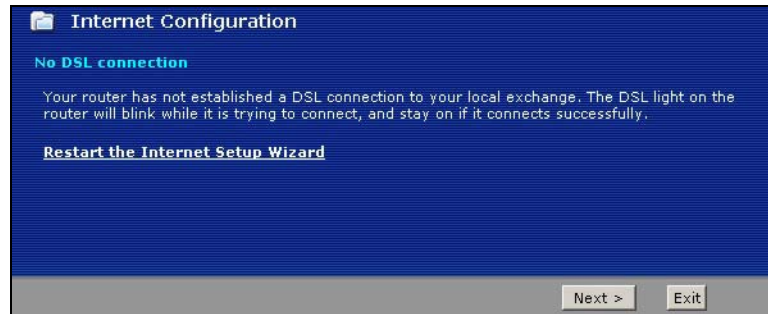


- The wizard attempts to detect which WAN connection type you are using.

If the wizard detects your connection type and your ISP uses PPPoE or PPPoA, go to [Section 3.2.1 on page 35](#). The screen varies depending on the connection type you use.

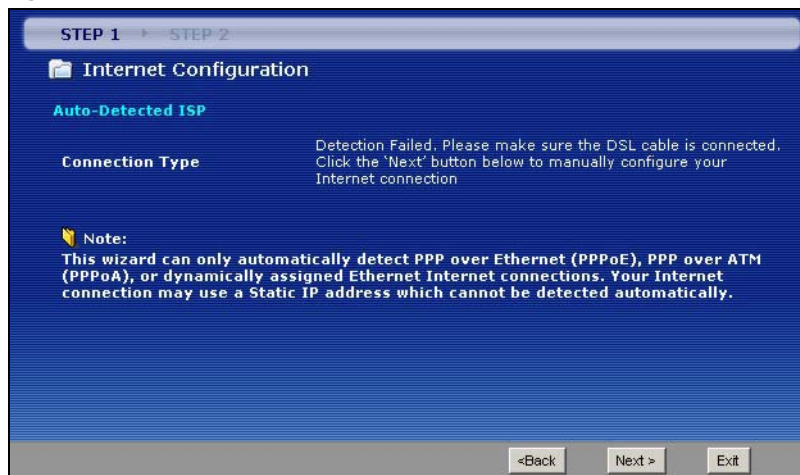
If the wizard does not detect a connection type and the following screen appears (see [Figure 12 on page 35](#)), check your hardware connections and click **Restart the Internet Setup Wizard** to have the ZyXEL Device detect your connection again.

**Figure 12** Auto Detection: No DSL Connection



If the wizard still cannot detect a connection type and the following screen appears (see [Figure 13 on page 35](#)), click **Next** and refer to [Section 3.2.2 on page 36](#) on how to configure the ZyXEL Device for Internet access manually.

**Figure 13** Auto Detection: Failed



## 3.2.1 Automatic Detection

- If you have a PPPoE or PPPoA connection, a screen displays prompting you to enter your Internet account information. Enter the username, password and/or service name exactly as provided.

- 2 Click **Next** to confirm your settings and test your connection.

**Figure 14** Auto-Detection: PPPoE

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

### 3.2.2 Manual Configuration

- 1 If the ZyXEL Device fails to detect your DSL connection type, enter the Internet access information given to you by your ISP exactly in the wizard screen. If not given, leave the fields set to the default.

**Figure 15** Internet Access Wizard Setup: ISP Parameters

The screenshot shows a wizard window titled "Internet Configuration" with a progress bar at the top indicating "STEP 1" and "STEP 2". Below the title is a folder icon and the text "Internet Configuration". Underneath, it says "ISP Parameters for Internet Access". The instruction reads: "Please verify the following settings with your Internet Service Provider (ISP). Your ISP may have given you a welcome letter or network setup letter including this information." There are four sections with dropdown menus: "Mode" (set to "Routing"), "Encapsulation" (set to "ENET ENCAP"), "Multiplexing" (set to "LLC"), and "Virtual Circuit ID" (with "VPI" set to "8" and "VCI" set to "35"). A note at the bottom states: "Select the VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) used by your ISP. The valid range for the VPI is 0 to 255 and VCI is 32 to 65535." At the bottom of the window are three buttons: "< Back", "Next >", and "Exit".

The following table describes the fields in this screen.

**Table 7** Internet Access Wizard Setup: ISP Parameters

LABEL	DESCRIPTION
Mode	From the <b>Mode</b> drop-down list box, select <b>Routing</b> (default) if your ISP allows multiple computers to share an Internet account. Otherwise select <b>Bridge</b> .
Encapsulation	Select the encapsulation type your ISP uses from the <b>Encapsulation</b> drop-down list box. Choices vary depending on what you select in the <b>Mode</b> field.  If you select <b>Bridge</b> in the <b>Mode</b> field, select either <b>PPPoA</b> or <b>RFC 1483</b> .  If you select <b>Routing</b> in the <b>Mode</b> field, select <b>PPPoA</b> , <b>RFC 1483</b> , <b>ENET ENCAP</b> or <b>PPPoE</b> .
Multiplexing	Select the multiplexing method used by your ISP from the <b>Multiplex</b> drop-down list box either VC-based or LLC-based.
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.
VPI	Enter the VPI assigned to you. This field may already be configured.
VCI	Enter the VCI assigned to you. This field may already be configured.
Back	Click <b>Back</b> to go back to the previous screen.
Next	Click <b>Next</b> to continue to the next wizard screen. The next wizard screen you see depends on what protocol you chose above.
Exit	Click <b>Exit</b> to close the wizard screen without saving your changes.

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

**Figure 16** Internet Connection with PPPoE

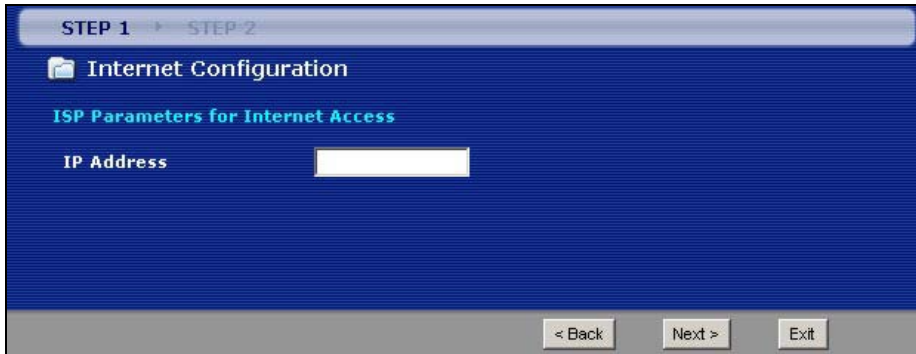
The screenshot shows a wizard window titled "Internet Configuration" with a progress bar at the top indicating "STEP 1" and "STEP 2". Below the title is a folder icon and the text "ISP Parameters for Internet Access". A message asks the user to enter their ISP-provided User Name, Password, and Service Name. There are three input fields corresponding to these fields. A "Note" icon is followed by text stating that the device is automatically configured to obtain an IP address. At the bottom, there are three buttons: "< Back", "Apply", and "Exit".

The following table describes the fields in this screen.

**Table 8** Internet Connection with PPPoE

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

**Figure 17** Internet Connection with RFC 1483



The following table describes the fields in this screen.

**Table 9** Internet Connection with RFC 1483

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

**Figure 18** Internet Connection with ENET ENCAP

STEP 1    STEP 2

Internet Configuration

ISP Parameters for Internet Access

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

Obtain an IP Address Automatically  
 Static IP Address

IP Address: 172.21.2.3  
 Subnet Mask: 255.0.0.0  
 Gateway IP address: 172.21.2.3  
 First DNS Server: 168.95.1.1  
 Second DNS Server: 0.0.0.0

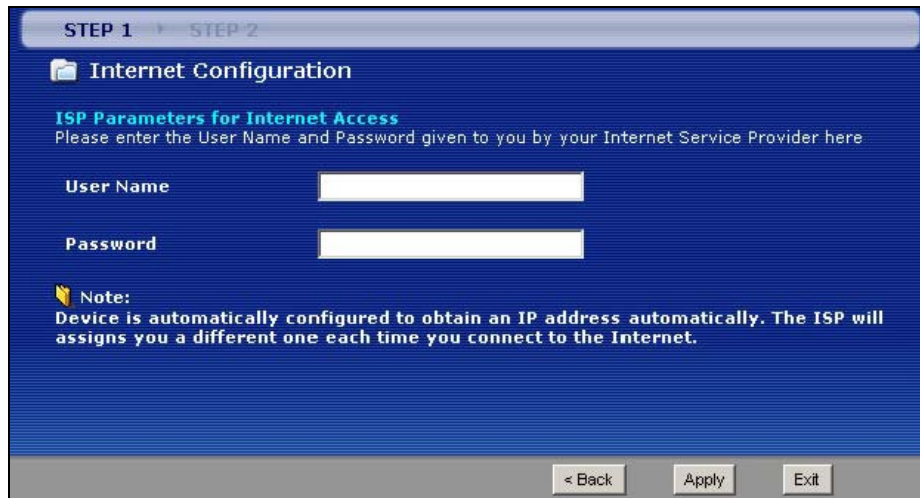
< Back    Apply >    Exit

The following table describes the fields in this screen.

**Table 10** Internet Connection with ENET ENCAP

LABEL	DESCRIPTION
Obtain an IP Address Automatically	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select <b>Obtain an IP Address Automatically</b> if you have a dynamic IP address.
Static IP Address	Select <b>Static IP Address</b> if your ISP gives you a fixed IP address.
IP Address	Enter your ISP assigned IP address.
Subnet Mask	Enter a subnet mask in dotted decimal notation. Refer to the appendices to calculate a subnet mask If you are implementing subnetting.
Gateway IP address	You must specify a gateway IP address (supplied by your ISP) when you use <b>ENET ENCAP</b> in the <b>Encapsulation</b> field in the previous screen.
First DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Second DNS Server	As above.
Back	Click <b>Back</b> to go back to the previous wizard screen.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Exit	Click <b>Exit</b> to close the wizard screen without saving your changes.

**Figure 19** Internet Connection with PPPoA



The following table describes the fields in this screen.

**Table 11** Internet Connection with PPPoA

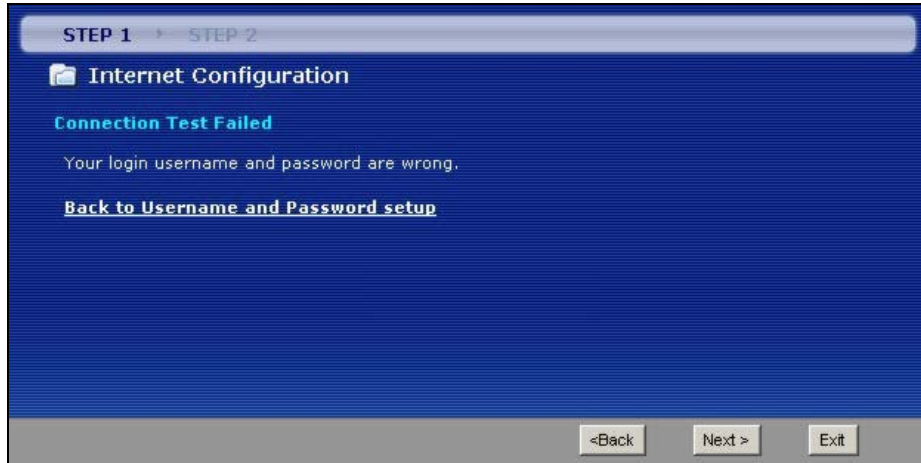
LABEL	DESCRIPTION
User Name	Enter the login name that your ISP gives you.
Password	Enter the password associated with the user name above.
Back	Click <b>Back</b> to go back to the previous wizard screen.



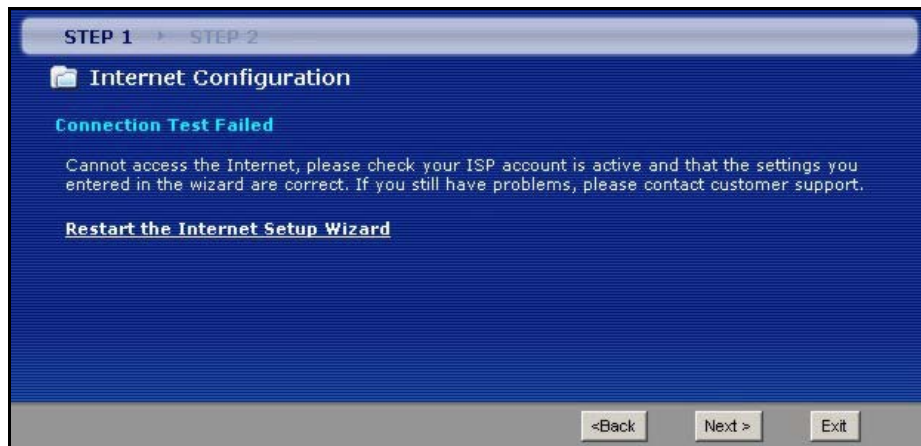
**Table 11** Internet Connection with PPPoA (continued)

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Exit	Click <b>Exit</b> to close the wizard screen without saving your changes.

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

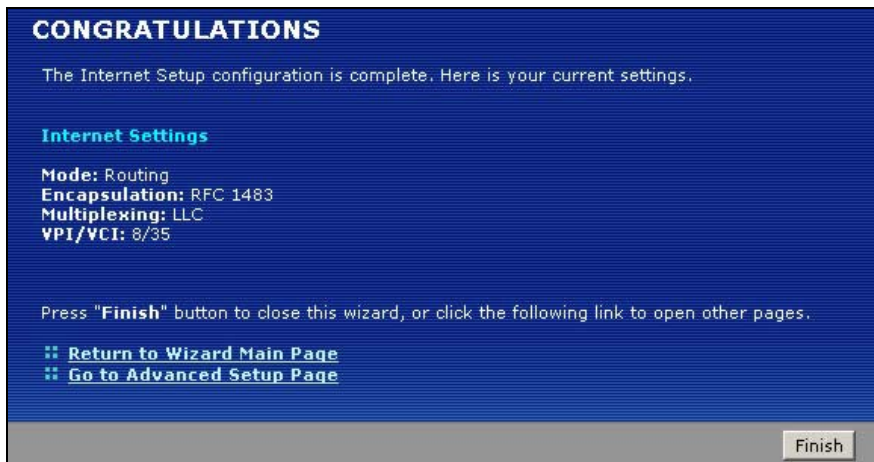
**Figure 20** Connection Test Failed-1

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

**Figure 21** Connection Test Failed-2.

When you are finished with the Internet Setup Wizard the following screen displays your configuration details. Click **Finish** to exit the wizard.

**Figure 22** Internet Setup Wizard Finished



# WAN Setup

This chapter describes how to configure WAN settings.

## 4.1 WAN Overview

A WAN (Wide Area Network) is an outside connection to another network or the Internet.

### 4.1.1 Encapsulation

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

#### 4.1.1.1 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.

#### 4.1.1.2 PPP over Ethernet

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

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

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

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

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

### 4.1.1.3 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 access multiplexer). Please refer to RFC 2364 for more information on PPPoA. Refer to RFC 1661 for more information on PPP.

### 4.1.1.4 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.

## 4.1.2 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.

### 4.1.2.1 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.

### 4.1.2.2 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.

## 4.1.3 Encapsulation and Multiplexing Scenarios

For Internet access you should use the encapsulation and multiplexing methods used by your ISP. Consult your telephone company for information on encapsulation and multiplexing methods for LAN-to-LAN applications, for example between a branch office and corporate headquarters. There must be prior agreement on encapsulation and multiplexing methods because they cannot be automatically determined. What method(s) you use also depends on how many VCs you have and how many different network protocols you need. The extra overhead that ENET ENCAP encapsulation entails makes it a poor choice in a LAN-to-LAN application. Here are some examples of more suitable combinations in such an application.

### 4.1.3.1 Scenario 1: One VC, Multiple Protocols

**PPPoA** (RFC-2364) encapsulation with **VC-based** multiplexing is the best combination because no extra protocol identifying headers are needed. The **PPP** protocol already contains this information.

### 4.1.3.2 Scenario 2: One VC, One Protocol (IP)

Selecting **RFC-1483** encapsulation with **VC-based** multiplexing requires the least amount of overhead (0 octets). However, if there is a potential need for multiple protocol support in the future, it may be safer to select **PPPoA** encapsulation instead of **RFC-1483**, so you do not need to reconfigure either computer later.

### 4.1.3.3 Scenario 3: Multiple VCs

If you have an equal number (or more) of VCs than the number of protocols, then select **RFC-1483** encapsulation and **VC-based** multiplexing.

## 4.1.4 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.

## 4.1.5 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.

### 4.1.5.1 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.

### 4.1.5.2 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.

### 4.1.5.3 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.

## 4.1.6 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

### 4.1.7 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.

## 4.2 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 4.5 on page 48](#))
- Traffic-redirect route (see [Section 4.7 on page 58](#))
- WAN-backup route, also called dial-backup (see [Section 4.8 on page 60](#))

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.

## 4.3 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.

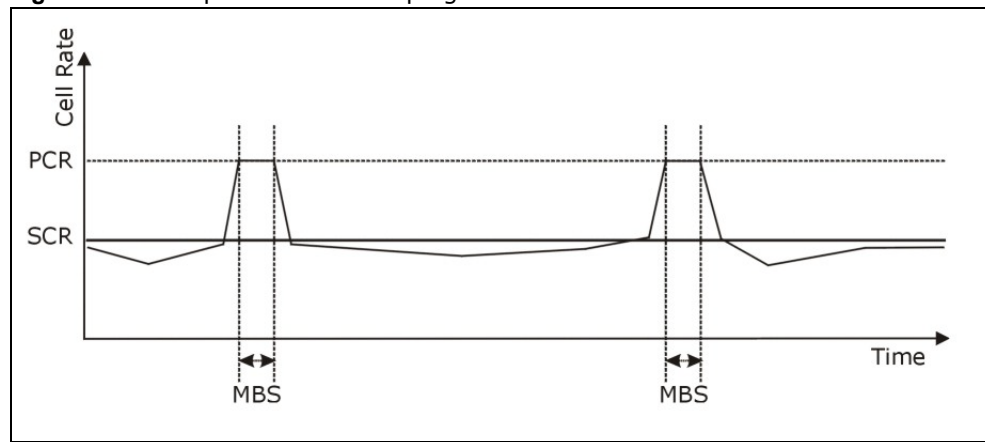
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

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 23** Example of Traffic Shaping



## 4.3.1 ATM Traffic Classes

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

### 4.3.1.1 Constant Bit Rate (CBR)

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

### 4.3.1.2 Variable Bit Rate (VBR)

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

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

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

#### 4.3.1.3 Unspecified Bit Rate (UBR)

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

## 4.4 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.

## 4.5 Internet Access Setup Screen

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



See [Section 4.1 on page 43](#) for more information.

**Figure 24** Internet Access Setup (PPPoE)

Internet Access Setup		More Connections	WAN Backup Setup
<b>Line</b>			
Modulation	Multi Mode		
<b>General</b>			
Mode	Routing		
Encapsulation	PPPoE		
User Name			
Password	*****		
Service Name			
Multiplexing	LLC		
Virtual Circuit ID			
VPI	8		
VCI	35		
<b>IP Address</b>			
<input checked="" type="radio"/> Obtain an IP Address Automatically <input type="radio"/> Static IP Address			
IP Address	0.0.0.0		
<b>DNS server</b>			
First DNS Server	Obtained From ISP	0.0.0.0	
Second DNS Server	Obtained From ISP	0.0.0.0	
Third DNS Server	Obtained From ISP	0.0.0.0	
<b>Connection</b>			
<input type="radio"/> Nailed-Up Connection <input checked="" type="radio"/> Connect on Demand			
	Max Idle Timeout	0	sec
		Apply	Cancel
		Advanced Setup	

The following table describes the labels in this screen.

**Table 12** Network > WAN > Internet Access Setup

LABEL	DESCRIPTION
Line	
Modulation	<p>Select the modulation supported by your ISP.</p> <p>Use <b>Multi Mode</b> if you are not sure which mode to choose from. The ZyXEL Device dynamically diagnoses the mode supported by the ISP and selects the best compatible one for your connection.</p> <p>Other options are <b>ADSL G.dmt, ADSL2, ADSL2+, ADSL2 AnnexM, ADSL2+ AnnexM, READSL2 Mode</b> and <b>ANSI T1.413</b>.</p>
General	
Mode	<p>Select <b>Routing</b> (default) from the drop-down list box if your ISP gives you one IP address only and you want multiple computers to share an Internet account. Select <b>Bridge</b> when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. If you select <b>Bridge</b>, you cannot use Firewall, DHCP server and NAT on the ZyXEL Device.</p>
Encapsulation	<p>Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the <b>Mode</b> field.</p> <p>If you select <b>Bridge</b> in the <b>Mode</b> field, select either <b>PPPoA</b> or <b>RFC 1483</b>.</p> <p>If you select <b>Routing</b> in the <b>Mode</b> field, select <b>PPPoA, RFC 1483, ENET ENCAP</b> or <b>PPPoE</b>.</p>
User Name	(PPPoA and PPPoE encapsulation only) Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	(PPPoA and PPPoE encapsulation only) Enter the password associated with the user name above.
Service Name	(PPPoE only) Type the name of your PPPoE service here.
Multiplexing	Select the method of multiplexing used by your ISP from the drop-down list. Choices are <b>VC</b> or <b>LLC</b> .
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
IP Address	<p>This option is available if you select <b>Routing</b> in the <b>Mode</b> field.</p> <p>A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet.</p> <p>If you use the encapsulation type except <b>RFC 1483</b>, select <b>Obtain an IP Address Automatically</b> when you have a dynamic IP address; otherwise select <b>Static IP Address</b> and type your ISP assigned IP address in the <b>IP Address</b> field below.</p> <p>If you use <b>RFC 1483</b>, enter the IP address given by your ISP in the <b>IP Address</b> field.</p>
Subnet Mask (ENET ENCAP encapsulation only)	<p>Enter a subnet mask in dotted decimal notation.</p> <p>Refer to the appendices to calculate a subnet mask If you are implementing subnetting.</p>

**Table 12** Network > WAN > Internet Access Setup

LABEL	DESCRIPTION
Gateway IP address (ENET ENCAP encapsulation only)	You must specify a gateway IP address (supplied by your ISP) when you select <b>ENET ENCAP</b> in the <b>Encapsulation</b> field
DNS Server	
First DNS Server	Select <b>Obtained From ISP</b> if your ISP dynamically assigns DNS server information (and the ZyXEL Device's WAN IP address) and you select <b>Obtain an IP Address Automatically</b> .
Second DNS Server	
Third DNS Server	<p>Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose <b>User-Defined</b>, but leave the IP address set to 0.0.0.0, <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b>. If you set a second choice to <b>User-Defined</b>, and enter the same IP address, the second <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b>.</p> <p>Select <b>None</b> if you do not want to configure DNS servers. You must have another DNS server on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.</p>
Connection (PPPoA and PPPoE encapsulation only)	
Nailed-Up Connection	Select <b>Nailed-Up Connection</b> when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select <b>Connect on Demand</b> when you don't want the connection up all the time and specify an idle time-out in the <b>Max Idle Timeout</b> field.
Max Idle Timeout	Specify an idle time-out in the <b>Max Idle Timeout</b> field when you select <b>Connect on Demand</b> . The default setting is 0, which means the Internet session will not timeout.
Apply	Click <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Advanced Setup	Click this button to display the <b>Advanced Internet Connection Setup</b> screen and edit more details of your WAN setup.

## 4.5.1 Configuring Advanced Internet Connection Setup

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

**Figure 25** Advanced Internet Connection Setup

The following table describes the labels in this screen.

**Table 13** Advanced Internet Connection Setup

LABEL	DESCRIPTION
RIP & Multicast Setup	
RIP Direction	Select the RIP direction from <b>None</b> , <b>Both</b> , <b>In Only</b> and <b>Out Only</b> .
RIP Version	Select the RIP version from <b>RIP-1</b> , <b>RIP-2B</b> and <b>RIP-2M</b> .
Multicast	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 ( <b>IGMP-v1</b> ) and <b>IGMP-v2</b> . Select <b>None</b> to disable it.
ATM QoS	
ATM QoS Type	Select <b>CBR</b> (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select <b>UBR</b> (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select <b>VBR-nRT</b> (Variable Bit Rate-non Real Time) or <b>VBR-RT</b> (Variable Bit Rate-Real Time) for bursty traffic and bandwidth sharing with other applications.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.

**Table 13** Advanced Internet Connection Setup (continued)

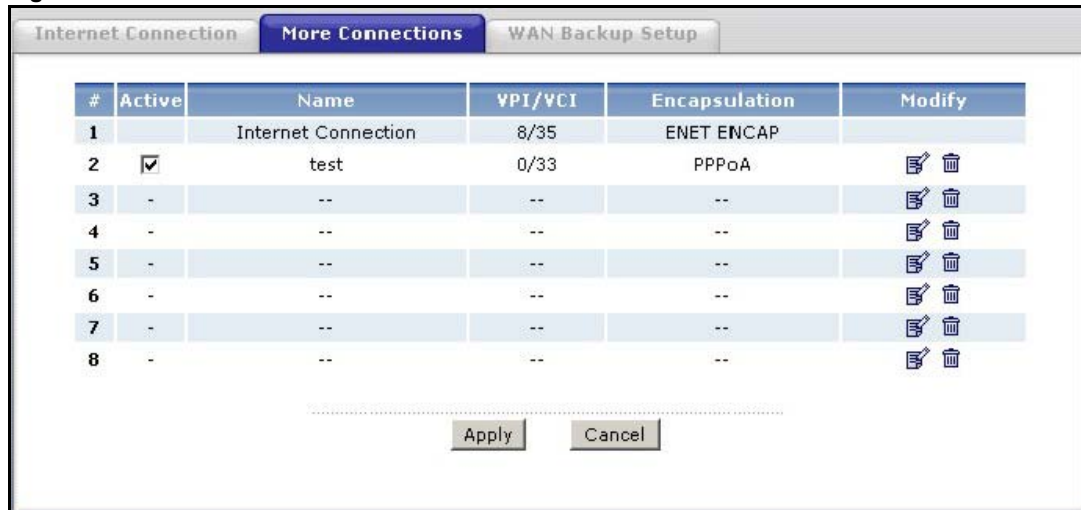
LABEL	DESCRIPTION
Sustain Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
Zero Configuration	<p>This feature is not applicable/available when you configure the ZyXEL Device to use a static WAN IP address or in bridge mode.</p> <p>Select <b>Yes</b> 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.</p> <p>Select <b>No</b> to disable this feature. You must manually configure the ZyXEL Device for Internet access.</p>
PPPoE Passthrough (PPPoE encapsulation only)	<p>This field is available when you select <b>PPPoE</b> encapsulation.</p> <p>In addition to the ZyXEL Device's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the ZyXEL Device. Each host can have a separate account and a public WAN IP address.</p> <p>PPPoE pass through is an alternative to NAT for application where NAT is not appropriate.</p> <p>Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.</p>
Packet Filter	
Incoming Filter Sets	
Protocol Filter	<p>Select the protocol filter(s) to control incoming traffic. You may choose up to 4 sets of filters.</p> <p>You can configure packet filters in the Packet Filter screen.</p>
Generic Filter	<p>Select the generic filter(s) to control outgoing traffic. You may choose up to 4 sets of filters.</p> <p>You can configure generic filters in the Packet Filter screen.</p>
Outgoing Filter Sets	
Protocol Filter	<p>Select the protocol filter(s) to control outgoing traffic. You may choose up to 4 sets of filters.</p> <p>You can configure protocol filters in the Packet Filter screen.</p>
Generic Filter	<p>Select the generic filter(s) to control outgoing traffic. You may choose up to 4 sets of filters.</p> <p>You can configure generic filters in the Packet Filter screen.</p>
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 4.6 Configuring More Connections

This section describes the protocol-independent parameters for a remote network. They are required for placing calls to a remote gateway and the network behind it across a WAN connection. When you use the **WAN > Internet Connection** screen to set up Internet access, you are configuring the first WAN connection.

Click **Network > WAN > More Connections** to display the screen as shown next.

**Figure 26** More Connections



The following table describes the labels in this screen.

**Table 14** More Connections

LABEL	DESCRIPTION
#	This is the index number of a connection.
Active	This display whether this connection is activated. Clear the check box to disable the connection. Select the check box to enable it.
Name	This is the descriptive name for this connection.
VPI/VCI	This is the VPI and VCI values used for this connection.
Encapsulation	This is the method of encapsulation used for this connection.
Modify	The first (ISP) connection is read-only in this screen. Use the <b>WAN &gt; Internet Connection</b> screen to edit it. Click the edit icon to go to the screen where you can edit the connection. Click the delete icon to remove an existing connection. You cannot remove the first connection.
Apply	Click <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 4.6.1 More Connections Edit

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

**Figure 27** More Connections Edit

The following table describes the labels in this screen.

**Table 15** More Connections Edit

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

**Table 15** More Connections Edit (continued)

LABEL	DESCRIPTION
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. Choices are <b>PPPoA</b> , <b>RFC 1483</b> , <b>ENET ENCAP</b> or <b>PPPoE</b> .
User Name	(PPPoA and PPPoE encapsulation only) Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	(PPPoA and PPPoE encapsulation only) Enter the password associated with the user name above.
Service Name	(PPPoE only) Type the name of your PPPoE service here.
Multiplexing	<p>Select the method of multiplexing used by your ISP from the drop-down list. Choices are <b>VC</b> or <b>LLC</b>.</p> <p>By prior agreement, a protocol is assigned a specific virtual circuit, for example, VC1 will carry IP. If you select VC, specify separate VPI and VCI numbers for each protocol.</p> <p>For LLC-based multiplexing or PPP encapsulation, one VC carries multiple protocols with protocol identifying information being contained in each packet header. In this case, only one set of VPI and VCI numbers need be specified for all protocols.</p>
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
IP Address	<p>This option is available if you select <b>Routing</b> in the <b>Mode</b> field.</p> <p>If you use <b>RFC 1483</b>, enter the IP address given by your ISP in the <b>IP Address</b> field.</p>
Subnet Mask	<p>Enter a subnet mask in dotted decimal notation.</p> <p>Refer to the appendices to calculate a subnet mask If you are implementing subnetting.</p>
Gateway IP address	Specify a gateway IP address (supplied by your ISP).
Connection	
Nailed-Up Connection	Select <b>Nailed-Up Connection</b> when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select <b>Connect on Demand</b> when you don't want the connection up all the time and specify an idle time-out in the <b>Max Idle Timeout</b> field.
Max Idle Timeout	Specify an idle time-out in the <b>Max Idle Timeout</b> field when you select <b>Connect on Demand</b> . The default setting is 0, which means the Internet session will not timeout.
NAT	<p><b>SUA only</b> is available only when you select <b>Routing</b> in the <b>Mode</b> field.</p> <p>Select <b>SUA Only</b> if you have one public IP address and want to use NAT. Click <b>Edit</b> to go to the <b>Port Forwarding</b> screen to edit a server mapping set.</p> <p>Otherwise, select <b>None</b> to disable NAT.</p>
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Advanced Setup	Click this button to display the <b>More Connections Advanced</b> screen and edit more details of your WAN setup.



## 4.6.2 Configuring More Connections Advanced Setup

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

**Figure 28** More Connections Advanced Setup

The following table describes the labels in this screen.

**Table 16** More Connections Advanced Setup

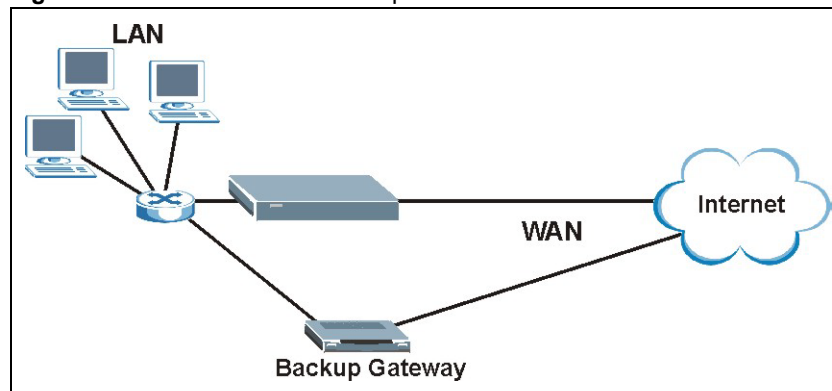
LABEL	DESCRIPTION
RIP & Multicast Setup	
RIP Direction	Select the RIP direction from <b>None</b> , <b>Both</b> , <b>In Only</b> and <b>Out Only</b> .
RIP Version	Select the RIP version from <b>RIP-1</b> , <b>RIP-2B</b> and <b>RIP-2M</b> .
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports both IGMP version 1 ( <b>IGMP-v1</b> ) and <b>IGMP-v2</b> . Select <b>None</b> to disable it.
ATM QoS	
ATM QoS Type	Select <b>CBR</b> (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select <b>UBR</b> (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select <b>VBR-nRT</b> (Variable Bit Rate-non Real Time) or <b>VBR-RT</b> (Variable Bit Rate-Real Time) for bursty traffic and bandwidth sharing with other applications.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.

**Table 16** More Connections Advanced Setup (continued)

LABEL	DESCRIPTION
Sustain Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
Packet Filter	
Incoming Filter Sets	
Protocol Filter	Select the protocol filter(s) to control incoming traffic. You may choose up to 4 sets of filters.  You can configure packet filters in the Packet Filter screen.
Generic Filter	Select the generic filter(s) to control outgoing traffic. You may choose up to 4 sets of filters.  You can configure generic filters in the Packet Filter screen.
Outgoing Filter Sets	
Protocol Filter	Select the protocol filter(s) to control outgoing traffic. You may choose up to 4 sets of filters.  You can configure protocol filters in the Packet Filter screen.
Generic Filter	Select the generic filter(s) to control outgoing traffic. You may choose up to 4 sets of filters.  You can configure generic filters in the Packet Filter screen.
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

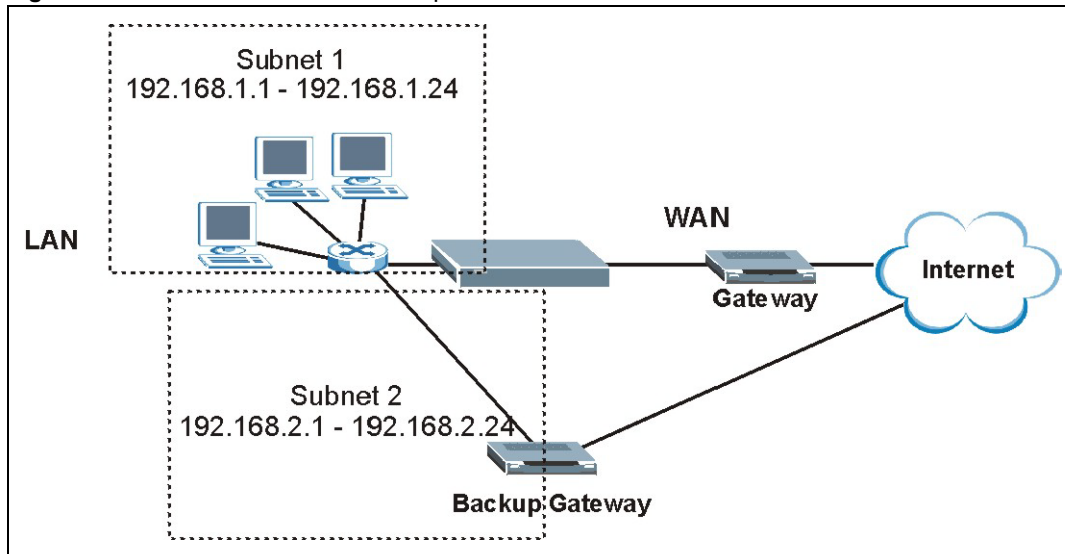
## 4.7 Traffic Redirect

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 29** 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 30** Traffic Redirect LAN Setup



## 4.8 Configuring WAN Backup

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

**Figure 31** WAN Backup Setup

The following table describes the labels in this screen.

**Table 17** WAN Backup Setup

LABEL	DESCRIPTION
Backup Type	Select the method that the ZyXEL Device uses to check the DSL connection. Select <b>DSL Link</b> to have the ZyXEL Device check if the connection to the DSLAM is up. Select <b>ICMP</b> to have the ZyXEL Device periodically ping the IP addresses configured in the <b>Check WAN IP Address</b> fields.
Check WAN IP Address 1-3	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).  <b>Note:</b> 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 <b>Check WAN IP Address</b> field without getting a response before switching to a WAN backup connection (or a different WAN backup connection).

**Table 17** WAN Backup Setup (continued)

LABEL	DESCRIPTION
Recovery Interval	<p>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.</p> <p>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.</p>
Timeout	<p>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 <b>Check WAN IP Address</b> 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 <b>Fail Tolerance</b> field. Use a higher value in this field if your network is busy or congested.</p>
Traffic Redirect	<p>Traffic redirect forwards traffic to a backup gateway when the ZyXEL Device cannot connect to the Internet.</p>
Active Traffic Redirect	<p>Select this check box to have the ZyXEL Device use traffic redirect if the normal WAN connection goes down.</p> <p><b>Note: If you activate traffic redirect, you must configure at least one Check WAN IP Address.</b></p>
Metric	<p>This field sets this route's priority among the routes the ZyXEL Device uses.</p> <p>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".</p>
Backup Gateway	<p>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.</p>
Apply	<p>Click <b>Apply</b> to save the changes.</p>
Cancel	<p>Click <b>Cancel</b> to begin configuring this screen afresh.</p>



## LAN Setup

This chapter describes how to configure LAN settings.

### 5.1 LAN Overview

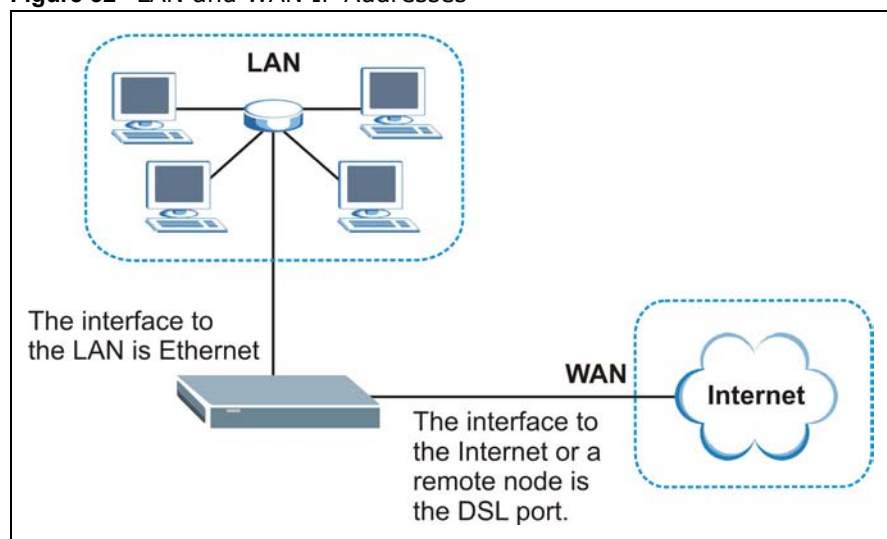
A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

See [Section 5.3 on page 68](#) to configure the **LAN** screens.

#### 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 32** LAN and WAN IP Addresses



#### 5.1.2 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyXEL Device as a DHCP server or disable it. When configured as a server, the ZyXEL Device provides the TCP/IP

configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

### 5.1.2.1 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.

### 5.1.3 DNS Server Address

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The DNS server addresses that you enter in the DHCP setup 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 first is for an ISP to tell a customer the DNS server addresses, usually in the form of an information sheet, when s/he signs up. If your ISP gives you the DNS server addresses, enter them in the **DNS Server** fields in **DHCP Setup**, otherwise, leave them blank.

Some ISP's choose to pass the DNS servers using the DNS server extensions of PPP 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.

If the **Primary** and **Secondary DNS Server** fields in the **DHCP Setup** screen are not specified, for instance, left as **0.0.0.0**, the ZyXEL Device tells the DHCP clients that it itself is the DNS server. When a computer sends a DNS query to the ZyXEL Device, the ZyXEL Device forwards the query to the real DNS server learned through IPCP and relays the response back to the computer.

Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the **DHCP Setup** screen. This way, the ZyXEL Device can pass the DNS servers to the computers and the computers can query the DNS server directly without the ZyXEL Device's intervention.

### 5.1.4 DNS Server Address Assignment

Use DNS (Domain Name System) to map 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.

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

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the DNS Server fields in the **DHCP Setup** screen.
- The ZyXEL Device acts as a DNS proxy when the **Primary** and **Secondary DNS Server** fields are left as **0.0.0.0** in the **DHCP Setup** screen.



## 5.2 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.

### 5.2.1 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

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

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

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

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

#### 5.2.1.1 Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space*.

## 5.2.2 RIP Setup

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

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

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

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

## 5.2.3 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.

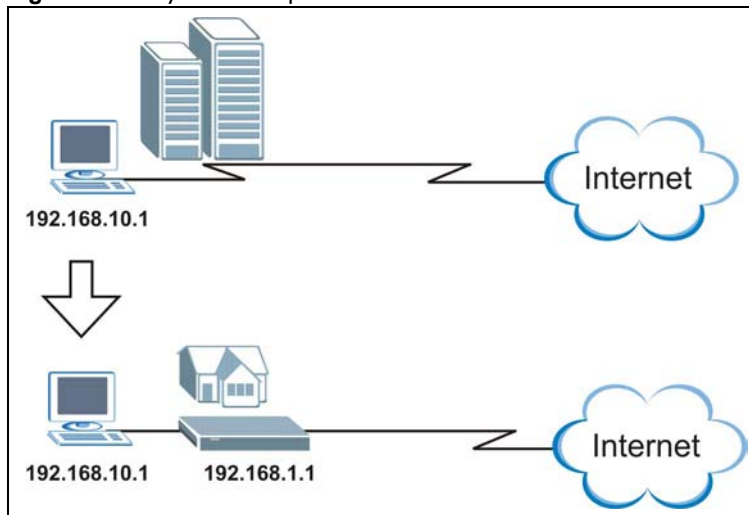
## 5.2.4 Any IP

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 33** 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.

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

### 5.2.4.1 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.

## 5.3 Configuring LAN IP

Click **LAN** to open the **IP** screen. See [Section 5.1 on page 63](#) for background information.

**Figure 34** LAN IP

The following table describes the fields in this screen.

**Table 18** LAN IP

LABEL	DESCRIPTION
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).
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Advanced Setup	Click this button to display the <b>Advanced LAN Setup</b> screen and edit more details of your LAN setup.

### 5.3.1 Configuring Advanced LAN Setup

To edit your ZyXEL Device's advanced LAN settings, click the **Advanced Setup** button in the **LAN IP** screen. The screen appears as shown.

**Figure 35** Advanced LAN Setup

The following table describes the labels in this screen.

**Table 19** Advanced LAN Setup

LABEL	DESCRIPTION
RIP & Multicast Setup	
RIP Direction	Select the RIP direction from <b>None</b> , <b>Both</b> , <b>In Only</b> and <b>Out Only</b> .
RIP Version	Select the RIP version from <b>RIP-1</b> , <b>RIP-2B</b> and <b>RIP-2M</b> .
Multicast	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 ( <b>IGMP-v1</b> ) and <b>IGMP-v2</b> . Select <b>None</b> to disable it.
Any IP Setup	Select the <b>Active</b> check box 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.  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.
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.
Allow between LAN and WAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic.  Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.

**Table 19** Advanced LAN Setup (continued)

LABEL	DESCRIPTION
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 5.4 DHCP Setup

Use this screen to configure the DNS server information that the ZyXEL Device sends to the DHCP client devices on the LAN.

**Figure 36** DHCP Setup

The following table describes the labels in this screen.

**Table 20** DHCP Setup

LABEL	DESCRIPTION
DHCP Setup	
DHCP	<p>If set to <b>Server</b>, 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 <b>None</b>, the DHCP server will be disabled.</p> <p>If set to <b>Relay</b>, 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 <b>Remote DHCP Server</b> field in this case.</p> <p>When DHCP is used, the following items need to be set:</p>
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.

**Table 20** DHCP Setup

LABEL	DESCRIPTION
Remote DHCP Server	If <b>Relay</b> is selected in the <b>DHCP</b> field above then enter the IP address of the actual remote DHCP server here.
DNS Server	
DNS Servers Assigned by DHCP Server	The ZyXEL Device passes a DNS (Domain Name System) server IP address to the DHCP clients.
Primary DNS Server	This field is not available when you set <b>DHCP</b> to <b>Relay</b> .
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.  If the fields are left as <b>0.0.0.0</b> , the ZyXEL Device acts as a DNS proxy and forwards the DHCP client's DNS query to the real DNS server learned through IPCP and relays the response back to the computer.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 5.5 LAN Client List

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

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

To change your ZyXEL Device's static DHCP settings, click **Network > LAN > Client List**. The screen appears as shown.

**Figure 37** LAN Client List

The screenshot shows the 'Client List' tab in the DHCP Setup interface. At the top, there are navigation tabs: IP, DHCP Setup, Client List (selected), and IP Alias. Below the tabs is the 'DHCP Client Table' section. It features two input fields: 'IP Address' with the value '0.0.0.0' and 'MAC Address' with the value '00:00:00:00:00:00', followed by an 'Add' button. The table itself has the following data:

#	Status	Host Name	IP Address	MAC Address	Reserve	Modify
1		tw11947	192.168.1.33	00:00:E8:7C:14:80	<input type="checkbox"/>	
2			192.168.1.35	00:AC:10:01:23:45	<input checked="" type="checkbox"/>	
3			192.168.1.64	00:A0:C5:01:23:46	<input checked="" type="checkbox"/>	

At the bottom of the table area, there are three buttons: 'Apply', 'Cancel', and 'Refresh'.

The following table describes the labels in this screen.

**Table 21** LAN Client List

LABEL	DESCRIPTION
IP Address	Enter the IP address that you want to assign to the computer on your LAN with the MAC address specified below.  The IP address should be within the range of IP addresses you specified in the <b>DHCP Setup</b> for the DHCP client.
MAC Address	Enter the MAC address of a computer on your LAN.
Add	Click <b>Add</b> to add a static DHCP entry.
#	This is the index number of the static IP table entry (row).
Status	This field displays whether the client is connected to the ZyXEL Device.
Host Name	This field displays the computer host name.
IP Address	This field displays the IP address relative to the # field listed above.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation).  A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
Reserve	Select the check box(es) in each entry to have the ZyXEL Device always assign the selected entry(ies)'s IP address(es) to the corresponding MAC address(es) (and host name(s)). You can select up to 32 entries in this table.
Modify	Click the modify icon to have the <b>IP address</b> field editable and change it.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Refresh	Click <b>Refresh</b> to reload the DHCP table.

## 5.6 LAN IP Alias

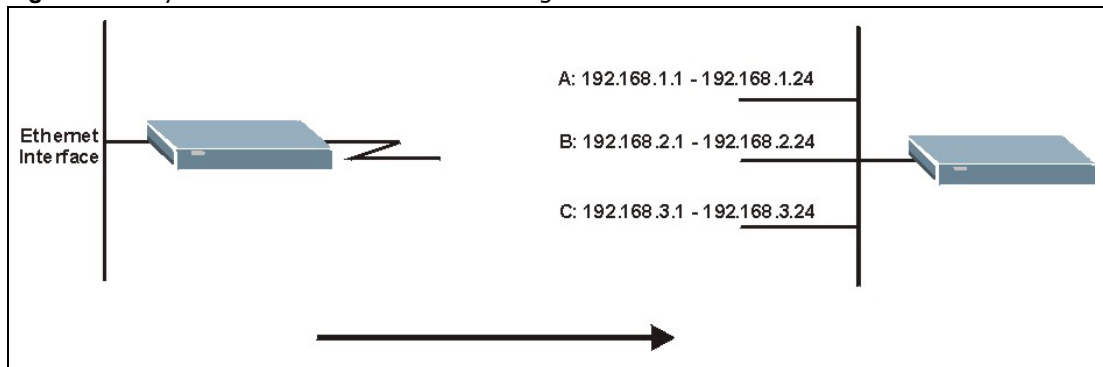
IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The ZyXEL Device supports three logical LAN interfaces via its single physical Ethernet interface with the ZyXEL Device itself as the gateway for each LAN network.

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



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

**Figure 38** Physical Network & Partitioned Logical Networks



To change your ZyXEL Device's IP alias settings, click **Network > LAN > IP Alias**. The screen appears as shown.

**Figure 39** LAN IP Alias

The screenshot shows the 'LAN IP Alias' configuration page. At the top, there are tabs for 'IP', 'DHCP Setup', 'Client List', and 'IP Alias'. The 'IP Alias' tab is selected. Below the tabs, there are two sections for configuring IP aliases:

- IP Alias 1:**
  - IP Alias 1
  - IP Address: 0.0.0.0
  - IP Subnet Mask: 0.0.0.0
  - RIP Direction: None
  - RIP Version: N/A
- IP Alias 2:**
  - IP Alias 2
  - IP Address: 0.0.0.0
  - IP Subnet Mask: 0.0.0.0
  - RIP Direction: None
  - RIP Version: N/A

At the bottom of the page, there are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

**Table 22** LAN IP Alias

LABEL	DESCRIPTION
IP Alias 1, 2	Select the check box to configure another LAN network for the ZyXEL Device.
IP Address	Enter the IP address of your ZyXEL Device in dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address.
IP Subnet Mask	Your ZyXEL Device will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyXEL Device.

**Table 22** LAN IP Alias

LABEL	DESCRIPTION
RIP Direction	RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. The <b>RIP Direction</b> field controls the sending and receiving of RIP packets. Select the RIP direction from <b>Both/In Only/Out Only/None</b> . When set to <b>Both</b> or <b>Out Only</b> , the ZyXEL Device will broadcast its routing table periodically. When set to <b>Both</b> or <b>In Only</b> , it will incorporate the RIP information that it receives; when set to <b>None</b> , it will not send any RIP packets and will ignore any RIP packets received.
RIP Version	The <b>RIP Version</b> field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). <b>RIP-1</b> 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 <b>RIP-2B</b> and <b>RIP-2M</b> sends the routing data in RIP-2 format; the difference being that <b>RIP-2B</b> uses subnet broadcasting while <b>RIP-2M</b> uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to <b>Both</b> and the Version set to <b>RIP-1</b> .
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

# Network Address Translation (NAT) Screens

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

## 6.1 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.

### 6.1.1 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 in the WAN side.

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

**Table 23** 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.

## 6.1.2 What NAT Does

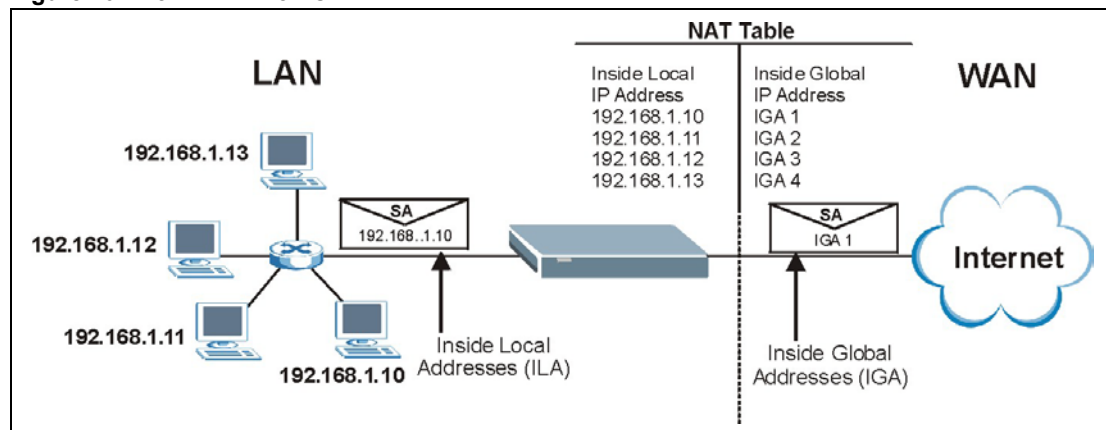
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) 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, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see [Table 24 on page 78](#)), 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)*.

## 6.1.3 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.

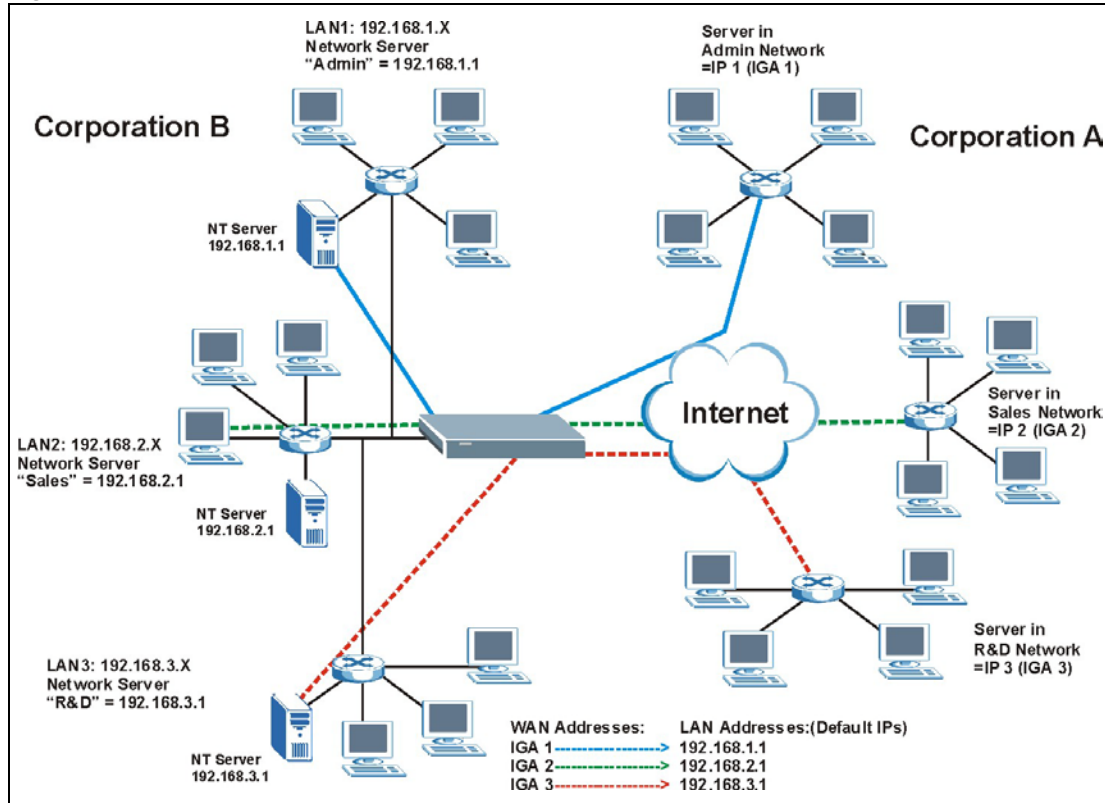
**Figure 40** How NAT Works



## 6.1.4 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 41** NAT Application With IP Alias



## 6.1.5 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 24** 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

## 6.2 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 24 on page 78](#).

- 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.

## 6.3 NAT General Setup

You must create a firewall rule in addition to setting up SUA/NAT, to allow traffic from the WAN to be forwarded through the ZyXEL Device. Click **Network > NAT** to open the following screen. Not all fields are available on all models.

**Figure 42** NAT General

The following table describes the labels in this screen.

**Table 25** NAT General

LABEL	DESCRIPTION
Active Network Address Translation (NAT)	Select this check box to enable NAT.
SUA Only	Select this radio button if you have just one public WAN IP address for your ZyXEL Device.
Full Feature	Select this radio button if you have multiple public WAN IP addresses for your ZyXEL Device.
Max NAT/ Firewall Session Per User	<p>When computers use peer to peer applications, such as file sharing applications, they may use a large number of NAT sessions. If you do not limit the number of NAT sessions a single client can establish, this can result in all of the available NAT sessions being used. In this case, no additional NAT sessions can be established, and users may not be able to access the Internet.</p> <p>Each NAT session establishes a corresponding firewall session. Use this field to limit the number of NAT/firewall sessions each client computer can establish through the ZyXEL Device.</p> <p>If your network has a small number of clients using peer to peer applications, you can raise this number to ensure that their performance is not degraded by the number of NAT sessions they can establish. If your network has a large number of users using peer to peer applications, you can lower this number to ensure no single client is using all of the available NAT sessions.</p>
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to reload the previous configuration for this screen.

## 6.4 Port Forwarding

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

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.

### 6.4.1 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.

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

### 6.4.2 Port Forwarding: Services and Port Numbers

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

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

**Table 26** Services and Port Numbers

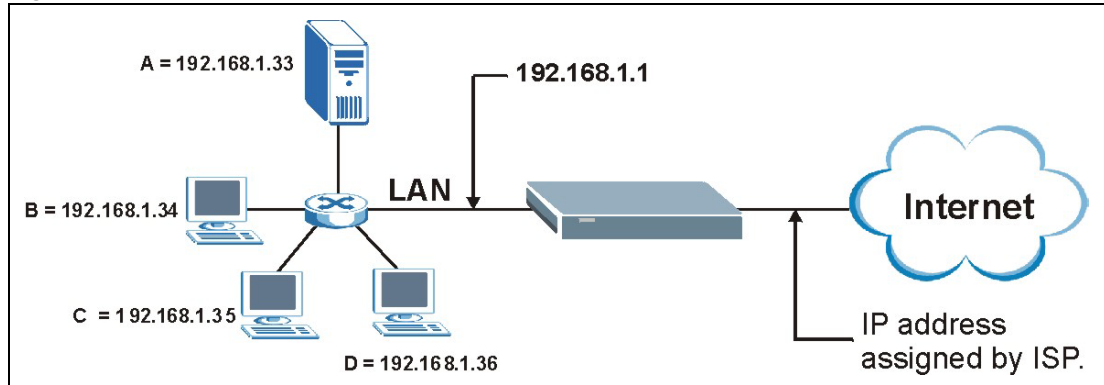
SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)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



### 6.4.3 Configuring Servers Behind Port Forwarding (Example)

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

**Figure 43** Multiple Servers Behind NAT Example



## 6.5 Configuring Port Forwarding

Note: The **Port Forwarding** screen is available only when you select **SUA Only** in the **NAT > General** screen.

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

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

See [Table 26 on page 80](#) for port numbers commonly used for particular services.

**Figure 44** NAT Port Forwarding

#	Active	Service Name	Start Port	End Port	Server IP Address	Modify
.....						

The following table describes the fields in this screen.

**Table 27** NAT Port Forwarding

LABEL	DESCRIPTION
Default Server Setup	
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a <b>Default Server</b> IP address, the ZyXEL Device discards all packets received for ports that are not specified here or in the remote management setup.
Port Forwarding	
Service Name	Select a service from the drop-down list box.
Server IP Address	Enter the IP address of the server for the specified service.
Add	Click this button to add a rule to the table below.
#	This is the rule index number (read-only).
Active	Click this check box to enable the rule.
Service Name	This is a service's name.
Start Port	This is the first port number that identifies a service.
End Port	This is the last port number that identifies a service.
Server IP Address	This is the server's IP address.
Modify	Click the edit icon to go to the screen where you can edit the port forwarding rule.  Click the delete icon to delete an existing port forwarding rule. Note that subsequent rules move up by one when you take this action.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to return to the previous configuration.

## 6.5.1 Port Forwarding Rule Edit

To edit a port forwarding rule, click the rule's edit icon in the **Port Forwarding** screen to display the screen shown next.

**Figure 45** Port Forwarding Rule Setup

The screenshot shows a web-based configuration interface for editing a port forwarding rule. The title bar reads "Rule Setup". Below the title, there is a list of configuration options:

- Active
- Service Name:
- Start Port:
- End Port:
- Server IP Address:

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

The following table describes the fields in this screen.

**Table 28** Port Forwarding Rule Setup

LABEL	DESCRIPTION
Active	Click this check box to enable the rule.
Service Name	Enter a name to identify this port-forwarding rule.
Start Port	Enter a port number in this field. To forward only one port, enter the port number again in the <b>End Port</b> field. To forward a series of ports, enter the start port number here and the end port number in the <b>End Port</b> field.
End Port	Enter a port number in this field. To forward only one port, enter the port number again in the <b>Start Port</b> field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the <b>Start Port</b> field above.
Server IP Address	Enter the inside IP address of the server here.
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 6.6 The SIP ALG Screen

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

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

**Figure 46** Network > NAT > ALG

The screenshot shows the 'ALG Settings' screen. At the top, there is a navigation bar with four tabs: 'General', 'Port Forwarding', 'ALG' (which is highlighted in blue), and 'DMZ Hosting'. Below the navigation bar, the main content area is titled 'ALG Settings'. It contains a single checkbox labeled 'Enable SIP ALG'. At the bottom of the screen, there are two buttons: 'Apply' and 'Reset'.

The following table describes the fields in this screen.

**Table 29** Network > NAT > ALG

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

## 6.7 DMZ Hosting

For some applications or devices, NAT can cause problems or it might be best to allow some functions to operate on an private LAN IP address without being "hidden" from the WAN side. DMZ Hosting allows a singel IP address to be visiblle from the WAN.

Use this screen to enable and disable DMZ Hosting and select a specific IP address to apply DMZ hosting. To access this screen, click **Network > NAT > ALG**.

**Figure 47** Network > NAT > DMZ



The following table describes the fields in this screen.

**Table 30** Network > NAT > DMZ

LABEL	DESCRIPTION
Active DMZ Hosting	Select this to activate DMZ Hosting for the specified IP address.
DMZ Hosting Address	Type the IP address used for DMZ hosting. This IP address will be outside that group of LAN IP addresses normally hidden by NAT. It will be visible to anyone actively looking for LAN IP addresses on your private network.
Apply	Click this to save your changes.

# Firewalls

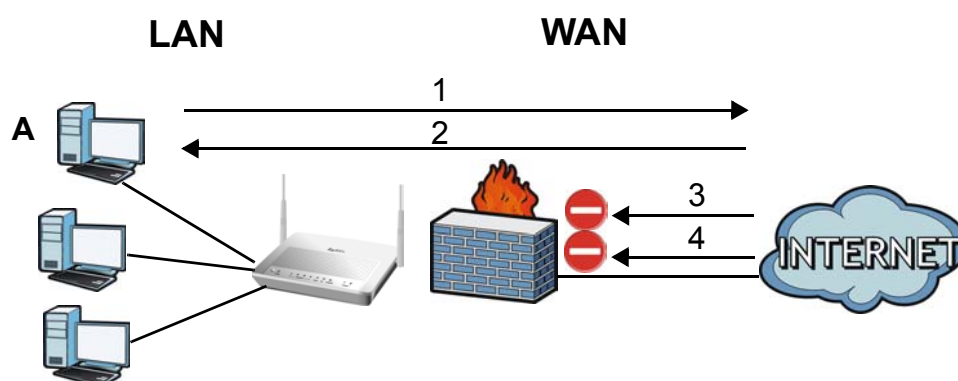
## 7.1 Overview

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

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

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

**Figure 48** Default Firewall Action



### 7.1.1 What You Can Do in the Firewall Screens

- Use the **General** screen to enable firewall and/or triangle route on the ZyXEL Device, and set the default action that the firewall takes on packets that do not match any of the firewall rules.
- Use the **Rules** screen to view the configured firewall rules and add, edit or remove a firewall rule.
- Use the **Threshold** screen to set the thresholds that the ZyXEL Device uses to determine when to start dropping sessions that do not become fully established (half-open sessions).

### 7.1.2 What You Need to Know About Firewall

#### DoS

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer

have access to network resources. The ZyXEL Device is pre-configured to automatically detect and thwart all known DoS attacks.

## Anti-Probing

If an outside user attempts to probe an unsupported port on your ZyXEL Device, an ICMP response packet is automatically returned. This allows the outside user to know the ZyXEL Device exists. The ZyXEL Device supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your ZyXEL Device when unsupported ports are probed.

## ICMP

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

## DoS Thresholds

For DoS attacks, the ZyXEL Device uses thresholds to determine when to drop sessions that do not become fully established. These thresholds apply globally to all sessions. You can use the default threshold values, or you can change them to values more suitable to your security requirements.

### 7.1.3 Firewall Rule Setup Example

The following Internet firewall rule example allows a hypothetical "MyService" connection from the Internet.

- 1 Click **Security > Firewall > Rules**.
- 2 Select **WAN to LAN** in the **Packet Direction** field.

**Figure 49** Firewall Example: Rules

General **Rules** Anti Probing Threshold

Rules

Firewall Rules Storage Space in Use ( 3%)

0% 100%

Packet Direction: WAN to LAN

Create a new rule after rule number : 1 Add

Move the rule to: 0 Move

#	Active	Source IP	Destination IP	Service	Action	Schedule	Log	Modify	Order
1	<input checked="" type="checkbox"/>	Any	Any	NetBIOS(TCP/UDP:137~139,445)	Permit	No	No		DN

Apply Cancel

- 3 In the **Rules** screen, select the index number after that you want to add the rule. For example, if you select "6", your new rule becomes number 7 and the previous rule 7 (if there is one) becomes rule 8.
- 4 Click **Add** to display the firewall rule configuration screen.
- 5 In the **Edit Rule** screen, click the **Edit Customized Services** link to open the **Customized Service** screen.
- 6 Click an index number to display the **Customized Services Config** screen and configure the screen as follows and click **Apply**.

**Figure 50** Edit Custom Port Example

The screenshot shows a configuration window with two main sections: 'Config' and 'Port Configuration'.  
 In the 'Config' section:  
 - Service Name: MyService  
 - Service Type: TCP/UDP  
 In the 'Port Configuration' section:  
 - Type: Single (selected with a radio button), Port Range (unselected)  
 - Port Number: From 123 To 123  
 At the bottom of the window are three buttons: Apply, Cancel, and Delete.

- 7 Select **Any** in the **Destination Address List** box and then click **Delete**.
- 8 Configure the destination address screen as follows and click **Add**.

**Figure 51** Firewall Example: Edit Rule: Destination Address

The screenshot shows the 'Edit Rule 1' configuration window. At the top, there is a checkbox for 'Active' which is checked, and a dropdown for 'Action for Matched Packets' set to 'Permit'.  
 The 'Source Address' section includes:  
 - Address Type: Any Address  
 - Start IP Address: 0.0.0.0  
 - End IP Address: 0.0.0.0  
 - Subnet Mask: 0.0.0.0  
 - Source Address List: Any  
 - Buttons: Add >>, Edit <<, Delete  
 The 'Destination Address' section includes:  
 - Address Type: Range Address  
 - Start IP Address: 10.0.0.10  
 - End IP Address: 10.0.0.15  
 - Subnet Mask: 0.0.0.0  
 - Destination Address List: 10.0.0.10 - 10.0.0.15  
 - Buttons: Add >>, Edit <<, Delete  
 The 'Service' section is partially visible at the bottom.

- 9 Use the **Add >>** and **Remove** buttons between **Available Services** and **Selected Services** list boxes to configure it as follows. Click **Apply** when you are done.

Note: Custom services show up with an "\*" before their names in the **Services** list box and the **Rules** list box.

**Figure 52** Firewall Example: Edit Rule: Select Customized Services

**Edit Rule 2**

Active  
Action for Matched Packets: **Permit**

**Source Address**

Address Type: Any Address  
Start IP Address: 0.0.0.0  
End IP Address: 0.0.0.0  
Subnet Mask: 0.0.0.0

Source Address List: Any

**Destination Address**

Address Type: Range Address  
Start IP Address: 10.0.0.10  
End IP Address: 10.0.0.15  
Subnet Mask: 0.0.0.0

Destination Address List: 10.0.0.10 - 10.0.0.15

**Service**

Available Services: Any(All), Any(ICMP), AIMNEW-ICQ(TCP:5190), AUTH(TCP:113), BGP(TCP:179)

Selected Services: \*MyService(TCP:123)

[Edit Customized Services](#)

**Schedule**

Day to Apply:  Everyday  
 Sun  Mon  Tue  Wed  Thu  Fri  Sat

Time of Day to Apply : (24-Hour Format)  
 All day  
Start: 0 hour 0 minute End: 0 hour 0 minute

Log:  Log Packet Detail Information.

Alert:  Send Alert Message to Administrator When Matched.

**Apply** **Cancel**

On completing the configuration procedure for this Internet firewall rule, the **Rules** screen should look like the following.



Rule 1 allows a “MyService” connection from the WAN to IP addresses 192.168.1.1 through 192.168.1.15 on the LAN.

**Figure 53** Firewall Example: Rules: MyService

The screenshot shows the 'Rules' configuration window with the 'Rules' tab selected. At the top, there are tabs for 'General', 'Rules', and 'Threshold'. Below the tabs, a progress bar indicates 'Firewall Rules Storage Space in Use ( 2%)' at 0%. The 'Packet Direction' is set to 'WAN to LAN'. Below this, there is a field 'Create a new rule after rule number : 1' with an 'Add' button. A table lists the rules:

#	Active	Source IP	Destination IP	Service	Action	Schedule	Log	Modify	Order
1	<input checked="" type="checkbox"/>	192.168.1.10 - 192.168.1.15	Any	Any(UDP)	Permit	No	No		1

At the bottom, there are 'Apply' and 'Cancel' buttons.

## 7.2 The Firewall General Screen

Use this screen to configure the firewall settings. Click **Security > Firewall** to display the following screen.

**Figure 54** Security > Firewall > General

The screenshot shows the 'General' configuration window for the firewall. At the top, there are tabs for 'General', 'Rules', 'Anti Probing', and 'Threshold'. The 'General' tab is selected. Below the tabs, there are two checkboxes: 'Active Firewall' (checked) and 'Bypass Triangle Route' (unchecked). A **Caution** message states: "When Bypass Triangle Route is checked, all LAN to LAN and WAN to WAN packets will bypass the Firewall check." Below this is a table:

Packet Direction	Default Action	Log
WAN to LAN	Drop	<input checked="" type="checkbox"/>
LAN to WAN	Permit	<input checked="" type="checkbox"/>
WAN to WAN / Router	Drop	<input checked="" type="checkbox"/>
LAN to LAN / Router	Permit	<input type="checkbox"/>

At the bottom right, there is a 'Basic...' link. At the bottom, there are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

**Table 31** Security > Firewall > General

LABEL	DESCRIPTION
Active Firewall	Select this check box to activate the firewall. The ZyXEL Device performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Bypass Triangle Route	<p>If an alternate gateway on the LAN has an IP address in the same subnet as the ZyXEL Device's LAN IP address, return traffic may not go through the ZyXEL Device. This is called an asymmetrical or "triangle" route. This causes the ZyXEL Device to reset the connection, as the connection has not been acknowledged.</p> <p>Select this check box to have the ZyXEL Device permit the use of asymmetrical route topology on the network (not reset the connection).</p> <p>Note: Allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the ZyXEL Device. A better solution is to use IP alias to put the ZyXEL Device and the backup gateway on separate subnets. See <a href="#">Section 7.5.4.1 on page 101</a> for an example.</p>
Packet Direction	<p>This is the direction of travel of packets (<b>LAN to Router, LAN to WAN, WAN to Router, WAN to LAN</b>).</p> <p>Firewall rules are grouped based on the direction of travel of packets to which they apply. For example, <b>LAN to Router</b> means packets traveling from a computer/subnet on the LAN to the ZyXEL Device itself.</p>
Default Action	<p>Use the drop-down list boxes to select the default action that the firewall is to take on packets that are traveling in the selected direction and do not match any of the firewall rules.</p> <p>Select <b>Drop</b> to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender.</p> <p>Select <b>Reject</b> to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender.</p> <p>Select <b>Permit</b> to allow the passage of the packets.</p>
Log	Select the check box to create a log (when the above action is taken) for packets that are traveling in the selected direction and do not match any of your customized rules.
Expand...	Click this to display more information.
Basic...	Click this to display less information.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

## 7.3 The Firewall Rule Screen

Note: The ordering of your rules is very important as rules are applied in turn.

Click **Security > Firewall > Rules** to bring up the following screen. This screen displays a list of the configured firewall rules. Note the order in which the rules are listed.

**Figure 55** Security > Firewall > Rules

The following table describes the labels in this screen.

**Table 32** Security > Firewall > Rules

LABEL	DESCRIPTION
Firewall Rules Storage Space in Use	This read-only bar shows how much of the ZyXEL Device's memory for recording firewall rules it is currently using. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red.
Packet Direction	Use the drop-down list box to select a direction of travel of packets for which you want to configure firewall rules.
Create a new rule after rule number	Select an index number and click <b>Add</b> to add a new firewall rule after the selected index number. For example, if you select "6", your new rule becomes number 7 and the previous rule 7 (if there is one) becomes rule 8.
	The following read-only fields summarize the rules you have created that apply to traffic traveling in the selected packet direction. The firewall rules that you configure (summarized below) take priority over the general firewall action settings in the <b>General</b> screen.
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.
Active	This field displays whether a firewall is turned on or not. Select the check box to enable the rule. Clear the check box to disable the rule.
Source IP	This drop-down list box displays the source addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to <b>Any</b> .
Destination IP	This drop-down list box displays the destination addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to <b>Any</b> .
Service	This drop-down list box displays the services to which this firewall rule applies.
Action	This field displays whether the firewall silently discards packets ( <b>Drop</b> ), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender ( <b>Reject</b> ) or allows the passage of packets ( <b>Permit</b> ).
Schedule	This field tells you whether a schedule is specified ( <b>Yes</b> ) or not ( <b>No</b> ).
Log	This field shows you whether a log is created when packets match this rule ( <b>Yes</b> ) or not ( <b>No</b> ).

**Table 32** Security > Firewall > Rules (continued)

LABEL	DESCRIPTION
Modify	Click the Edit icon to go to the screen where you can edit the rule.  Click the Remove icon to delete an existing firewall rule. A window displays asking you to confirm that you want to delete the firewall rule. Note that subsequent firewall rules move up by one when you take this action.
Order	Click the Move icon to display the <b>Move the rule to</b> field. Type a number in the <b>Move the rule to</b> field and click the <b>Move</b> button to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

## 7.3.1 Configuring Firewall Rules

Use this screen to configure firewall rules. In the **Rules** screen, select an index number and click **Add** or click a rule's **Edit** icon to display this screen and refer to the following table for information on the labels.

**Figure 56** Security > Firewall > Rules: Edit

**Edit Rule 2**

Active  
Action for Matched Packets: Permit

---

**Source Address**

Address Type: Any Address

Start IP Address: 0.0.0.0

End IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Source Address List

Any

Add >>
Edit <<
Delete

---

**Destination Address**

Address Type: Any Address

Start IP Address: 0.0.0.0

End IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Destination Address List

Any

Add >>
Edit <<
Delete

---

**Service**

Available Services

Any(All)  
 Any(ICMP)  
 AIMNEW-ICQ(TCP:5190)  
 AUTH(TCP:113)  
 BGP(TCP:179)

[Edit Customized Services](#)

Selected Services

Any(UDP)  
 Any(TCP)

Add >>
Remove

---

**Schedule**

Day to Apply

Everyday

Sun  Mon  Tue  Wed  Thu  Fri  Sat

Time of Day to Apply : (24-Hour Format)

All day

Start  hour  minute    End  hour  minute

Log

Log Packet Detail Information.

Alert

Send Alert Message to Administrator When Matched.

Apply
Cancel

The following table describes the labels in this screen.

**Table 33** Security > Firewall > Rules: Edit

LABEL	DESCRIPTION
Edit Rule	
Active	Select this option to enable this firewall rule.
Action for Matched Packet	Use the drop-down list box to select whether to discard ( <b>Drop</b> ), deny and send an ICMP destination-unreachable message to the sender of ( <b>Reject</b> ) or allow the passage of ( <b>Permit</b> ) packets that match this rule.
Source/Destination Address	
Address Type	Do you want your rule to apply to packets with a particular (single) IP, a range of IP addresses (for instance, 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop-down list box that includes: <b>Single Address, Range Address, Subnet Address</b> and <b>Any Address</b> .
Start IP Address	Enter the single IP address or the starting IP address in a range here.
End IP Address	Enter the ending IP address in a range here.
Subnet Mask	Enter the subnet mask here, if applicable.
Add >>	Click <b>Add &gt;&gt;</b> to add a new address to the <b>Source</b> or <b>Destination Address</b> box. You can add multiple addresses, ranges of addresses, and/or subnets.
Edit <<	To edit an existing source or destination address, select it from the box and click <b>Edit &lt;&lt;</b> .
Delete	Highlight an existing source or destination address from the <b>Source</b> or <b>Destination Address</b> box above and click <b>Delete</b> to remove it.
Services	
Available/ Selected Services	Highlight a service from the <b>Available Services</b> box on the left, then click <b>Add &gt;&gt;</b> to add it to the <b>Selected Services</b> box on the right. To remove a service, highlight it in the <b>Selected Services</b> box on the right, then click <b>Remove</b> .
Edit Customized Service	Click the <b>Edit Customized Services</b> link to bring up the screen that you use to configure a new custom service that is not in the predefined list of services.
Schedule	
Day to Apply	Select everyday or the day(s) of the week to apply the rule.
Time of Day to Apply (24-Hour Format)	Select <b>All Day</b> or enter the start and end times in the hour-minute format to apply the rule.
Log	
Log Packet Detail Information	This field determines if a log for packets that match the rule is created or not. Go to the <b>Log Settings</b> page and select the <b>Access Control</b> logs category to have the ZyXEL Device record these logs.
Alert	
Send Alert Message to Administrator When Matched	Select the check box to have the ZyXEL Device generate an alert when the rule is matched.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

## 7.3.2 Customized Services

Configure customized services and port numbers not predefined by the ZyXEL Device. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number

Authority) website. Click the **Edit Customized Services** link while editing a firewall rule to configure a custom service port. This displays the following screen.

**Figure 57** Security > Firewall > Rules: Edit: Edit Customized Services

No.	Name	Protocol	Port
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

Back

The following table describes the labels in this screen.

**Table 34** Security > Firewall > Rules: Edit: Edit Customized Services

LABEL	DESCRIPTION
No.	This is the number of your customized port. Click a rule's number of a service to go to the <b>Firewall Customized Services Config</b> screen to configure or edit a customized service.
Name	This is the name of your customized service.
Protocol	This shows the IP protocol ( <b>TCP</b> , <b>UDP</b> or <b>TCP/UDP</b> ) that defines your customized service.
Port	This is the port number or range that defines your customized service.
Back	Click this to return to the <b>Firewall Edit Rule</b> screen.

### 7.3.3 Configuring a Customized Service

Use this screen to add a customized rule or edit an existing rule. Click a rule number in the **Firewall Customized Services** screen to display the following screen.

**Figure 58** Security > Firewall > Rules: Edit: Edit Customized Services: Config

Config

Service Name

Service Type TCP

Port Configuration

Type  Single  Port Range

Port Number From  To

Apply Cancel Delete

The following table describes the labels in this screen.

**Table 35** Security > Firewall > Rules: Edit: Edit Customized Services: Config

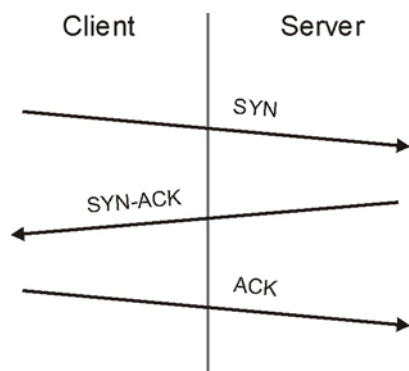
LABEL	DESCRIPTION
Config	
Service Name	Type a unique name for your custom port.
Service Type	Choose the IP port ( <b>TCP</b> , <b>UDP</b> or <b>TCP/UDP</b> ) that defines your customized port from the drop down list box.
Port Configuration	
Type	Click <b>Single</b> to specify one port only or <b>Range</b> to specify a span of ports that define your customized service.
Port Number	Type a single port number or the range of port numbers that define your customized service.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.
Delete	Click this to delete the current rule.

## 7.4 The Firewall Threshold Screen

For DoS attacks, the ZyXEL Device uses thresholds to determine when to start dropping sessions that do not become fully established (half-open sessions). These thresholds apply globally to all sessions.

For TCP, half-open means that the session has not reached the established state-the TCP three-way handshake has not yet been completed. Under normal circumstances, the application that initiates a session sends a SYN (synchronize) packet to the receiving server. The receiver sends back an ACK (acknowledgment) packet and its own SYN, and then the initiator responds with an ACK (acknowledgment). After this handshake, a connection is established.

**Figure 59** Three-Way Handshake



For UDP, half-open means that the firewall has detected no return traffic. An unusually high number (or arrival rate) of half-open sessions could indicate a DOS attack.



## 7.4.1 Threshold Values

If everything is working properly, you probably do not need to change the threshold settings as the default threshold values should work for most small offices. Tune these parameters when you believe the ZyXEL Device has been receiving DoS attacks that are not recorded in the logs or the logs show that the ZyXEL Device is classifying normal traffic as DoS attacks. Factors influencing choices for threshold values are:

- 1 The maximum number of opened sessions.
- 2 The minimum capacity of server backlog in your LAN network.
- 3 The CPU power of servers in your LAN network.
- 4 Network bandwidth.
- 5 Type of traffic for certain servers.

Reduce the threshold values if your network is slower than average for any of these factors (especially if you have servers that are slow or handle many tasks and are often busy).

- If you often use P2P applications such as file sharing with eMule or eDonkey, it's recommended that you increase the threshold values since lots of sessions will be established during a small period of time and the ZyXEL Device may classify them as DoS attacks.

## 7.4.2 Configuring Firewall Thresholds

The ZyXEL Device also sends alerts whenever **TCP Maximum Incomplete** is exceeded. The global values specified for the threshold and timeout apply to all TCP connections.

Click **Firewall > Threshold** to bring up the next screen.

**Figure 60** Security > Firewall > Threshold

Denial of Service Thresholds	
One Minute Low	<input type="text" value="80"/> ( Sessions per Minute)
One Minute High	<input type="text" value="100"/> ( Sessions per Minute)
Maximum Incomplete Low	<input type="text" value="80"/> ( Sessions)
Maximum Incomplete High	<input type="text" value="100"/> ( Sessions)
TCP Maximum Incomplete	<input type="text" value="10"/> ( Sessions)

Action taken when TCP Maximum Incomplete reached threshold	
<input checked="" type="radio"/>	Delete the Oldest Half Open Session when New Connection Request Comes.
<input type="radio"/>	Deny New Connection Request for <input type="text" value="10"/> Minutes(1~255)

The following table describes the labels in this screen.

**Table 36** Security > Firewall > Threshold

LABEL	DESCRIPTION
Denial of Service Thresholds	The ZyXEL Device measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.
One Minute Low	This is the rate of new half-open sessions per minute that causes the firewall to stop deleting half-open sessions. The ZyXEL Device continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below this number.
One Minute High	<p>This is the rate of new half-open sessions per minute that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the ZyXEL Device deletes half-open sessions as required to accommodate new connection attempts.</p> <p>For example, if you set the one minute high to 100, the ZyXEL Device starts deleting half-open sessions when more than 100 session establishment attempts have been detected in the last minute. It stops deleting half-open sessions when the number of session establishment attempts detected in a minute goes below the number set as the one minute low.</p>
Maximum Incomplete Low	This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The ZyXEL Device continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number.
Maximum Incomplete High	<p>This is the number of existing half-open sessions that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the ZyXEL Device deletes half-open sessions as required to accommodate new connection requests. Do not set <b>Maximum Incomplete High</b> to lower than the current <b>Maximum Incomplete Low</b> number.</p> <p>For example, if you set the maximum incomplete high to 100, the ZyXEL Device starts deleting half-open sessions when the number of existing half-open sessions rises above 100. It stops deleting half-open sessions when the number of existing half-open sessions drops below the number set as the maximum incomplete low.</p>
TCP Maximum Incomplete	<p>An unusually high number of half-open sessions with the same destination host address could indicate that a DoS attack is being launched against the host.</p> <p>Specify the number of existing half-open TCP sessions with the same destination host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between 1 and 256. As a general rule, you should choose a smaller number for a smaller network, a slower system or limited bandwidth. The ZyXEL Device sends alerts whenever the <b>TCP Maximum Incomplete</b> is exceeded.</p>
Action taken when TCP Maximum Incomplete reached threshold	<p>Select the action that ZyXEL Device should take when the TCP maximum incomplete threshold is reached. You can have the ZyXEL Device either:</p> <p>Delete the oldest half open session when a new connection request comes.</p> <p>or</p> <p>Deny new connection requests for the number of minutes that you specify (between 1 and 255).</p>
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

## 7.5 Firewall Technical Reference

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

### 7.5.1 Firewall Rules Overview

Your customized rules take precedence and override the ZyXEL Device's default settings. The ZyXEL Device checks the source IP address, destination IP address and IP protocol type of network traffic against the firewall rules (in the order you list them). When the traffic matches a rule, the ZyXEL Device takes the action specified in the rule.

Firewall rules are grouped based on the direction of travel of packets to which they apply:

- LAN to Router
- LAN to WAN
- WAN to LAN
- WAN to Router

**Note:** The LAN includes both the LAN port and the WLAN.

By default, the ZyXEL Device's stateful packet inspection allows packets traveling in the following directions:

- LAN to Router  
These rules specify which computers on the LAN can manage the ZyXEL Device (remote management).

**Note:** You can also configure the remote management settings to allow only a specific computer to manage the ZyXEL Device.

- LAN to WAN  
These rules specify which computers on the LAN can access which computers or services on the WAN.

By default, the ZyXEL Device's stateful packet inspection drops packets traveling in the following directions:

- WAN to LAN  
These rules specify which computers on the WAN can access which computers or services on the LAN.

**Note:** You also need to configure NAT port forwarding (or full featured NAT address mapping rules) to allow computers on the WAN to access devices on the LAN.

- WAN to Router  
By default the ZyXEL Device stops computers on the WAN from managing the ZyXEL Device. You could configure one of these rules to allow a WAN computer to manage the ZyXEL Device.

**Note:** You also need to configure the remote management settings to allow a WAN computer to manage the ZyXEL Device.

You may define additional rules and sets or modify existing ones but please exercise extreme caution in doing so.

For example, you may create rules to:

- Block certain types of traffic, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
- Allow everyone except your competitors to access a web server.
- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

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

## 7.5.2 Guidelines For Enhancing Security With Your Firewall

- 1 Change the default password via web configurator.
- 2 Think about access control before you connect to the network in any way.
- 3 Limit who can access your router.
- 4 Don't enable any local service (such as telnet or FTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
- 5 For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
- 6 Protect against IP spoofing by making sure the firewall is active.
- 7 Keep the firewall in a secured (locked) room.

## 7.5.3 Security Considerations

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

Consider these security ramifications before creating a rule:

- 1 Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
- 2 Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?

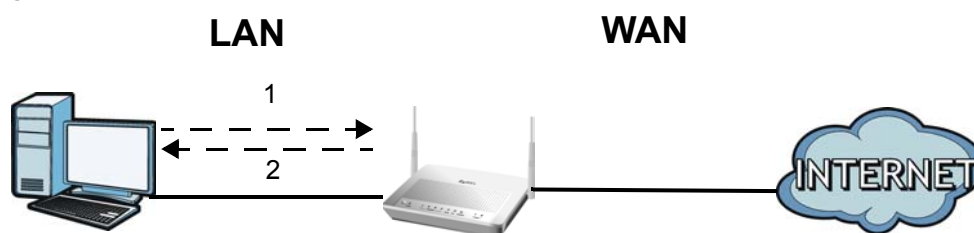
- 3 Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.
- 4 Does this rule conflict with any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

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

## 7.5.4 Triangle Route

When the firewall is on, your ZyXEL Device acts as a secure gateway between your LAN and the Internet. In an ideal network topology, all incoming and outgoing network traffic passes through the ZyXEL Device to protect your LAN against attacks.

**Figure 61** Ideal Firewall Setup



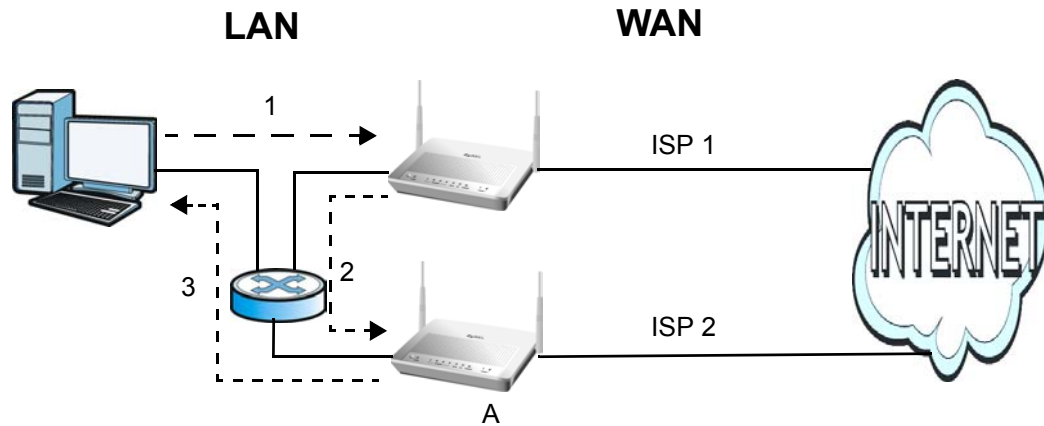
### 7.5.4.1 The “Triangle Route” Problem

A traffic route is a path for sending or receiving data packets between two Ethernet devices. You may have more than one connection to the Internet (through one or more ISPs). If an alternate gateway is on the LAN (and its IP address is in the same subnet as the ZyXEL Device’s LAN IP address), the “triangle route” (also called asymmetrical route) problem may occur. The steps below describe the “triangle route” problem.

- 1 A computer on the LAN initiates a connection by sending out a SYN packet to a receiving server on the WAN.
- 2 The ZyXEL Device reroutes the SYN packet through Gateway **A** on the LAN to the WAN.
- 3 The reply from the WAN goes directly to the computer on the LAN without going through the ZyXEL Device.

As a result, the ZyXEL Device resets the connection, as the connection has not been acknowledged.

**Figure 62** “Triangle Route” Problem



### 7.5.4.2 Solving the “Triangle Route” Problem

If you have the ZyXEL Device allow triangle route sessions, traffic from the WAN can go directly to a LAN computer without passing through the ZyXEL Device and its firewall protection.

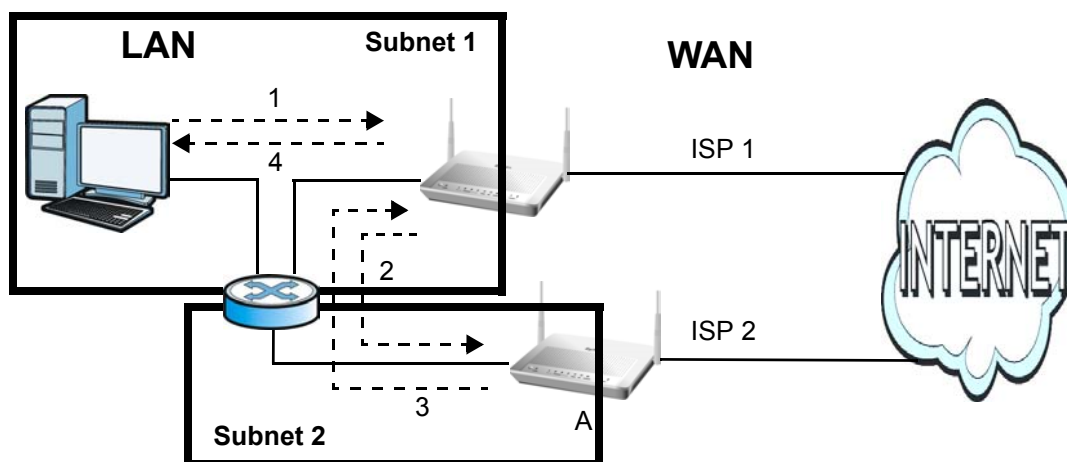
Another solution is to use IP alias. IP alias allows you to partition your network into logical sections over the same Ethernet interface. Your ZyXEL Device supports up to three logical LAN interfaces with the ZyXEL Device being the gateway for each logical network.

It’s like having multiple LAN networks that actually use the same physical cables and ports. By putting your LAN and Gateway **A** in different subnets, all returning network traffic must pass through the ZyXEL Device to your LAN. The following steps describe such a scenario.

- 1 A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.
- 2 The ZyXEL Device reroutes the packet to Gateway A, which is in Subnet 2.
- 3 The reply from the WAN goes to the ZyXEL Device.

- The ZyXEL Device then sends it to the computer on the LAN in Subnet 1.

**Figure 63** IP Alias







# Packet Filters

## 8.1 Overview

Your ZyXEL Device uses filters to decide whether to allow passage of traffic. This chapter discusses how to create and apply filters.

### 8.1.1 What You Can Do in the Packet Filter Screen

Use the **Packet Filter** screens to display the filter sets and configure the rules for protocol and generic filters.

### 8.1.2 What You Need to Know About the Packet Filter

#### Filters

Your ZyXEL Device uses filters to decide whether to allow passage of a data packet. Filters are subdivided into generic and protocol filters. Generic filter rules act on the raw data from/to LAN and WAN. Protocol filter rules act on IP packets.

#### Filter Structure

A filter set consists of one or more filter rules. The ZyXEL Device allows you to configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system. You cannot mix generic filter rules and protocol filter rules within the same set. You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

## 8.2 The Packet Filter Screen

Use this screen to set up packet filters on your ZyXEL Device. Click Security > Packet Filter to display the following screen.

**Figure 64** Security > Packet Filter

#	Name	Filter Type	Modify
1	<input type="text"/>	Protocol Filter	
2	<input type="text"/>	Protocol Filter	
3	<input type="text"/>	Protocol Filter	
4	<input type="text"/>	Protocol Filter	
5	<input type="text"/>	Protocol Filter	
6	<input type="text"/>	Protocol Filter	
7	<input type="text"/>	Protocol Filter	
8	<input type="text"/>	Protocol Filter	
9	<input type="text"/>	Protocol Filter	
10	<input type="text"/>	Protocol Filter	
11	<input type="text"/>	Protocol Filter	
12	<input type="text"/>	Protocol Filter	

The following table describes the fields in this screen.

**Table 37** Security > Packet Filter













LABEL	DESCRIPTION
#	This field displays the index number of the filter set.
Name	Enter a name for the filter set. The text may consist of up to 16 letters, numerals and any printable character found on a typical English language keyboard.
Filter Type	Select <b>Protocol Filter</b> or <b>Generic Filter</b> for your filter set. Protocol filter rules are used to filter IP packets while generic filter rules allow filtering of non-IP packets.
Modify	Click the <b>Edit</b> button to configure a filter set. Click the <b>Remove</b> button to delete a filter set.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

## 8.2.1 Editing Protocol Filters

Use this screen to display a protocol filter set on your ZyXEL Device. Protocol rules allow you to base the rule on the fields in the IP and the upper layer protocol, for example, UDP and TCP headers.

In the **Packet Filter** screen, select **Protocol Filter** from the **Filter Type** field. Then click the **Edit** button from the **Modify** field to display the following screen.

**Figure 65** Security > Packet Filter > Edit (Protocol Filter)

#	Active	Filter Type	Protocol	SA	DA	Modify
1	<input checked="" type="checkbox"/>	Protocol Filter	TCP	0.0.0.0	0.0.0.0	 
2	-					 
3	-					 
4	-					 
5	-					 
6	-					 

LABEL	DESCRIPTION
#	This is the index number of the rules in a filter set.
Active	Use the check box to turn a filter rule on or off.
Filter Type	This field displays whether the filter type is a protocol filter or generic filter.
Protocol	This field displays the upper layer protocol.
SA	This field displays the source IP address.
DA	This field displays the destination IP address.
Modify	Click the <b>Edit</b> icon to configure a filter rule. Click the <b>Remove</b> icon to delete a filter rule.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

## 8.2.2 Configuring Protocol Filter Rules

Use this screen to configure protocol filter rules. In the **Edit (Protocol Filter)** screen, click an **Edit** icon to display the following screen.

**Figure 66** Security > Packet Filter > Edit (Protocol Filter) > Edit Rule

Label	Value
Active	<input type="checkbox"/>
Protocol	ICMP
IP Source Route	<input type="checkbox"/>
Destination Address	0.0.0.0
Destination Subnet Netmask	0.0.0.0
Destination Port	0
Port Compare	None
Source Address	0.0.0.0
Source Subnet Netmask	0.0.0.0
Source Port	0
Port Compare	None
TCP Estab	N/A
More	No
Log	None
Action Match	Check Next Rule
Action Not Match	Check Next Rule

The following table describes the labels in this screen.

**Table 38** Security > Packet Filter > Edit (Protocol Filter) > Edit Rule

LABEL	DESCRIPTION
Active	Select the check box to enable the filter rule.
Protocol	Select <b>ICMP</b> , <b>TCP</b> or <b>UDP</b> for the upper layer protocol.
IP Source Route	Select the check box to apply the filter rule to packets with an IP source route option. The majority of IP packets do not have source route.
Destination Address	Enter the destination IP address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.
Destination Subnet Netmask	Enter the IP subnet mask for the destination IP address.
Destination Port	Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.
Port Compare	Select the comparison to apply to the destination port in the packet against the value given in the <b>Destination Port</b> field.  Options are <b>None</b> , <b>Equal</b> , <b>Not Equal</b> , <b>Less</b> and <b>Greater</b> .
Source Address	Enter the source IP address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.
Source Subnet Netmask	Enter the IP subnet mask for the source IP address
Source Port	Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.

LABEL	DESCRIPTION
Port Compare	Select the comparison to apply to the source port in the packet against the value given in the <b>Source Port</b> field. Options are <b>None, Equal, Not Equal, Less</b> and <b>Greater</b> .
TCP Estab	This field is only available when you select <b>TCP</b> in the <b>Protocol</b> field. Select <b>Yes</b> to have the rule match packets that want to establish a TCP connection. This field is ignored if you select <b>No</b> .
More	Select <b>Yes</b> to pass a matching packet to the next filter rule before an action is taken. Select <b>No</b> to act upon the packet according to the action fields.
Log	Select a logging option from the following: <b>None</b> - No packets will be logged. <b>Match</b> - Only packets that match the rule parameters will be logged. <b>Not Match</b> - Only packets that do not match the rule parameters will be logged. <b>Both</b> - All packets will be logged.
Action Match	Select the action for a matching packet. Options are <b>Check Next Rule, Forward</b> and <b>Drop</b> .
Action Not Match	Select the action for a packet not matching the rule. Options are <b>Check Next Rule, Forward</b> and <b>Drop</b> .
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.













### 8.2.3 Editing Generic Filters

Use this screen to display a generic filter set on your ZyXEL Device. The purpose of generic rules is to allow you to filter non-IP packets. For IP packets, it is generally easier to use the IP rules directly.

For generic rules, the ZyXEL Device treats a packet as a byte stream as opposed to an IP or IPX packet. You specify the portion of the packet to check with the Offset (from 0) and the Length fields, both in bytes. The ZyXEL Device applies the Mask (bit-wise ANDing) to the data portion before comparing the result against the Value to determine a match. The Mask and Value are specified in hexadecimal numbers. Note that it takes two hexadecimal digits to represent a byte, so if the length is 4 bytes, the value in either field will take 8 digits, for example, FFFFFFFF.

In the **Packet Filter** screen, select **Generic Filter** from the **Filter Type** field. Then click the **Edit** button from the **Modify** field to display the following screen.

**Figure 67** Security > Packet Filter > Edit (Generic Filter)

#	Active	Filter Type	Offset	Length	Mask	Value	Modify
1	<input type="checkbox"/>	Generic Filter	0	3	ffffff	012345	 
2	-						 
3	-						 
4	-						 
5	-						 
6	-						 

The following table describes the labels in this screen.

**Table 39** Security > Packet Filter > Edit (Generic Filter)

LABEL	DESCRIPTION
#	This is the index number of the rules in a filter set.
Active	Use the check box to turn on or off a filter rule.
Filter Type	This field displays whether the filter type is a protocol filter or generic filter.
Offset	This field displays the offset value.
Length	This field displays the length value.
Mask	This field displays the mask value.
Value	This field displays the value.
Modify	Click the <b>Edit</b> icon to configure a filter rule. Click the <b>Remove</b> icon to delete a filter rule.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

## 8.2.4 Configuring Generic Packet Rules

Use this screen to configure generic filter rules. In the **Edit (Generic Filter)** screen, click the **Edit** button from the **Modify** field to display the following screen.

**Figure 68** Security > Packet Filter > Edit (Generic Filter) > Edit Rule

The screenshot shows the 'Edit Rule' configuration window. The title bar reads 'Edit Rule'. The settings are as follows:

- Active:
- Protocol: ICMP (dropdown)
- IP Source Route:
- Destination Address: 0.0.0.0
- Destination Subnet: 0.0.0.0
- Destination Netmask: 0.0.0.0
- Destination Port: 0
- Port Compare: None (dropdown)
- Source Address: 0.0.0.0
- Source Subnet: 0.0.0.0
- Source Netmask: 0.0.0.0
- Source Port: 0
- Port Compare: None (dropdown)
- TCP Estab: N/A (dropdown)
- More: No (dropdown)
- Log: None (dropdown)
- Action Match: Check Next Rule (dropdown)
- Action Not Match: Check Next Rule (dropdown)

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

The following table describes the labels in this screen.

**Table 40** Security > Packet Filter > Edit (Generic Filter) > Edit Rule

LABEL	DESCRIPTION
Active	Select the check box to enable the filter rule.
Offset	Enter the starting byte of the data portion in the packet that you wish to compare. The range for this field is from 0 to 255.
Length	Enter the byte count of the data portion in the packet that you wish to compare. The range for this field is 0 to 8.
Mask	Enter the mask (in hexadecimal notation) to apply to the data portion before comparison.
Value	Enter the value (in hexadecimal notation) to compare with the data portion.
More	Select <b>Yes</b> to pass a matching packet to the next filter rule before an action is taken. Select <b>No</b> to act upon the packet according to the action fields.

LABEL	DESCRIPTION
Log	Select a logging option from the following: <b>None</b> – No packets will be logged. <b>Match</b> - Only packets that match the rule parameters will be logged. <b>Not Match</b> - Only packets that do not match the rule parameters will be logged. <b>Both</b> – All packets will be logged.
Action Match	Select the action for a matching packet. Options are <b>Check Next Rule, Forward</b> and <b>Drop</b> .
Action Not Match	Select the action for a packet not matching the rule. Options are <b>Check Next Rule, Forward</b> and <b>Drop</b> .
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

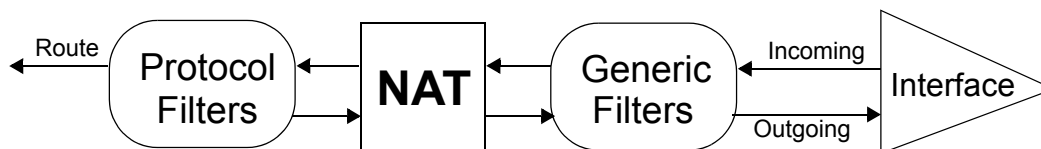
## 8.3 Packet Filter Technical Reference

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

### 8.3.1 Filter Types and NAT

There are two classes of filter rules, generic filter rules and protocol filter rules. Generic filter rules act on the raw data from/to LAN and WAN. Protocol filter rules act on the IP packets. When NAT (Network Address Translation) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the ZyXEL Device applies the protocol filters to the “native” IP address and port number before NAT for outgoing packets and after NAT for incoming packets. On the other hand, the generic filters are applied to the raw packets that appear on the wire. They are applied at the point when the ZyXEL Device is receiving and sending the packets; that is the interface. The interface can be an Ethernet port or any other hardware port. The following diagram illustrates this.

**Figure 69** Protocol and Generic Filter Sets



### 8.3.2 Firewall Versus Filters

Below are some comparisons between the ZyXEL Device’s filtering and firewall functions.



## Packet Filtering

- The router filters packets as they pass through the router's interface according to the filter rules you designed.
- Packet filtering is a powerful tool, yet can be complex to configure and maintain, especially if you need a chain of rules to filter a service.
- Packet filtering only checks the header portion of an IP packet.

## When To Use Filtering

- 1 To block/allow LAN packets by their MAC addresses.
- 2 To block/allow special IP packets which are neither TCP nor UDP, nor ICMP packets.
- 3 To block/allow both inbound (WAN to LAN) and outbound (LAN to WAN) traffic between the specific inside host/network "A" and outside host/network "B". If the filter blocks the traffic from A to B, it also blocks the traffic from B to A. Filters cannot distinguish traffic originating from an inside host or an outside host by IP address.
- 4 To block/allow IP trace route.

## Firewall

- The firewall inspects packet contents as well as their source and destination addresses. Firewalls of this type employ an inspection module, applicable to all protocols, that understands data in the packet is intended for other layers, from the network layer (IP headers) up to the application layer.
- The firewall performs stateful inspection. It takes into account the state of connections it handles so that, for example, a legitimate incoming packet can be matched with the outbound request for that packet and allowed in. Conversely, an incoming packet masquerading as a response to a non-existent outbound request can be blocked.
- The firewall uses session filtering, i.e., smart rules, that enhance the filtering process and control the network session rather than control individual packets in a session.
- The firewall provides e-mail service to notify you of routine reports and when alerts occur.

## When To Use The Firewall

- 1 To prevent DoS attacks and prevent hackers cracking your network.
- 2 A range of source and destination IP addresses as well as port numbers can be specified within one firewall rule making the firewall a better choice when complex rules are required.
- 3 To selectively block/allow inbound or outbound traffic between inside host/networks and outside host/networks. Remember that filters cannot distinguish traffic originating from an inside host or an outside host by IP address.
- 4 The firewall performs better than filtering if you need to check many rules.
- 5 Use the firewall if you need routine e-mail reports about your system or need to be alerted when attacks occur.

- 6 The firewall can block specific URL traffic that might occur in the future. The URL can be saved in an Access Control List (ACL) database.

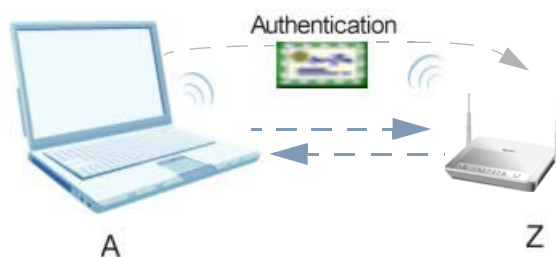
# Certificates

## 9.1 Overview

This chapter describes how your ZyXEL Device can use certificates as a means of authenticating wireless clients. It gives background information about public-key certificates and explains how to use them.

A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

**Figure 70** Certificates Example



In the figure above, the ZyXEL Device (Z) checks the identity of the notebook (A) using a certificate before granting it access to the network.

### 9.1.1 What You Can Do in the Certificates Screens

- Use the **My Certificates** screens to generate and export self-signed certificates or certification requests and import the ZyXEL Device's CA-signed certificates.
- Use the **Trusted CAs** screens to save CA certificates to the ZyXEL Device.
- Use the **Trusted Remote Hosts** screens to import self-signed certificates.
- Use the **Directory Servers** screens to configure a list of addresses of directory servers (that contain lists of valid and revoked certificates).

### 9.1.2 What You Need to Know About Certificates

#### Certification Authority

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

## Certificate File Formats

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

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

## 9.2 The My Certificates Screen

This is the ZyXEL Device's summary list of certificates and certification requests. Certificates display in black and certification requests display in gray. Click **Security > Certificates > My Certificates** to open the **My Certificates** screen.

**Figure 71** My Certificates

The following table describes the labels in this screen.

**Table 41** My Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyXEL Device's PKI storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
My Certificate Setting	
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Type	<p>This field displays what kind of certificate this is.</p> <p><b>REQ</b> represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the <b>My Certificate Import</b> screen to import the certificate and replace the request.</p> <p><b>SELF</b> represents a self-signed certificate.</p> <p><b>*SELF</b> represents the default self-signed certificate, which the ZyXEL Device uses to sign imported trusted remote host certificates.</p> <p><b>CERT</b> represents a certificate issued by a certification authority.</p>

LABEL	DESCRIPTION
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the <b>Subject</b> field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Modify	<p>Click the <b>Edit</b> icon to open a screen with an in-depth list of information about the certificate.</p> <p>Click the <b>Remove</b> icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificate.</p> <p>You cannot delete a certificate that one or more features is configured to use.</p> <p>Do the following to delete a certificate that shows <b>*SELF</b> in the <b>Type</b> field.</p> <ol style="list-style-type: none"> <li>1. Make sure that no other features, such as HTTPS, VPN, SSH are configured to use the <b>*SELF</b> certificate.</li> <li>2. Click the <b>Edit</b> icon next to another self-signed certificate (see the description on the <b>Create</b> button if you need to create a self-signed certificate).</li> <li>3. Select the <b>Default self-signed certificate which signs the imported remote host certificates</b> check box.</li> <li>4. Click <b>Apply</b> to save the changes and return to the <b>My Certificates</b> screen.</li> <li>5. The certificate that originally showed <b>*SELF</b> displays <b>SELF</b> and you can delete it now.</li> </ol> <p>Note that subsequent certificates move up by one when you take this action</p>
Create	Click this to go to the screen where you can have the ZyXEL Device generate a certificate or a certification request.
Import	Click this to open a screen where you can save the certificate that you have enrolled from a certification authority from your computer to the ZyXEL Device.
Refresh	Click this to display the current validity status of the certificates.

## 9.2.1 My Certificate Import

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

Note: You can only import a certificate that matches a corresponding certification request that was generated by the ZyXEL Device.

Note: The certificate you import replaces the corresponding request in the **My Certificates** screen.

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

**Figure 72** My Certificate Import

**Certificates - MY Certificates - Import**

Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

- Binary X.509
- PEM (Base-64) encoded X.509
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7

For my certificate importation to be successful, a certification request corresponding to the imported certificate must already exist on Prestige. After the importation, the certification request will automatically be deleted.

File Path:

---

The following table describes the labels in this screen.

**Table 42** My Certificate Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse</b> to find it.
Browse	Click this to find the certificate file you want to upload.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save the certificate on the ZyXEL Device.
Cancel	Click this to clear your settings.

## 9.2.2 My Certificate Create

Use this screen to have the ZyXEL Device create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request. Click **Security > Certificates > My Certificates > Create** to open the **My Certificate Create** screen.

**Figure 73** My Certificate Create

The following table describes the labels in this screen.

**Table 43** My Certificate Create

LABEL	DESCRIPTION
Certificate Name	Type up to 31 ASCII characters (not including spaces) to identify this certificate.
Subject Information	Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although the <b>Common Name</b> is mandatory. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information.
Common Name	Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 31 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Organizational Unit	Type up to 127 characters to identify the organizational unit or department to which the certificate owner belongs. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
Organization	Type up to 127 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.



LABEL	DESCRIPTION
Country	Type up to 127 characters to identify the nation where the certificate owner is located. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
Key Length	Select a number from the drop-down list box to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
Enrollment Options	These radio buttons deal with how and when the certificate is to be generated.
Create a self-signed certificate	Select <b>Create a self-signed certificate</b> to have the ZyXEL Device generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.
Create a certification request and save it locally for later manual enrollment	Select <b>Create a certification request and save it locally for later manual enrollment</b> to have the ZyXEL Device generate and store a request for a certificate. Use the <b>My Certificate Details</b> screen to view the certification request and copy it to send to the certification authority.  Copy the certification request from the <b>My Certificate Details</b> screen and then send it to the certification authority.
Create a certification request and enroll for a certificate immediately online	Select <b>Create a certification request and enroll for a certificate immediately online</b> to have the ZyXEL Device generate a request for a certificate and apply to a certification authority for a certificate.  You must have the certification authority's certificate already imported in the <b>Trusted CAs</b> screen.  When you select this option, you must select the certification authority's enrollment protocol and the certification authority's certificate from the drop-down list boxes and enter the certification authority's server address. You also need to fill in the <b>Reference Number</b> and <b>Key</b> if the certification authority requires them.
Enrollment Protocol	Select the certification authority's enrollment protocol from the drop-down list box.  <b>Simple Certificate Enrollment Protocol (SCEP)</b> is a TCP-based enrollment protocol that was developed by VeriSign and Cisco.  <b>Certificate Management Protocol (CMP)</b> is a TCP-based enrollment protocol that was developed by the Public Key Infrastructure X.509 working group of the Internet Engineering Task Force (IETF) and is specified in RFC 2510.
CA Server Address	Enter the IP address (or URL) of the certification authority server.
CA Certificate	Select the certification authority's certificate from the <b>CA Certificate</b> drop-down list box.  You must have the certification authority's certificate already imported in the <b>Trusted CAs</b> screen. Click <b>Trusted CAs</b> to go to the <b>Trusted CAs</b> screen where you can view (and manage) the ZyXEL Device's list of certificates of trusted certification authorities.
Request Authentication	When you select <b>Create a certification request and enroll for a certificate immediately online</b> , the certification authority may want you to include a reference number and key to identify you when you send a certification request. Fill in both the <b>Reference Number</b> and the <b>Key</b> fields if your certification authority uses CMP enrollment protocol. Just fill in the <b>Key</b> field if your certification authority uses the SCEP enrollment protocol.
Key	Type the key that the certification authority gave you.
Back	Click this to return to the previous screen without saving.

LABEL	DESCRIPTION
Apply	Click this to save the certificate on the ZyXEL Device.
Cancel	Click this to clear your settings.

After you click Apply in the **My Certificate Create** screen, you see a screen that tells you the ZyXEL Device is generating the self-signed certificate or certification request.

After the ZyXEL Device successfully enrolls a certificate or generates a certification request or a self-signed certificate, you see a screen with a **Return** button that takes you back to the **My Certificates** screen.

If you configured the **My Certificate Create** screen to have the ZyXEL Device enroll a certificate and the certificate enrollment is not successful, you see a screen with a Return button that takes you back to the **My Certificate Create** screen. Click **Return** and check your information in the **My Certificate Create** screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the ZyXEL Device to enroll a certificate online.

### 9.2.3 My Certificate Details

Use this screen to view in-depth certificate information and change the certificate's name. In the case of a self-signed certificate, you can set it to be the one that the ZyXEL Device uses to sign the trusted remote host certificates that you import to the ZyXEL Device. Click **Security >**

**Certificates > My Certificates** to open the **My Certificates** screen. Click the edit icon to open the **My Certificate Details** screen.

**Figure 74** My Certificate Details

The following table describes the labels in this screen.

**Table 44** My Certificate Details

LABEL	DESCRIPTION
Certificate Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this certificate. You may use any character (not including spaces).
Property Default self-signed certificate which signs the imported remote host certificates.	Select this check box to have the ZyXEL Device use this certificate to sign the trusted remote host certificates that you import to the ZyXEL Device. This check box is only available with self-signed certificates.  If this check box is already selected, you cannot clear it in this screen, you must select this check box in another self-signed certificate's details screen. This automatically clears the check box in the details screen of the certificate that was previously set to sign the imported trusted remote host certificates.

LABEL	DESCRIPTION
Certification Path	<p>Click the <b>Refresh</b> button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself).</p> <p>If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The ZyXEL Device does not trust the certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.</p>
Refresh	Click this to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	<p>This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.</p>
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority or generated by the ZyXEL Device.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	<p>This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country.</p> <p>With self-signed certificates, this is the same as the <b>Subject Name</b> field.</p>
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. The ZyXEL Device uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyXEL Device uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.

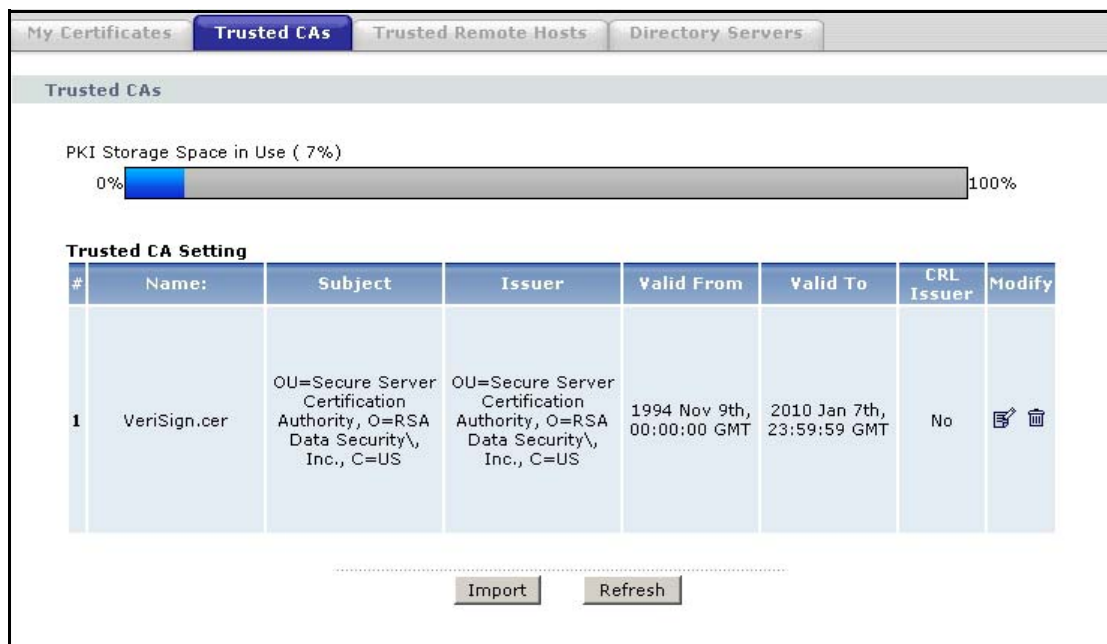
LABEL	DESCRIPTION
MD5 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the MD5 algorithm.
SHA1 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the SHA1 algorithm.
Certificate in PEM (Base-64) Encoded Format	<p>This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form.</p> <p>You can copy and paste a certification request into a certification authority's web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment.</p> <p>You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).</p>
Back	Click this to return to the previous screen without saving.
Export	Click this and then <b>Save</b> in the <b>File Download</b> screen. The <b>Save As</b> screen opens, browse to the location that you want to use and click <b>Save</b> .
Apply	Click this to save your changes. You can only change the name, except in the case of a self-signed certificate, which you can also set to be the default self-signed certificate that signs the imported trusted remote host certificates.
Cancel	Click this to restore your previously saved settings.

## 9.3 The Trusted CAs Screen

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

certificate that is signed by one of these certification authorities. Click **Security > Certificates > Trusted CAs** to open the **Trusted CAs** screen.

**Figure 75** Trusted CAs



The following table describes the labels in this screen.

**Table 45** Trusted CAs

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyXEL Device’s PKI storage space that is currently in use. The bar turns from blue to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate’s owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate’s issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the <b>Subject</b> field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.

LABEL	DESCRIPTION
CRL Issuer	This field displays Yes if the certification authority issues Certificate Revocation Lists for the certificates that it has issued and you have selected the <b>Issues certificate revocation lists (CRL)</b> check box in the certificate's details screen to have the ZyXEL Device check the CRL before trusting any certificates issued by the certification authority. Otherwise the field displays "No".
Modify	Click the Edit icon to open a screen with an in-depth list of information about the certificate.  Click the Remove icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificates. Note that subsequent certificates move up by one when you take this action.
Import	Click this to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the ZyXEL Device.
Refresh	Click this to display the current validity status of the certificates.

### 9.3.1 Trusted CA Import

Follow the instructions in this screen to save a trusted certification authority's certificate to the ZyXEL Device. Click **Security > Certificates > Trusted CAs** to open the **Trusted CAs** screen and then click Import to open the **Trusted CA Import** screen.

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

**Figure 76** Trusted CA Import

The following table describes the labels in this screen.

**Table 46** Trusted CA Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse</b> to find it.
Browse	Click this to find the certificate file you want to upload.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save the certificate on the ZyXEL Device.
Cancel	Click this to restore your previously saved settings.

## 9.3.2 Trusted CA Details

Use this screen to view in-depth information about the certification authority's certificate, change the certificate's name and set whether or not you want the ZyXEL Device to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority. Click **Security > Certificates > Trusted CAs** to open the **Trusted CAs** screen. Click the details icon to open the **Trusted CA Details** screen.

**Figure 77** Trusted CA Details

The following table describes the labels in this screen.

**Table 47** Trusted CA Details

LABEL	DESCRIPTION
Certificate Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Property Issues certificate revocation lists (CRLs)	Select this check box to have the ZyXEL Device check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL).  Clear this check box to have the ZyXEL Device not check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL).



LABEL	DESCRIPTION
Certificate Path	Click the <b>Refresh</b> button to have this read-only text box display the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the end entity's own certificate). The ZyXEL Device does not trust the end entity's certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click this to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country.  With self-signed certificates, this is the same information as in the <b>Subject Name</b> field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyXEL Device uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
CRL Distribution Points	This field displays how many directory servers with Lists of revoked certificates the issuing certification authority of this certificate makes available. This field also displays the domain names or IP addresses of the servers.

LABEL	DESCRIPTION
MD5 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the MD5 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
SHA1 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the SHA1 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form.  You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Back	Click this to return to the previous screen without saving.
Export	Click this and then <b>Save</b> in the <b>File Download</b> screen. The <b>Save As</b> screen opens, browse to the location that you want to use and click <b>Save</b> .
Apply	Click this to save your changes. You can only change the name and/or set whether or not you want the ZyXEL Device to check the CRL that the certification authority issues before trusting a certificate issued by the certification authority.
Cancel	Click this to restore your previously saved settings.

## 9.4 The Trusted Remote Hosts Screens

This screen displays a list of the certificates of peers that you trust but which are not signed by one of the certification authorities on the **Trusted CAs** screen. Click **Security > Certificates > Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen.

You do not need to add any certificate that is signed by one of the certification authorities on the **Trusted CAs** screen since the ZyXEL Device automatically accepts any valid certificate signed by a trusted certification authority as being trustworthy.

**Figure 78** Trusted Remote Hosts

My Certificates Trusted CAs **Trusted Remote Hosts** Directory Servers

Trusted Remote Hosts

PKI Storage Space in Use ( 7%)

0% 100%

**Trusted Remote Host Certificates**  
**Issuer (My Default Self-signed Certificate): CN=P-2602HWL-D1A 001349000001**

#	Name:	Subject	Valid From	Valid To	Modify
1	VeriSign.cer	OU=Secure Server Certification Authority, O=RSA Data Security, Inc., C=US	1994 Nov 9th, 00:00:00 GMT	2010 Jan 7th, 23:59:59 GMT	

Import Refresh

The following table describes the labels in this screen.

**Table 48** Trusted Remote Hosts

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyXEL Device's PKI storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
Issuer (My Default Self-signed Certificate)	This field displays identifying information about the default self-signed certificate on the ZyXEL Device that the ZyXEL Device uses to sign the trusted remote host certificates.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Modify	Click the Edit icon to open a screen with an in-depth list of information about the certificate.  Click the Remove icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action.
Import	Click this to open a screen where you can save the certificate of a remote host (which you trust) from your computer to the ZyXEL Device.
Refresh	Click this to display the current validity status of the certificates.

## 9.4.1 Trusted Remote Hosts Import

Click **Security > Certificates > Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen and then click Import to open the **Trusted Remote Host Import** screen. Follow the instructions in this screen to save a trusted host's certificate to the ZyXEL Device.

Note: The trusted remote host certificate must be a self-signed certificate; and you must remove any spaces from its filename before you can import it.

**Figure 79** Trusted Remote Host Import

The following table describes the labels in this screen.

**Table 49** Trusted Remote Host Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse</b> to find it.
Browse	Click this to find the certificate file you want to upload.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save the certificate on the ZyXEL Device.
Cancel	Click this to restore your previously saved settings.

## 9.4.2 Trusted Remote Host Certificate Details

Use this screen to view in-depth information about the trusted remote host's certificate and/or change the certificate's name. Click **Security > Certificates > Trusted Remote Hosts** to open

the **Trusted Remote Hosts** screen. Click the details icon to open the **Trusted Remote Host Details** screen.

**Figure 80** Trusted Remote Host Details

The following table describes the labels in this screen.

**Table 50** Trusted Remote Host Details

LABEL	DESCRIPTION
Certificate Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Certificate Path	Click the <b>Refresh</b> button to have this read-only text box display the end entity's own certificate and a list of certification authority certificates in the hierarchy of certification authorities that validate a certificate's issuing certification authority. For a trusted host, the list consists of the end entity's own certificate and the default self-signed certificate that the ZyXEL Device uses to sign remote host certificates.
Refresh	Click this to display the certification path.
Certificate Path	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. With trusted remote host certificates, this field always displays CA-signed. The ZyXEL Device is the Certification Authority that signed the certificate. X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.

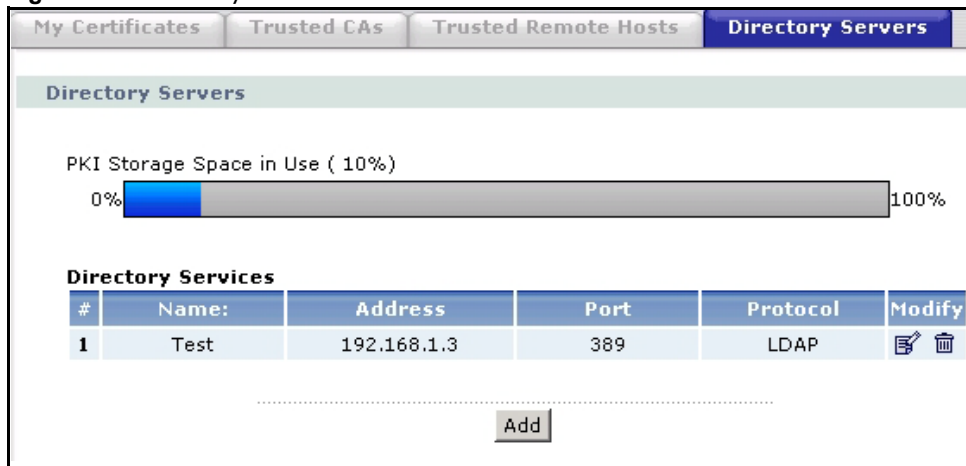
LABEL	DESCRIPTION
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the device that created the certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the default self-signed certificate on the ZyXEL Device that the ZyXEL Device uses to sign the trusted remote host certificates.
Signature Algorithm	This field displays the type of algorithm that the ZyXEL Device used to sign the certificate, which is rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyXEL Device uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
MD5 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the MD5 algorithm. You cannot use this value to verify that this is the remote host's correct certificate because the ZyXEL Device has signed the certificate; thus causing this value to be different from that of the remote host's correct certificate.
SHA1 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the SHA1 algorithm. You cannot use this value to verify that this is the remote host's correct certificate because the ZyXEL Device has signed the certificate; thus causing this value to be different from that of the remote host's correct certificate.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form.  You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Back	Click this to return to the previous screen without saving.
Export	Click this and then <b>Save</b> in the <b>File Download</b> screen. The <b>Save As</b> screen opens, browse to the location that you want to use and click <b>Save</b> .

LABEL	DESCRIPTION
Apply	Click this to save your changes. You can only change the name of the certificate.
Cancel	Click this to restore your previously saved settings.

## 9.5 The Directory Servers Screens

This screen displays a summary list of directory servers (that contain lists of valid and revoked certificates) that have been saved into the ZyXEL Device. If you decide to have the ZyXEL Device check incoming certificates against the issuing certification authority's list of revoked certificates, the ZyXEL Device first checks the server(s) listed in the CRL Distribution Points field of the incoming certificate. If the certificate does not list a server or the listed server is not available, the ZyXEL Device checks the servers listed here. Click **Security > Certificates > Directory Servers** to open the Directory Servers screen.

**Figure 81** Directory Servers



The following table describes the labels in this screen.

**Table 51** Directory Servers

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyXEL Device's PKI storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
#	The index number of the directory server. The servers are listed in alphabetical order.
Name	This field displays the name used to identify this directory server.
Address	This field displays the IP address or domain name of the directory server.
Port	This field displays the port number that the directory server uses.
Protocol	This field displays the protocol that the directory server uses.

LABEL	DESCRIPTION
Modify	Click the Edit icon to open a screen where you can change the information about the directory server.  Click the Remove icon to remove the directory server entry. A window displays asking you to confirm that you want to delete the directory server. Note that subsequent certificates move up by one when you take this action.
Add	Click this to open a screen where you can configure information about a directory server so that the ZyXEL Device can access it.

## 9.5.1 Directory Server Add and Edit

Use this screen to configure information about a directory server that the ZyXEL Device can access. Click **Security > Certificates > Directory Servers** to open the **Directory Servers** screen. Click **Add** (or the details icon) to open the **Directory Server Add** screen.

**Figure 82** Directory Server Add and Edit

The following table describes the labels in this screen.

**Table 52** Directory Server Add and Edit

LABEL	DESCRIPTION
Directory Service Setting	
Name	Type up to 31 ASCII characters (spaces are not permitted) to identify this directory server.
Access Protocol	Use the drop-down list box to select the access protocol used by the directory server.  <b>LDAP</b> (Lightweight Directory Access Protocol) is a protocol over TCP that specifies how clients access directories of certificates and lists of revoked certificates. <sup>1</sup>
Server Address	Type the IP address (in dotted decimal notation) or the domain name of the directory server.



LABEL	DESCRIPTION
Server Port	This field displays the default server port number of the protocol that you select in the <b>Access Protocol</b> field.  You may change the server port number if needed, however you must use the same server port number that the directory server uses.  389 is the default server port number for LDAP.
Login Setting	
Login	The ZyXEL Device may need to authenticate itself in order to assess the directory server. Type the login name (up to 31 ASCII characters) from the entity maintaining the directory server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the directory server (usually a certification authority).
Back	Click this to return to the <b>Directory Servers</b> screen.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

1. At the time of writing, LDAP is the only choice of directory server access protocol.

## 9.6 Certificates Technical Reference

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

### 9.6.1 Certificates Overview

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

The ZyXEL Device uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

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

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

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

## Advantages of Certificates

Certificates offer the following benefits.

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

## Self-signed Certificates

You can have the ZyXEL Device act as a certification authority and sign its own certificates.

### 9.6.2 Private-Public Certificates

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available. The other key is private and must be kept secure.

These keys work like a handwritten signature (in fact, certificates are often referred to as “digital signatures”). Only you can write your signature exactly as it should look. When people know what your signature looks like, they can verify whether something was signed by you, or by someone else. In the same way, your private key “writes” your digital signature and your public key allows people to verify whether data was signed by you, or by someone else. This process works as follows.

- 1 Tim wants to send a message to Jenny. He needs her to be sure that it comes from him, and that the message content has not been altered by anyone else along the way. Tim generates a public key pair (one public key and one private key).
- 2 Tim keeps the private key and makes the public key openly available. This means that anyone who receives a message seeming to come from Tim can read it and verify whether it is really from him or not.
- 3 Tim uses his private key to sign the message and sends it to Jenny.
- 4 Jenny receives the message and uses Tim’s public key to verify it. Jenny knows that the message is from Tim, and that although other people may have been able to read the message, no-one can have altered it (because they cannot re-sign the message with Tim’s private key).
- 5 Additionally, Jenny uses her own private key to sign a message and Tim uses Jenny’s public key to verify the message.

### 9.6.3 Verifying a Trusted Remote Host’s Certificate

Certificates issued by certification authorities have the certification authority’s signature for you to check. Self-signed certificates only have the signature of the host itself. This means that you must be very careful when deciding to import (and thereby trust) a remote host’s self-signed certificate.

## Trusted Remote Host Certificate Fingerprints

A certificate's fingerprints are message digests calculated using the MD5 or SHA1 algorithms. The following procedure describes how to use a certificate's fingerprint to verify that you have the remote host's correct certificate.

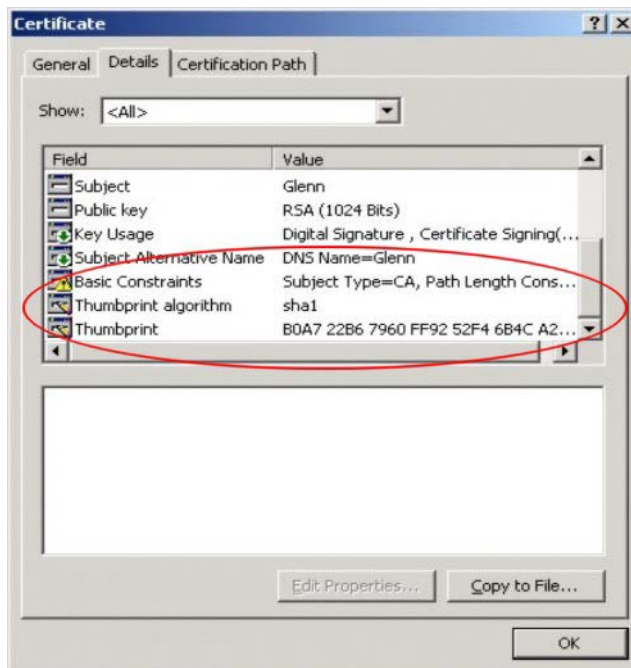
- 1 Browse to where you have the remote host's certificate saved on your computer.
- 2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

**Figure 83** Remote Host Certificates



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

**Figure 84** Certificate Details



- 4 Verify (over the phone for example) that the remote host has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields.



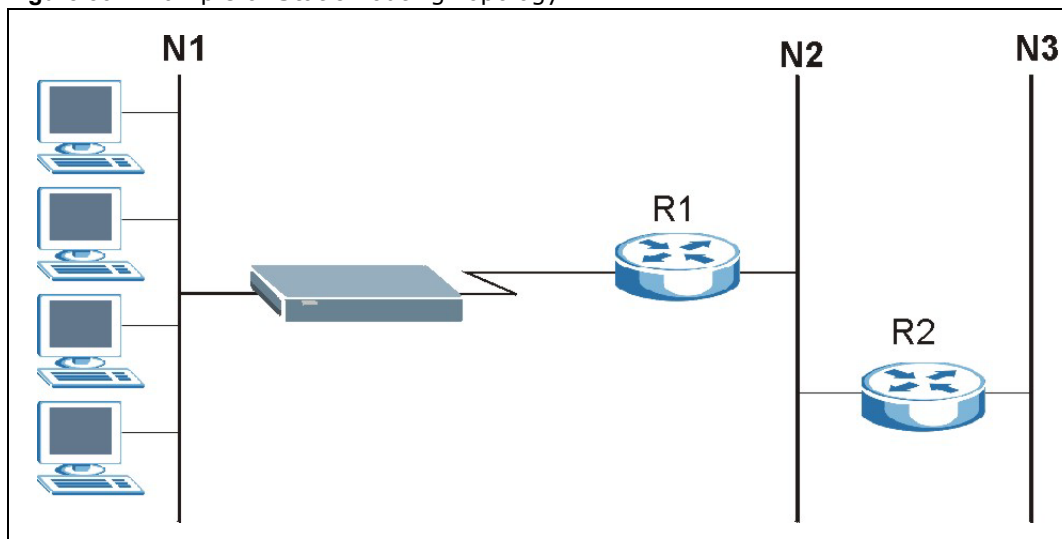
## Static Route

This chapter shows you how to configure static routes for your ZyXEL Device.

### 10.1 Static Route

Each remote node specifies only the network to which the gateway is directly connected, and the ZyXEL Device has no knowledge of the networks beyond. For instance, the ZyXEL Device knows about network N2 in the following figure through remote node Router 1. However, the ZyXEL Device is unable to route a packet to network N3 because it doesn't know that there is a route through the same remote node Router 1 (via gateway Router 2). The static routes are for you to tell the ZyXEL Device about the networks beyond the remote nodes.

**Figure 85** Example of Static Routing Topology



## 10.2 Configuring Static Route

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

**Figure 86** Static Route

#	Active	Name	Destination	Gateway	Subnet Mask	Modify
1	<input checked="" type="checkbox"/>	test	10.10.1.2	192.168.1.3	255.0.0.0	
2	<input type="checkbox"/>	-	-	-	-	
3	<input type="checkbox"/>	-	-	-	-	
4	<input type="checkbox"/>	-	-	-	-	
5	<input type="checkbox"/>	-	-	-	-	
6	<input type="checkbox"/>	-	-	-	-	
7	<input type="checkbox"/>	-	-	-	-	
8	<input type="checkbox"/>	-	-	-	-	
9	<input type="checkbox"/>	-	-	-	-	
10	<input type="checkbox"/>	-	-	-	-	
11	<input type="checkbox"/>	-	-	-	-	
12	<input type="checkbox"/>	-	-	-	-	
13	<input type="checkbox"/>	-	-	-	-	
14	<input type="checkbox"/>	-	-	-	-	
15	<input type="checkbox"/>	-	-	-	-	
16	<input type="checkbox"/>	-	-	-	-	

The following table describes the labels in this screen.

**Table 53** Static Route

LABEL	DESCRIPTION
#	This is the number of an individual static route.
Active	Select the check box to activate this static route. Otherwise, clear the check box.
Name	This is the name that describes or identifies this route.
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Subnet Mask	This is the IP subnet mask.
Modify	Click the Edit icon to go to the screen where you can set up a static route on the ZyXEL Device.  Click the Delete icon to remove a static route from the ZyXEL Device. A window displays asking you to confirm that you want to delete the route.

## 10.2.1 Static Route Edit

Select a static route index number and click **Edit**. The screen shown next appears. Use this screen to configure the required information for a static route.

**Figure 87** Static Route Edit

The following table describes the labels in this screen.

**Table 54** Static Route Edit

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway Type	Use either <b>Gateway Address</b> or <b>Gateway Node</b> to configure a static route.
Gateway IP Address	This field is available when you select <b>Gateway Address</b> from <b>Gateway Type</b> . Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Gateway Node	This field is available when you select <b>Gateway Node</b> from <b>Gateway Type</b> . Select a remote node to set the static route. A remote node is a connection point outside of the local area network. One example of a remote node is your connection to your ISP.
Back	Click <b>Back</b> to return to the previous screen without saving.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.





# Quality Of Service

## 11.1 Overview

Use the QoS screens to set up your ZyXEL Device to use QoS for traffic management.

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control bandwidth. QoS allows the ZyXEL Device to group and prioritize application traffic and fine-tune network performance.

Without QoS, all traffic data are equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical applications such as video-on-demand.

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

### 11.1.1 What You Can Do in the QoS Screens

- Use the **General** screen to enable QoS on the ZyXEL Device, decide allowable bandwidth using QoS and configure priority mapping settings for traffic that does not match a custom class.
- Use the **Class Setup** screen to set up classifiers to sort traffic into different flows and assign priority and define actions to be performed for a classified traffic flow.
- Use the **Monitor** screen to view the ZyXEL Device's QoS-related packet statistics.

### 11.1.2 What You Need to Know About QoS

#### QoS versus Cos

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

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

## Tagging and Marking

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

### 11.1.3 QoS Class Setup Example

In the following figure, your Internet connection has an upstream transmission speed of 50 Mbps. You configure a classifier to assign the highest priority queue (6) to VoIP traffic from the LAN interface, so that voice traffic would not get delayed when there is network congestion. Traffic from the boss's IP address (192.168.1.23 for example) is mapped to queue 5. Traffic that does not

match these two classes are assigned priority queue based on the internal QoS mapping table on the ZyXEL Device.

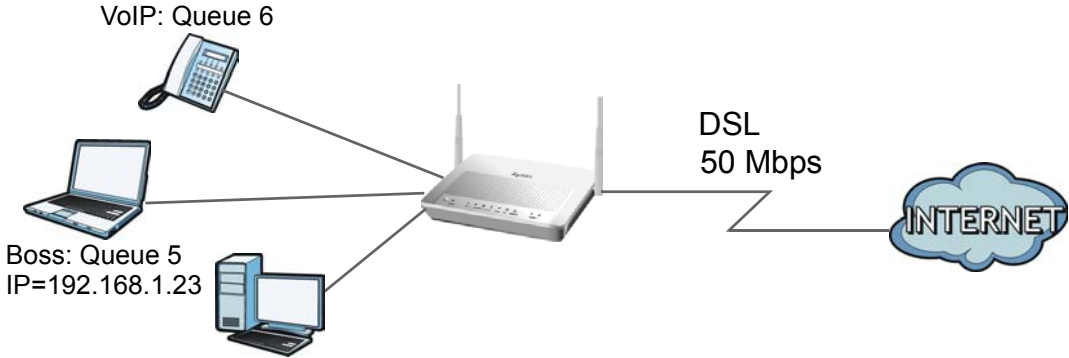


Figure 88 QoS Class Example: VoIP -

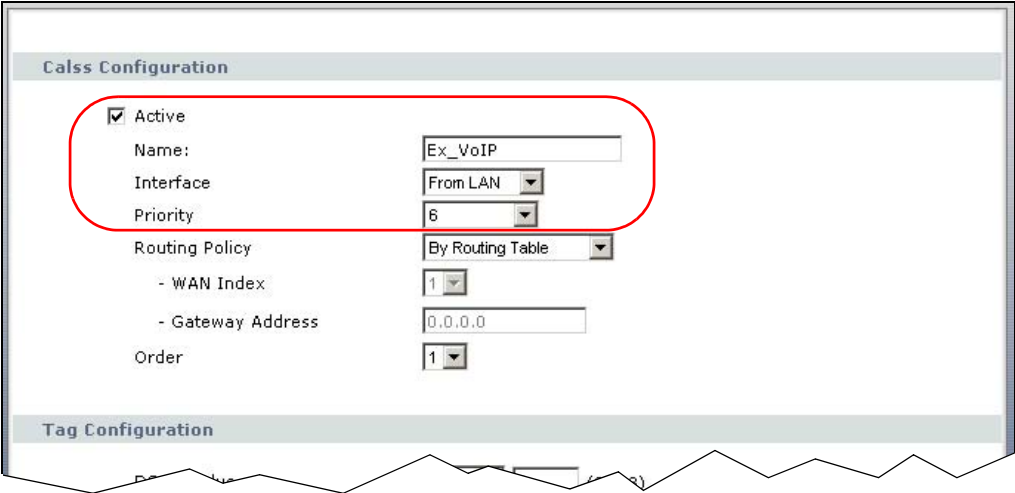


Figure 89 QoS Class Example: VoIP -2

The screenshot shows a configuration window for a QoS class. It is divided into three sections: Source, Destination, and Others. Each section contains several fields with checkboxes and 'Exclude' options. In the 'Others' section, the 'Service' checkbox is checked and the dropdown menu is set to 'VoIP(SIP)', which is highlighted with a red circle. Other settings include Protocol (TCP), Packet Length (0-0), DSCP (0), Ethernet Priority (0-BE), VLAN ID (2), Physical Port (1), and Remote Node (WAN1).

**Source:**

- Address: 0.0.0.0 Subnet Netmask: 0.0.0.0  Exclude
- Port: 0 ~ 0  Exclude
- MAC: 00:00:00:00:00:00 MAC Mask: 00:00:00:00:00:00  Exclude

**Destination:**

- Address: 0.0.0.0 Subnet Netmask: 0.0.0.0  Exclude
- Port: 0 ~ 0  Exclude
- MAC: 00:00:00:00:00:00 MAC Mask: 00:00:00:00:00:00  Exclude

**Others:**

- Service: VoIP(SIP)
- Protocol: TCP 0  Exclude
- Packet Length: 0 ~ 0  Exclude
- DSCP: 0 (0~63)  Exclude
- Ethernet Priority: 0-BE  Exclude
- VLAN ID: 2 (2~4094)  Exclude
- Physical Port: 1  Exclude
- Remote Node: WAN1  Exclude

Buttons: Back, Apply, Cancel

Figure 90 QoS Class Example: Boss -1

The screenshot shows a configuration window for a QoS class. It is divided into two sections: Class Configuration and Tag Configuration. In the 'Class Configuration' section, the 'Active' checkbox is checked and the 'Name' field is set to 'Ex\_Boss', which is highlighted with a red circle. Other settings include Interface (From LAN), Priority (5), Routing Policy (By Routing Table), WAN Index (1), Gateway Address (0.0.0.0), and Order (2).

**Class Configuration:**

- Active
- Name: Ex\_Boss
- Interface: From LAN
- Priority: 5
- Routing Policy: By Routing Table
- WAN Index: 1
- Gateway Address: 0.0.0.0
- Order: 2

**Tag Configuration:**

Figure 91 QoS Class Example: Boss -2

The screenshot shows a configuration window titled "QoS Class Example: Boss -2". It is divided into three main sections: Source, Destination, and Others. Each section contains various fields and checkboxes for configuration. The "Source" section is highlighted with a red circle. At the bottom, there are "Back", "Apply", and "Cancel" buttons.

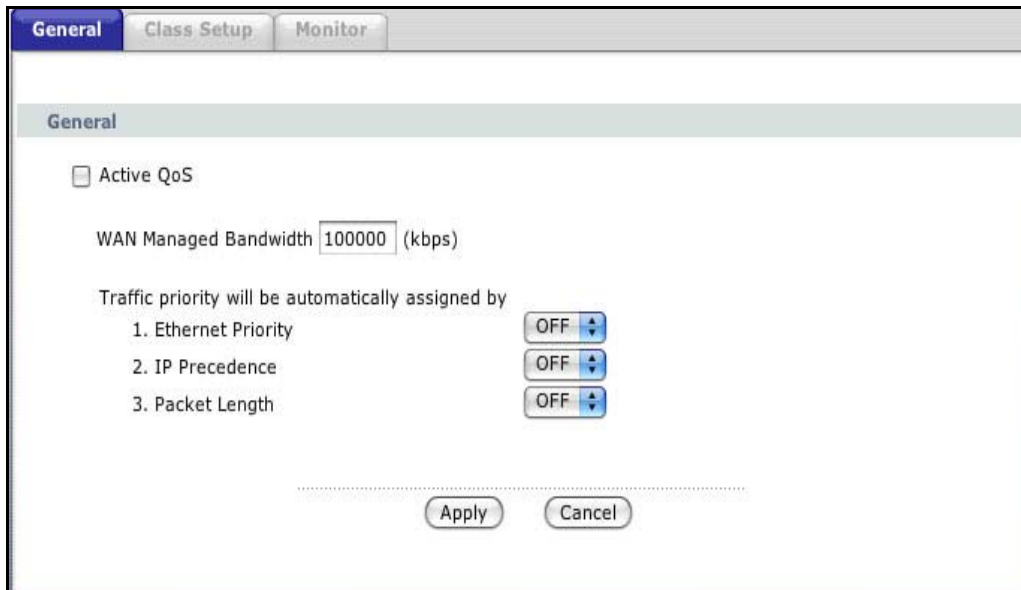
Section	Field	Value	Exclude
Source	<input checked="" type="checkbox"/> Address	192.168.1.23	<input type="checkbox"/> Exclude
	<input type="checkbox"/> Port	0 ~ 0	<input type="checkbox"/> Exclude
	<input type="checkbox"/> MAC	00:00:00:00:00:00	<input type="checkbox"/> Exclude
Destination	<input type="checkbox"/> Address	0.0.0.0	<input type="checkbox"/> Exclude
	<input type="checkbox"/> Port	0 ~ 0	<input type="checkbox"/> Exclude
	<input type="checkbox"/> MAC	00:00:00:00:00:00	<input type="checkbox"/> Exclude
Others	<input type="checkbox"/> Service	FTP	<input type="checkbox"/> Exclude
	<input type="checkbox"/> Protocol	TCP	<input type="checkbox"/> Exclude
	<input type="checkbox"/> Packet Length	0 ~ 0	<input type="checkbox"/> Exclude
	<input type="checkbox"/> DSCP	0 (0~63)	<input type="checkbox"/> Exclude
	<input type="checkbox"/> Ethernet Priority	0-BE	<input type="checkbox"/> Exclude
	<input type="checkbox"/> VLAN ID	2 (2~4094)	<input type="checkbox"/> Exclude
	<input type="checkbox"/> Physical Port	1	<input type="checkbox"/> Exclude
	<input type="checkbox"/> Remote Node	WAN1	<input type="checkbox"/> Exclude

## 11.2 The QoS General Screen

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

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

**Figure 92** Advanced > QoS > General



The following table describes the labels in this screen.

**Table 55** Advanced > QoS > General

LABEL	DESCRIPTION
Active QoS	Select the check box to turn on QoS to improve your network performance.  You can give priority to traffic that the ZyXEL Device forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.
WAN Managed Bandwidth	Enter the amount of bandwidth for the WAN interface that you want to allocate using QoS.  The recommendation is to set this speed to match the interface’s actual transmission speed. For example, set the WAN interface speed to 1000 kbps if your Internet connection has an upstream transmission speed of 1 Mbps.  You can set this number higher than the interface’s actual transmission speed. This will stop lower priority traffic from being sent if higher priority traffic uses all of the actual bandwidth.  You can also set this number lower than the interface’s actual transmission speed. This will cause the ZyXEL Device to not use some of the interface’s available bandwidth.
Traffic priority will be automatically assigned by	These fields are ignored if traffic matches a class you configured in the <b>Class Setup</b> screen.  If you select <b>ON</b> and traffic does not match a class configured in the <b>Class Setup</b> screen, the ZyXEL Device assigns priority to unmatched traffic based on the IEEE 802.1p priority level, IP precedence and/or packet length.  If you select <b>OFF</b> , traffic which does not match a class is mapped to queue two.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

## 11.3 The Class Setup Screen

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

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

**Figure 93** Advanced > QoS > Class Setup

The following table describes the labels in this screen.

**Table 56** Advanced > QoS > Class Setup

LABEL	DESCRIPTION
Create a new Class	Click this to create a new classifier.
No	This is the number of each classifier. The ordering of the classifiers is important as the classifiers are applied in turn.
Active	Select the check box to enable this classifier.
Name	This is the name of the classifier.
Interface	This shows the interface from which traffic of this classifier should come.
Priority	This is the priority assigned to traffic of this classifier.
Filter Content	This shows criteria specified in this classifier.
Modify	Click the Edit icon to go to the screen where you can edit the classifier. Click the Remove icon to delete an existing classifier.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

### 11.3.1 The Class Configuration Screen

Use this screen to configure a classifier. Click the **Add** button or the **Edit** icon in the **Modify** field to display the following screen.

**Figure 94** Advanced > QoS > Class Setup: Edit

The screenshot shows the 'Class Configuration' screen with three main sections: Class Configuration, Tag Configuration, and Filter Configuration. The Class Configuration section includes fields for Name (Default), Interface (From LAN), Priority (2 (Default)), Routing Policy (By Routing Table), WAN Index, Gateway Address (0.0.0.0), and Order. The Tag Configuration section includes DSCP Value (Same), 802.1Q Tag (Same), Ethernet Priority (0 BE), and VLAN ID (2). The Filter Configuration section includes Source and Destination criteria (Address, Port, MAC) and Others criteria (Service, Protocol, Packet Length, DSCP, Ethernet Priority, VLAN ID, Remote Node), each with an 'Exclude' checkbox. At the bottom are 'Back', 'Apply', and 'Cancel' buttons.

The following table describes the labels in this screen.

**Table 57** Advanced > QoS > Class Setup: Edit (continued)

LABEL	DESCRIPTION
Class Configuration	
Active	Select the check box to enable this classifier.
Name	The text may consist of up to 20 letters, numerals and any printable character found on a typical English language keyboard.
Interface	Select from which interface traffic of this class should come.
Priority	Select a priority level (between 0 and 7) or select <b>Auto</b> to have the ZyXEL Device map the matched traffic to a queue according to the internal QoS mapping table.  "0" is the lowest priority level and "7" is the highest.



LABEL	DESCRIPTION
Routing Policy	<p>Select the next hop to which traffic of this class should be forwarded.</p> <p>Select <b>By Routing Table</b> to have the ZyXEL Device use the routing table to find a next hop and forward the matched packets automatically.</p> <p>Select <b>To WAN Index</b> to route the matched packets through the specified PVC. This option is available only when the WAN type is ADSL.</p> <p>Select <b>To Gateway Address</b> to route the matched packets to the router or switch you specified in the <b>Gateway Address</b> field.</p>
WAN Index	Select a PVC index number.
Gateway Address	Enter the IP address of the gateway, which should be a router or switch on the same segment as the ZyXEL Device's interface(s), that can forward the packet to the destination.
Order	This shows the ordering number of this classifier. Select an existing number for where you want to put this classifier and click <b>Apply</b> to move the classifier to the number you selected. For example, if you select 2, the classifier you are moving becomes number 2 and the previous classifier 2 gets pushed down one.
Tag Configuration	
DSCP Value	<p>Select <b>Same</b> to keep the DSCP fields in the packets.</p> <p>Select <b>Auto</b> to map the DSCP value to 802.1 priority level automatically.</p> <p>Select <b>Mark</b> to set the DSCP field with the value you configure in the field provided.</p>
802.1Q Tag	<p>Select <b>Same</b> to keep the priority setting and VLAN ID of the frames.</p> <p>Select <b>Auto</b> to map the 802.1 priority level to the DSCP value automatically.</p> <p>Select <b>Remove</b> to delete the priority queue tag and VLAN ID of the frames.</p> <p>Select <b>Mark</b> to replace the 802.1 priority field and VLAN ID with the value you set in the fields below.</p> <p>Select <b>Add</b> to treat all matched traffic untagged and add a second priority queue tag and VLAN.</p>
Ethernet Priority	Select a priority level (between 0 and 7) from the drop down list box.
VLAN ID	Specify a VLAN ID number between 2 and 4094.
Filter Configuration	
Use the following fields to configure the criteria for traffic classification.	
Source	
Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
Subnet Netmask	Enter the source subnet mask. Refer to the appendix for more information on IP subnetting.
Port	Select the check box and enter the port number of the source. 0 means any source port number.
MAC	Select the check box and enter the source MAC address of the packet.
MAC Mask	<p>Type the mask for the specified MAC address to determine which bits a packet's MAC address should match.</p> <p>Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.</p>

LABEL	DESCRIPTION
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Destination	
Address	Select the check box and enter the destination IP address in dotted decimal notation.
Subnet Netmask	Enter the destination subnet mask. Refer to the appendix for more information on IP subnetting.
Port	Select the check box and enter the port number of the destination. 0 means any source port number.
MAC	Select the check box and enter the destination MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match.  Enter "f" for each bit of the specified destination MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Others	
Service	This field simplifies classifier configuration by allowing you to select a predefined application. When you select a predefined application, you do not configure the rest of the filter fields.  SIP (Session Initiation Protocol) is a signaling protocol used in Internet telephony, instant messaging and other VoIP (Voice over IP) applications. Select the check box and select <b>VoIP(SIP)</b> from the drop-down list box to configure this classifier for traffic that uses SIP.  File Transfer Protocol (FTP) is an Internet file transfer service that operates on the Internet and over TCP/IP networks. A system running the FTP server accepts commands from a system running an FTP client. The service allows users to send commands to the server for uploading and downloading files. Select the check box and select <b>FTP</b> from the drop-down list box to configure this classifier for FTP traffic.
Protocol	Select this option and select the protocol ( <b>TCP</b> or <b>UDP</b> ) or select <b>User defined</b> and enter the protocol (service type) number. 0 means any protocol number.
Packet Length	Select this option and enter the minimum and maximum packet length (from 28 to 1500) in the fields provided.
DSCP	Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
Ethernet Priority	Select this option and select a priority level (between 0 and 7) from the drop down list box.  "0" is the lowest priority level and "7" is the highest.
VLAN ID	Select this option and specify a VLAN ID number between 2 and 4094.
Physical Port	Select this option and select a LAN port.
Remote Node	Select this option and select a remote node from the drop down list box. When the WAN type is <b>Ethernet</b> in the <b>WAN &gt; Internet Access Setup</b> screen, you can select <b>WAN1</b> only.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.

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

## 11.4 The QoS Monitor Screen

Use this screen to view the ZyXEL Device's QoS packet statistics. Click Advanced > QoS > Monitor. The screen appears as shown.

**Figure 95** Advanced > QoS > Monitor

Priority Queue	Pass	Drop
0	0 bps	0 bps
1	0 bps	0 bps
2	0 bps	0 bps
3	0 bps	0 bps
4	0 bps	0 bps
5	0 bps	0 bps
6	0 bps	0 bps
7	0 bps	0 bps

Poll Interval(s) :  sec

The following table describes the labels in this screen.

**Table 58** Advanced > QoS > Monitor

LABEL	DESCRIPTION
Priority Queue	This shows the priority queue number. Traffic assigned to higher index queues gets through faster while traffic in lower index queues is dropped if the network is congested.
Pass	This shows how many packets mapped to this priority queue are transmitted successfully.
Drop	This shows how many packets mapped to this priority queue are dropped.
Poll Interval(s)	Enter the time interval for refreshing statistics in this field.

LABEL	DESCRIPTION
Set Interval	Click this to apply the new poll interval you entered in the <b>Poll Interval(s)</b> field.
Stop	Click this to stop refreshing statistics.

## 11.5 QoS Technical Reference

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

### 11.5.1 IEEE 802.1Q Tag

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

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

**Table 59** IEEE 802.1p Priority Level and Traffic Type

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

### 11.5.2 IP Precedence

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

### 11.5.3 DiffServ

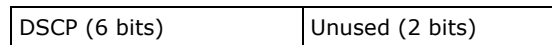
QoS is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

Differentiated Services (DiffServ) is a Class of Service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

#### DSCP and Per-Hop Behavior

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

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



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

### 11.5.4 Automatic Priority Queue Assignment

If you enable QoS on the ZyXEL Device, the ZyXEL Device can automatically base on the IEEE 802.1p priority level, IP precedence and/or packet length to assign priority to traffic which does not match a class.

The following table shows you the internal layer-2 and layer-3 QoS mapping on the ZyXEL Device. On the ZyXEL Device, traffic assigned to higher priority queues gets through faster while traffic in lower index queues is dropped if the network is congested.

**Table 60** Internal Layer2 and Layer3 QoS Mapping

PRIORITY QUEUE	LAYER 2	LAYER 3		
	IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY)	TOS (IP PRECEDENCE)	DSCP	IP PACKET LENGTH (BYTE)
0	1	0	000000	
1	2			
2	0	0	000000	>1100

PRIORITY QUEUE	LAYER 2	LAYER 3		
	IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY)	TOS (IP PRECEDENCE)	DSCP	IP PACKET LENGTH (BYTE)
3	3	1	001110 001100 001010 001000	250~1100
4	4	2	010110 010100 010010 010000	
5	5	3	011110 011100 011010 011000	<250
6	6	4	100110 100100 100010 100000	
		5	101110 101000	
7	7	6	110000	
		7	111000	

# Dynamic DNS Setup

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

## 12.1 Dynamic DNS Overview

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

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

### 12.1.1 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.

See [Section 12.2 on page 159](#) for configuration instruction.

## 12.2 Configuring Dynamic DNS

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

See [Section 12.1 on page 159](#) for more information.

**Figure 96** Dynamic DNS

The following table describes the fields in this screen.

**Table 61** Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Active Dynamic DNS	Select this check box to use dynamic DNS.
Service Provider	This is the name of your Dynamic DNS service provider.
Dynamic DNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.
Host Name	Type the domain name assigned to your ZyXEL Device by your Dynamic DNS provider. You can specify up to two host names in the field separated by a comma (",").
User Name	Type your user name.
Password	Type the password assigned to you.
Enable Wildcard Option	Select the check box to enable DynDNS Wildcard.
Enable off line option	This option is available when <b>Custom DNS</b> is selected in the <b>DDNS Type</b> field. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
IP Address Update Policy	
Use WAN IP Address	Select this option to update the IP address of the host name(s) to the WAN IP address.



**Table 61** Dynamic DNS (continued)

LABEL	DESCRIPTION
Dynamic DNS server auto detect IP Address	Select this option only when there are one or more NAT routers between the ZyXEL Device and the DDNS server. This feature has the DDNS server automatically detect and use the IP address of the NAT router that has a public IP address.  Note: The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the ZyXEL Device and the DDNS server.
Use specified IP Address	Type the IP address of the host name(s). Use this if you have a static IP address.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.



# Remote Management Configuration

This chapter provides information on configuring remote management.

## 13.1 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 **Access Status** 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

### 13.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

- You have disabled that service in one of the remote management screens.
- 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.
- There is a firewall rule that blocks it.

### 13.1.2 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.

### 13.1.3 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.

## 13.2 The WWW Screen

To change your ZyXEL Device's World Wide Web settings, click **Advanced > Remote MGMT** to display the **WWW** screen.

### 13.2.1 WWW and HTTPS

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).

It relies upon certificates, public keys, and private keys.

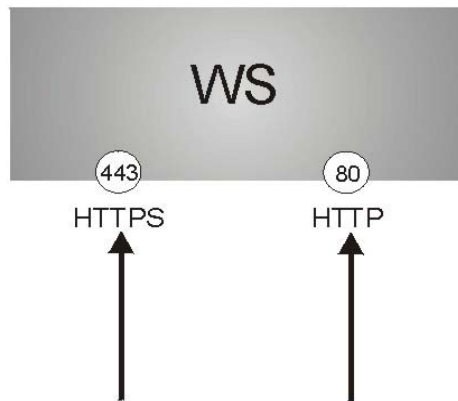
HTTPS on the ZyXEL Device is used so that you may securely access the ZyXEL Device using the web configurator. The SSL protocol specifies that the SSL server (the ZyXEL Device) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the ZyXEL Device), whereas the SSL client only should authenticate itself when the SSL server requires it to do so (select **Authenticate Client Certificates** in the **Remote MGMT > WWW** screen). **Authenticate Client Certificates** is optional and if selected means the SSL-client must send the ZyXEL Device a certificate. You must apply for a certificate for the browser from a CA that is a trusted CA on the ZyXEL Device.

Please refer to the following figure.

- 1 HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the ZyXEL Device's WS (web server).

- 2 HTTP connection requests from a web browser go to port 80 (by default) on the ZyXEL Device's WS (web server).

**Figure 97** HTTPS Implementation



Note: If you disable the WWW service in the Remote MGMT > WWW screen, then the ZyXEL Device blocks all HTTP connection attempts.

**Figure 98** Remote Management: WWW

The screenshot shows the configuration interface for the WWW and HTTPS services. The top navigation bar includes tabs for WWW, Telnet, FTP, SNMP, DNS, and ICMP. The WWW section is currently selected and shows the following settings:

- Port: 80
- LAN Access Status: Enable
- LAN Access Authentication: Enable
- WAN Access Status: Disable
- Secured Client IP:  All  Selected

The HTTPS section shows the following settings:

- Server Host Key: auto\_generated\_self\_signed\_cert (See [My Certificates](#))
- Authenticate Client Certificates (See [Trusted CAs](#))
- Port: 443
- LAN Access Status: LAN & WAN
- Secured Client IP:  All  Selected

**Note :**

- 1: For [UPnP](#) to function normally, the HTTP service must be available for LAN computers using [UPnP](#).
- 2: You may also need to create a [Firewall](#) rule
- 3: WWW WAN access will have a 20 minute expiry.

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

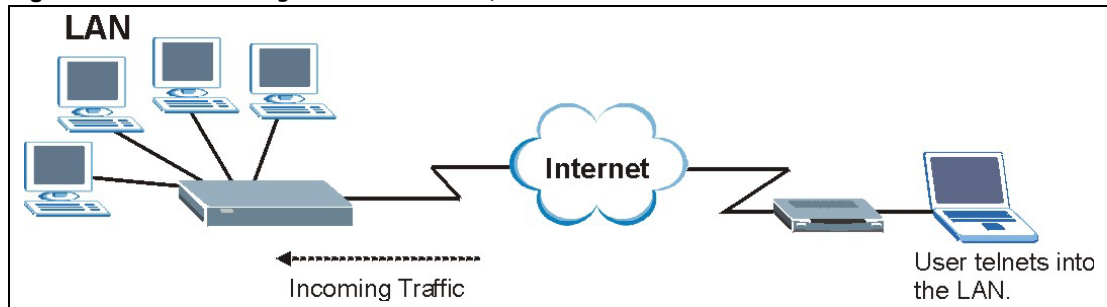
The following table describes the labels in this screen.

LABEL	DESCRIPTION
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
LAN Access Status	Select <b>Enable</b> to use the LAN interface for Access Status. When Access Status is enabled on the LAN interface, this is the interface(s) through which a computer may access the ZyXEL Device using this service. Select <b>Disable</b> to discontinue Access Status on the LAN interface.
LAN Access Authentication	Select <b>Enable</b> to enforce authentication for access on the LAN interface. Access Status must first be enabled on the LAN interface to use authentication. Select <b>Disable</b> to discontinue authentication for access on the LAN interface.
WAN Access Status	Select <b>Enable</b> to use the WAN interface for Access Status. When Access Status is enabled on the WAN interface, this is the interface(s) through which a computer may access the ZyXEL Device using this service. Select <b>Disable</b> to discontinue Access Status on the WAN interface.
Secured Client IP	A secured client is a "trusted" computer that is allowed to communicate with the ZyXEL Device using this service.  Select <b>All</b> to allow any computer to access the ZyXEL Device using this service.  Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
HTTPS	
Server Host Key	Select the <b>Server Host Key</b> that the ZyXEL Device will use to identify itself. The ZyXEL Device is the SSL server and must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the ZyXEL Device).
Authenticate Client Certificates	Select <b>Authenticate Client Certificates</b> (optional) to require the SSL client to authenticate itself with the ZyXEL Device by sending the ZyXEL Device a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the ZyXEL Device.
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP	A secured client is a "trusted" computer that is allowed to communicate with the ZyXEL Device using this service.  Select <b>All</b> to allow any computer to access the ZyXEL Device using this service.  Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click <b>Apply</b> to save your settings back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 13.3 Telnet

You can configure your ZyXEL Device for remote Telnet access as shown next. The administrator uses Telnet from a computer on a remote network to access the ZyXEL Device.

**Figure 99** Telnet Configuration on a TCP/IP Network



## 13.4 Configuring Telnet

Click **Advanced > Remote MGMT > Telnet** tab to display the screen as shown.

**Figure 100** Remote Management: Telnet

The screenshot shows the 'Telnet' configuration page. At the top, there are tabs for 'WWW', 'Telnet', 'FTP', 'SNMP', 'DNS', and 'ICMP'. The 'Telnet' tab is active. Below the tabs, the configuration options are:
 

- Port:** A text box containing '23'.
- LAN Access Status:** A dropdown menu with 'LAN' selected.
- Secured Client IP:** Radio buttons for 'All' (selected) and 'Selected', followed by a text box containing '0.0.0.0'.

 A note with a hand icon says: 'Note: You may also need to create a [Firewall rule](#)'. At the bottom, there are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

**Table 62** Remote Management: Telnet

LABEL	DESCRIPTION
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP	A secured client is a "trusted" computer that is allowed to communicate with the ZyXEL Device using this service.  Select <b>All</b> to allow any computer to access the ZyXEL Device using this service.  Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.

**Table 62** Remote Management: Telnet

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 13.5 Configuring FTP

You can upload and download the ZyXEL Device's firmware and configuration files using FTP, please see the chapter on firmware and configuration file maintenance for details. To use this feature, your computer must have an FTP client.

To change your ZyXEL Device's FTP settings, click **Advanced > Remote MGMT > FTP** tab. The screen appears as shown.

**Figure 101** Remote Management: FTP

The following table describes the labels in this screen.

**Table 63** Remote Management: FTP

LABEL	DESCRIPTION
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP	A secured client is a "trusted" computer that is allowed to communicate with the ZyXEL Device using this service. Select <b>All</b> to allow any computer to access the ZyXEL Device using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

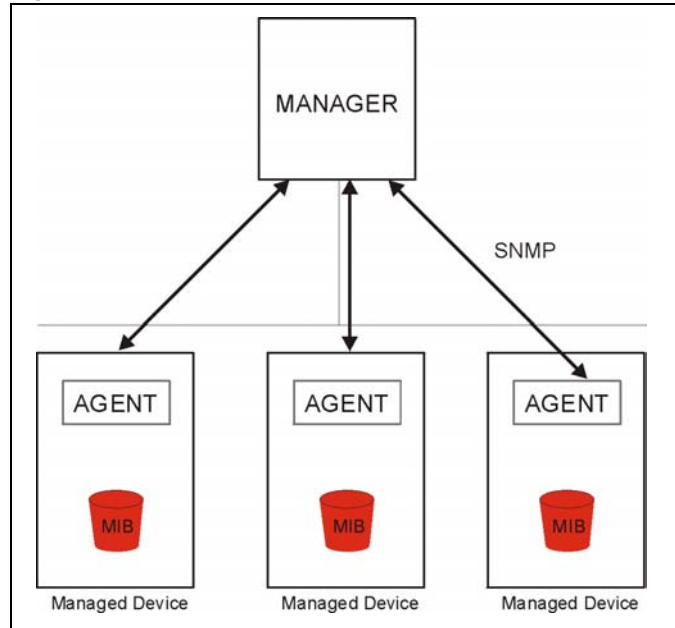


## 13.6 SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyXEL Device supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyXEL Device through the network. The ZyXEL Device supports SNMP version one (SNMPv1) and version two (SNMPv2). The next figure illustrates an SNMP management operation.

Note: SNMP is only available if TCP/IP is configured.

**Figure 102** SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the ZyXEL Device). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.

- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

### 13.6.1 Supported MIBs

The ZyXEL Device supports MIB II that is defined in RFC-1213 and RFC-1215. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

### 13.6.2 SNMP Traps

The ZyXEL Device will send traps to the SNMP manager when any one of the following events occurs:

**Table 64** SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
0	coldStart (defined in <i>RFC-1215</i> )	A trap is sent after booting (power on).
1	warmStart (defined in <i>RFC-1215</i> )	A trap is sent after booting (software reboot).
6	whyReboot (defined in ZYXEL-MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).
6a	For intentional reboot:	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CI command "sys reboot", etc.).
6b	For fatal error:	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.

### 13.6.3 Configuring SNMP

To change your ZyXEL Device's SNMP settings, click **Advanced > Remote MGMT > SNMP**. The screen appears as shown.

**Figure 103** Remote Management: SNMP

The following table describes the labels in this screen.

**Table 65** Remote Management: SNMP

LABEL	DESCRIPTION
SNMP	
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP	A secured client is a "trusted" computer that is allowed to communicate with the ZyXEL Device using this service. Select <b>All</b> to allow any computer to access the ZyXEL Device using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
SNMP Configuration	
Get Community	Enter the <b>Get Community</b> , which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the <b>Set community</b> , which is the password for incoming Set requests from the management station. The default is public and allows all requests.
Trap	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.

**Table 65** Remote Management: SNMP

LABEL	DESCRIPTION
Destination	Type the IP address of the station to send your SNMP traps to.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 13.7 Configuring DNS

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. Refer to the chapter on LAN for background information.

To change your ZyXEL Device's DNS settings, click **Advanced > Remote MGMT > DNS**. The screen appears as shown. Use this screen to set from which IP address the ZyXEL Device will accept DNS queries and on which interface it can send them your ZyXEL Device's DNS settings.

**Figure 104** Remote Management: DNS

The following table describes the labels in this screen.

**Table 66** Remote Management: DNS

LABEL	DESCRIPTION
Port	The DNS service port number is 53.
Access Status	Select the interface(s) through which a computer may send DNS queries to the ZyXEL Device.
Secured Client IP	A secured client is a "trusted" computer that is allowed to send DNS queries to the ZyXEL Device. Select <b>All</b> to allow any computer to send DNS queries to the ZyXEL Device. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to send DNS queries to the ZyXEL Device.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 13.8 Configuring ICMP

To change your ZyXEL Device's security settings, click **Advanced > Remote MGMT > ICMP**. The screen appears as shown.

If an outside user attempts to probe an unsupported port on your ZyXEL Device, an ICMP response packet is automatically returned. This allows the outside user to know the ZyXEL Device exists. Your ZyXEL Device supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your ZyXEL Device when unsupported ports are probed.

**Figure 105** Remote Management: ICMP

The following table describes the labels in this screen.

**Table 67** Remote Management: ICMP

LABEL	DESCRIPTION
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The ZyXEL Device will not respond to any incoming Ping requests when <b>Disable</b> is selected. Select <b>LAN</b> to reply to incoming LAN Ping requests. Select <b>WAN</b> to reply to incoming WAN Ping requests. Otherwise select <b>LAN &amp; WAN</b> to reply to both incoming LAN and WAN Ping requests.
Do not respond to requests for unauthorized services	Select this option to prevent hackers from finding the ZyXEL Device by probing for unused ports. If you select this option, the ZyXEL Device will not respond to port request(s) for unused ports, thus leaving the unused ports and the ZyXEL Device unseen. If this option is not selected, the ZyXEL Device will reply with an ICMP port unreachable packet for a port probe on its unused UDP ports and a TCP reset packet for a port probe on its unused TCP ports.  Note that the probing packets must first traverse the ZyXEL Device's firewall rule checks before reaching this anti-probing mechanism. Therefore if a firewall rule stops a probing packet, the ZyXEL Device reacts based on the firewall rule to either send a TCP reset packet for a blocked TCP packet (or an ICMP port-unreachable packet for a blocked UDP packets) or just drop the packets without sending a response packet.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

# Universal Plug-and-Play (UPnP)

This chapter introduces the UPnP feature in the web configurator.

## 14.1 Introducing Universal Plug and Play

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 14.2.1 on page 175](#) for configuration instructions.

### 14.1.1 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.

### 14.1.2 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.

### 14.1.3 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.

## 14.2 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.

### 14.2.1 Configuring UPnP

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

See [Section 14.1 on page 174](#) for more information.

**Figure 106** Configuring UPnP

The following table describes the fields in this screen.

**Table 68** Configuring UPnP

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

## 14.3 Installing UPnP in Windows Example

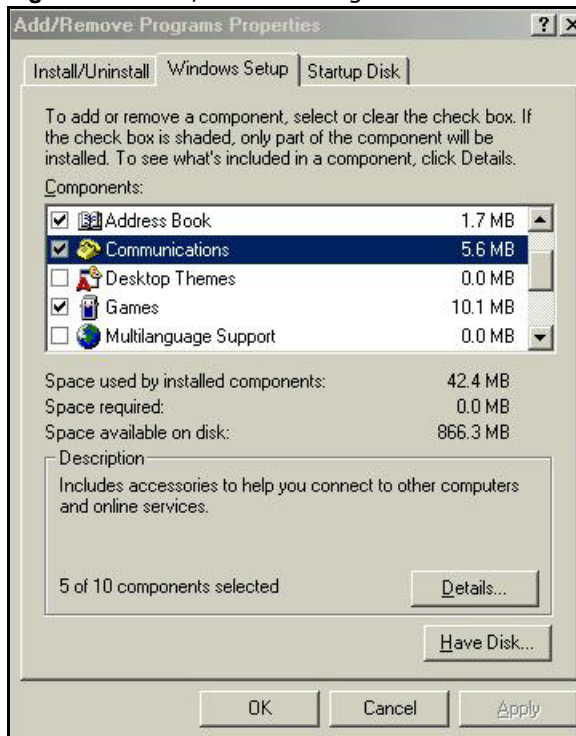
This section shows how to install UPnP in Windows Me and Windows XP.

### 14.3.1 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**.

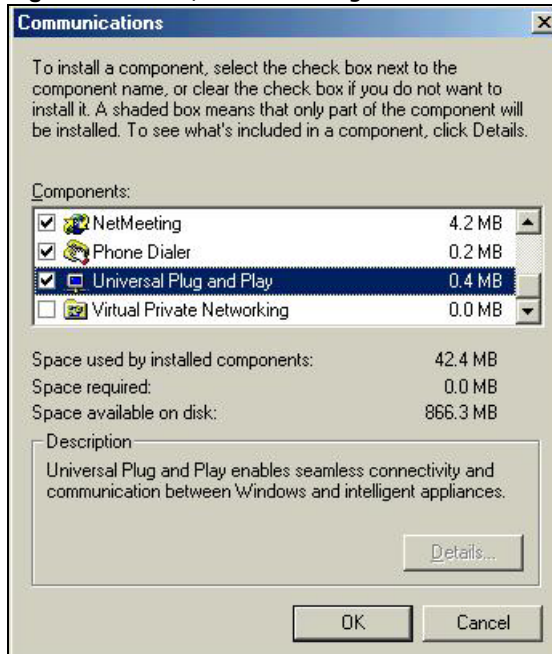
**Figure 107** Add/Remove Programs: Windows Setup: Communication





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

**Figure 108** Add/Remove Programs: Windows Setup: Communication: Components



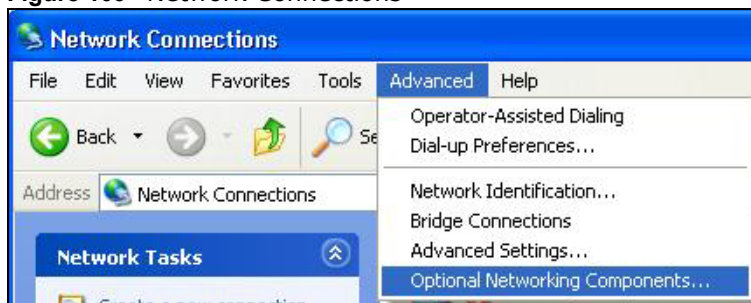
- 4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.
- 5 Restart the computer when prompted.

## 14.3.2 Installing UPnP in Windows XP

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

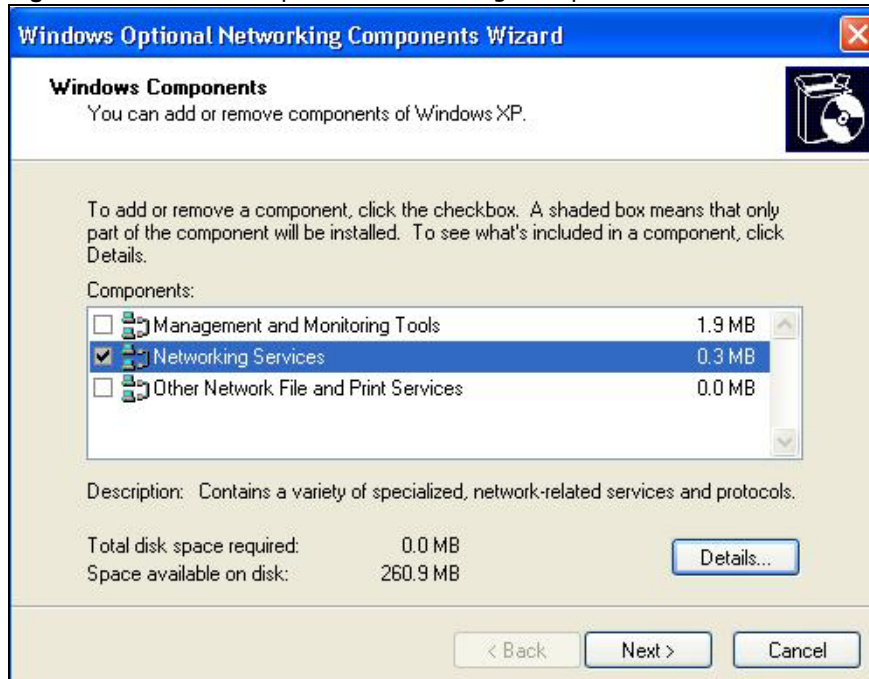
- 1 Click **start** and **Control Panel**.
- 2 Double-click **Network Connections**.
- 3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ...**

**Figure 109** Network Connections



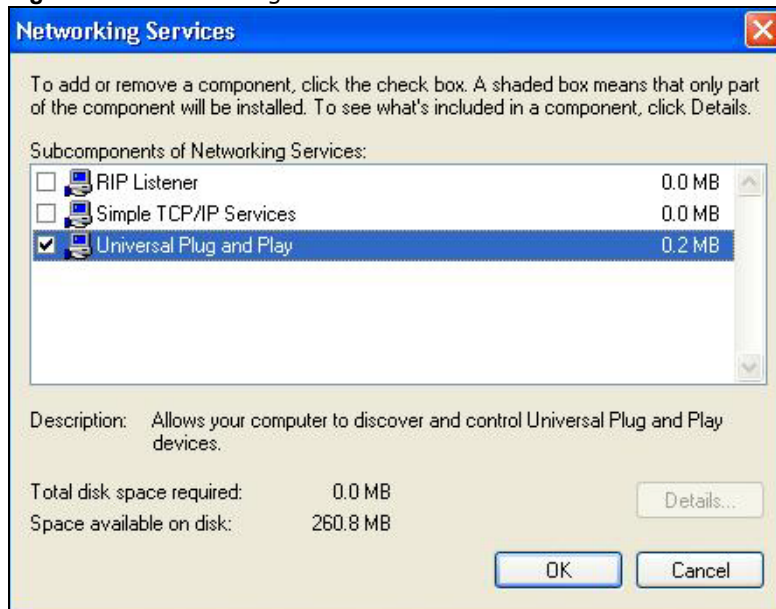
- 4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

**Figure 110** Windows Optional Networking Components Wizard



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

**Figure 111** Networking Services



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

## 14.4 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.

### 14.4.1 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 112** Network Connections



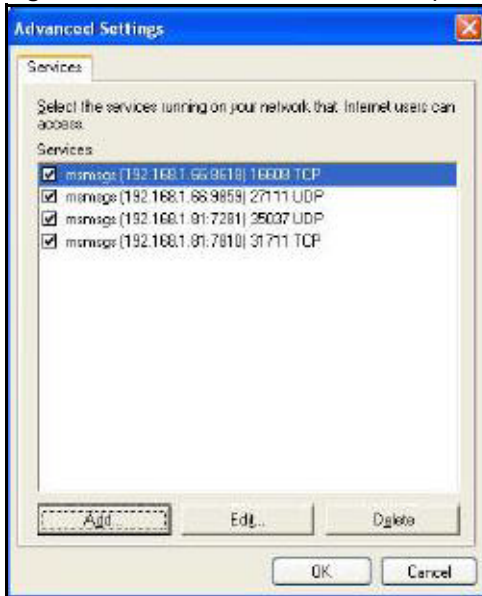
- 3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

**Figure 113** Internet Connection Properties

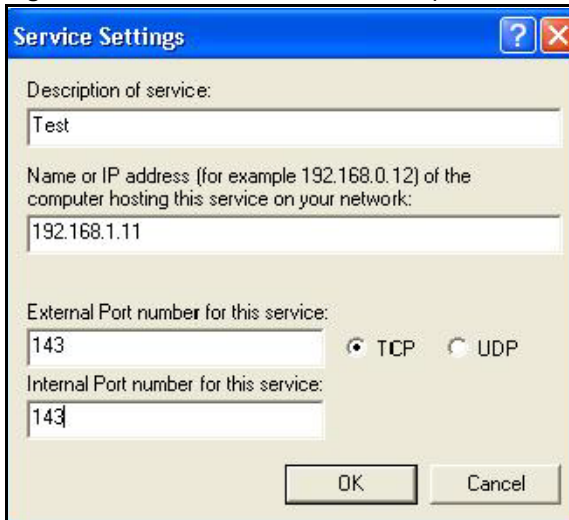


- You may edit or delete the port mappings or click **Add** to manually add port mappings.

**Figure 114** Internet Connection Properties: Advanced Settings



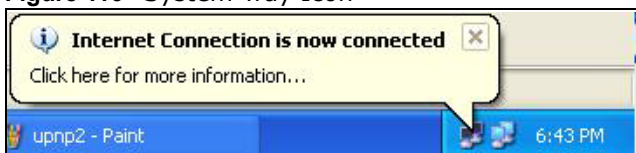
**Figure 115** Internet Connection Properties: Advanced Settings: Add



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

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

**Figure 116** System Tray Icon



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

**Figure 117** Internet Connection Status



## 14.4.2 Web Configurator Easy Access

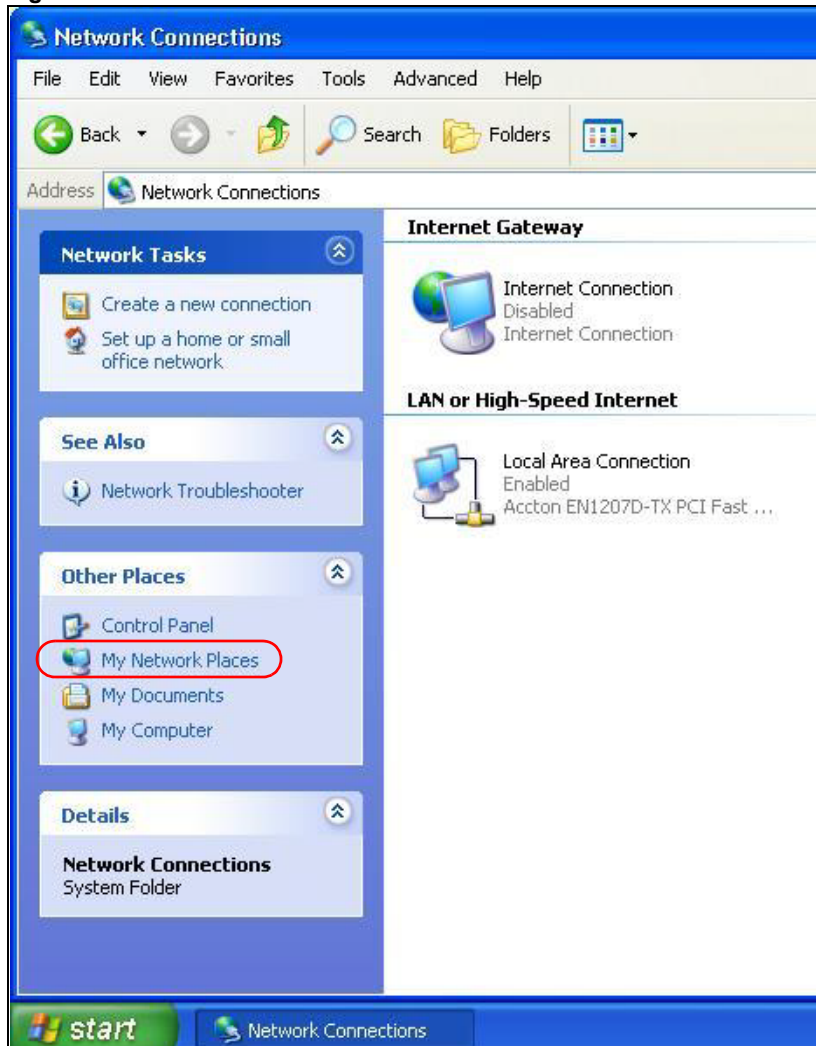
With UPnP, you can access the web-based configurator on the ZyXEL Device without finding out the IP address of the ZyXEL Device first. This comes helpful if you do not know the IP address of the ZyXEL Device.

Follow the steps below to access the web configurator.

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

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

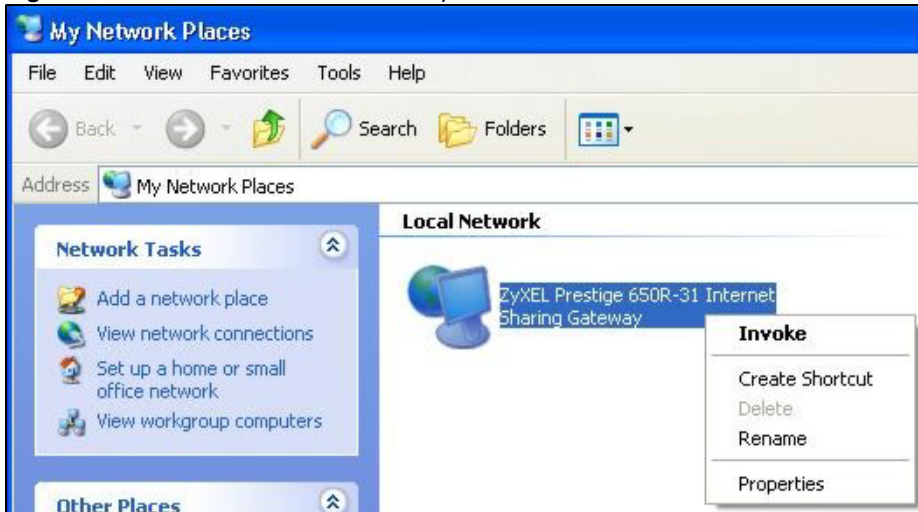
Figure 118 Network Connections



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

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

**Figure 119** Network Connections: My Network Places



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

**Figure 120** Network Connections: My Network Places: Properties: Example





Use this screen to configure the ZyXEL Device's time and date settings.

## 15.1 General Setup

### 15.1.1 General Setup and System Name

**General Setup** contains administrative and system-related information. **System Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

- In Windows 95/98 click **Start, Settings, Control Panel, Network**. Click the Identification tab, note the entry for the **Computer Name** field and enter it as the **System Name**.
- In Windows 2000, click **Start, Settings, Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.
- In Windows XP, click **start, My Computer, View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the ZyXEL Device **System Name**.

### 15.1.2 General Setup

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name), the domain name can be assigned from the ZyXEL Device via DHCP.

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

**Figure 121** System General Setup

The following table describes the labels in this screen.

**Table 69** System General Setup

LABEL	DESCRIPTION
General Setup	
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP.  The domain name entered by you is given priority over the ISP assigned domain name.
Administrator Inactivity Timer	Type how many minutes a management session can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Password	
User Password	If you log in with the user password, you can only view the ZyXEL Device status. The default user password is <b>user</b> .
New Password	Type your new user password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the ZyXEL Device.

**Table 69** System General Setup

LABEL	DESCRIPTION
Retype to Confirm	Type the new password again for confirmation.
Admin Password	If you log in with the admin password, you can configure the advanced features as well as the wizard setup on the ZyXEL Device.
Old Password	Type the default admin password ( <b>1234</b> ) or the existing password you use to access the system for configuring advanced features.
New Password	Type your new admin password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the ZyXEL Device.
Retype to Confirm	Type the new password again for confirmation.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 15.2 Time Setting

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

**Figure 122** System Time Setting

The screenshot displays the 'Time Setting' configuration page. At the top, there are tabs for 'General' and 'Time Setting'. Below the tabs, the 'Current Time' section shows the device's current time as 23:19:45 and the current date as 2000-01-01. The 'Time and Date Setup' section offers two options: 'Manual' (selected) and 'Get from Time Server'. Under 'Manual', there are input fields for 'New Time (hh:mm:ss)' showing 23:18:56 and 'New Date (yyyy/mm/dd)' showing 2000/1/1. Under 'Get from Time Server', there are fields for 'Time Protocol' (set to Daytime (RFC-867)) and 'Time Server Address' (set to 0.0.0.0). The 'Time Zone Setup' section shows the selected time zone as '(GMT) Greenwich Mean Time : Dublin Edinburgh, Lisbon, London'. There is an unchecked checkbox for 'Daylight Savings'. Below this, there are two rows for 'Start Date' and 'End Date', both set to 'First Sunday of January (2000-01-02) at 0 o'clock'. At the bottom of the form, there are 'Apply' and 'Cancel' buttons.

The following table describes the fields in this screen.

**Table 70** System Time Setting

LABEL	DESCRIPTION
Current Time and Date	
Current Time	<p>This field displays the time of your ZyXEL Device.</p> <p>Each time you reload this page, the ZyXEL Device synchronizes the time with the time server.</p>
Current Date	<p>This field displays the date of your ZyXEL Device.</p> <p>Each time you reload this page, the ZyXEL Device synchronizes the date with the time server.</p>
Time and Date Setup	
Manual	<p>Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.</p>
New Time (hh:mm:ss)	<p>This field displays the last updated time from the time server or the last time configured manually.</p> <p>When you set <b>Time and Date Setup</b> to <b>Manual</b>, enter the new time in this field and then click <b>Apply</b>.</p>
New Date (yyyy/mm/dd)	<p>This field displays the last updated date from the time server or the last date configured manually.</p> <p>When you set <b>Time and Date Setup</b> to <b>Manual</b>, enter the new date in this field and then click <b>Apply</b>.</p>
Get from Time Server	<p>Select this radio button to have the ZyXEL Device get the time and date from the time server you specified below.</p>
Time Protocol	<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><b>Daytime (RFC 867)</b> format is day/month/year/time zone of the server.</p> <p><b>Time (RFC 868)</b> format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.</p> <p>The default, <b>NTP (RFC 1305)</b>, is similar to Time (RFC 868).</p>
Time Server Address	<p>Enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.</p>
Time Zone Setup	
Time Zone	<p>Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).</p>
Daylight Savings	<p>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.</p> <p>Select this option if you use Daylight Saving Time.</p>

**Table 70** System Time Setting (continued)

LABEL	DESCRIPTION
Start Date	<p>Configure the day and time when Daylight Saving Time starts if you selected <b>Enable Daylight Saving</b>. The <b>o'clock</b> field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time starts in most parts of the United States on the first Sunday of April. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select <b>First, Sunday, April</b> and type 2 in the <b>o'clock</b> field.</p> <p>Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select <b>Last, Sunday, March</b>. The time you type in the <b>o'clock</b> field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>
End Date	<p>Configure the day and time when Daylight Saving Time ends if you selected <b>Enable Daylight Saving</b>. The <b>o'clock</b> field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select <b>Last, Sunday, October</b> and type 2 in the <b>o'clock</b> field.</p> <p>Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select <b>Last, Sunday, October</b>. The time you type in the <b>o'clock</b> field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.



## 16.1 Overview

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

The web configurator allows you to choose which categories of events and/or alerts to have the ZyXEL Device log and then display the logs or have the ZyXEL Device send them to an administrator (as e-mail) or to a syslog server.

### 16.1.1 What You Can Do in the Log Screens

- Use the View Log screen ([Section 16.2 on page 191](#)) to see the logs for the categories that you selected in the Log Settings screen.
- Use The Log Settings screen ([Section 16.3 on page 193](#)) to configure the mail server, the syslog server, when to send logs and what logs to send.

### 16.1.2 What You Need To Know About Logs

#### Alerts

An alert is a message that is enabled as soon as the event occurs. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as System Errors consist of both logs and alerts. You may differentiate them by their color in the View Log screen. Alerts display in red and logs display in black.

#### Logs

A log is a message about an event that occurred on your ZyXEL Device. For example, when someone logs in to the ZyXEL Device, you can set a schedule for how often logs should be enabled, or sent to a syslog server.

## 16.2 The View Log Screen

Use the View Log screen to see the logs for the categories that you selected in the Log Settings screen ([Section 16.3 on page 193](#)). Click Maintenance > Logs to open the View Log screen.

Entries in red indicate alerts. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

**Figure 123** Maintenance > Logs > View Log

#	Time	Message	Source	Destination	Notes
1	01/01/2000 00:33:40	WEB Login Successfully			User:admin
2	01/01/2000 00:31:32	none: UDP	192.168.1.1:53	192.168.1.34:1197	ACCESS PERMITTED
3	01/01/2000 00:31:32	none: UDP	192.168.1.1:53	192.168.1.34:1196	ACCESS PERMITTED
4	01/01/2000 00:31:32	none: UDP	192.168.1.1:53	192.168.1.34:1195	ACCESS PERMITTED
5	01/01/2000 00:30:23	WEB Login Successfully			User:user

The following table describes the fields in this screen.

**Table 71** Maintenance > Logs > View Log

LABEL	DESCRIPTION
Display	The categories that you select in the <b>Log Settings</b> screen display in the drop-down list box.  Select a category of logs to view; select <b>All Logs</b> to view logs from all of the log categories that you selected in the <b>Log Settings</b> page.
Email Log Now	Click this to send the log screen to the e-mail address specified in the <b>Log Settings</b> page (make sure that you have first filled in the <b>E-mail Log Settings</b> fields in <b>Log Settings</b> ).
Refresh	Click this to renew the log screen.
Clear Log	Click this to delete all the logs.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.
Destination	This field lists the destination IP address and the port number of the incoming packet.
Notes	This field displays additional information about the log entry.
Use WAN IP Address	Select this option to update the IP address of the host name(s) to the WAN IP address.



## 16.3 The Log Settings Screen

Use the Log Settings screen to configure the mail server, the syslog server, when to send logs and what logs to send.

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

Alerts are e-mailed as soon as they happen. Logs may be e-mailed as soon as the log is full. Selecting many alert and/or log categories (especially **Access Control**) may result in many e-mails being sent.

**Figure 124** Maintenance > Logs > Log Settings

The screenshot shows the 'Log Settings' configuration page. It features three main sections:

- E-mail Log Settings:** Includes input fields for Mail Server (with a tooltip: '(Outgoing SMTP Server Name or IP Address)'), Mail Subject, Send Log to (with a tooltip: '(E-Mail Address)'), and Send Alerts to (with a tooltip: '(E-Mail Address)'). It also has a dropdown for Log Schedule (set to 'When Log is Full'), a dropdown for Day for Sending Log (set to 'Monday'), and a time selection for Time for Sending Log (0 hour, 0 minute). A checkbox 'Clear log after sending mail' is present.
- Syslog Logging:** Contains a checkbox for 'Active', a Syslog IP Address field (set to '0.0.0.0' with a tooltip: '(Server Name or IP Address)'), and a Log Facility dropdown (set to 'Local 1').
- Active Log and Alert:** Divided into two columns. The 'Log' column has checkboxes for System Maintenance, System Errors, Access Control, UPnP, Attacks, Any IP, and PKI. The 'Send Immediate Alert' column has checkboxes for System Errors, Access Control, Attacks, and PKI.

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

The following table describes the fields in this screen.

**Table 72** Maintenance > Logs > Log Settings

LABEL	DESCRIPTION
E-mail Log Settings	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via E-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the ZyXEL Device sends. Not all ZyXEL Device models have this field.
Send Log to	The ZyXEL Device sends logs to the e-mail address specified in this field. If this field is left blank, the ZyXEL Device does not send logs via e-mail.
Send Alerts to	Alerts are real-time notifications that are sent as soon as an event, such as a DoS attack, system error, or forbidden web access attempt occurs. Enter the E-mail address where the alert messages will be sent. Alerts include system errors, attacks and attempted access to blocked web sites. If this field is left blank, alert messages will not be sent via E-mail.
Log Schedule	This drop-down menu is used to configure the frequency of log messages being sent as E-mail: <ul style="list-style-type: none"> <li>• Daily</li> <li>• Weekly</li> <li>• Hourly</li> <li>• When Log is Full</li> <li>• None.</li> </ul> <p>If you select <b>Weekly</b> or <b>Daily</b>, specify a time of day when the E-mail should be sent. If you select <b>Weekly</b>, then also specify which day of the week the E-mail should be sent. If you select <b>When Log is Full</b>, an alert is sent when the log fills up. If you select <b>None</b>, no log messages are sent.</p>
Day for Sending Log	Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Clear log after sending mail	Select the checkbox to delete all the logs after the ZyXEL Device sends an E-mail of the logs.
Syslog Logging	The ZyXEL Device sends a log to an external syslog server.
Active	Click <b>Active</b> to enable syslog logging.
Syslog IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the syslog server manual for more information.
Active Log and Alert	
Log	Select the categories of logs that you want to record.
Send Immediate Alert	Select log categories for which you want the ZyXEL Device to send E-mail alerts immediately.
Apply	Click this to save your customized settings and exit this screen.
Cancel	Click this to restore your previously saved settings.

## 16.4 SMTP Error Messages

If there are difficulties in sending e-mail the following error message appears.

"SMTP action request failed. ret= ??". The "??" are described in the following table.

**Table 73** SMTP Error Messages

-1 means ZyXEL Device out of socket
-2 means tcp SYN fail
-3 means smtp server OK fail
-4 means HELO fail
-5 means MAIL FROM fail
-6 means RCPT TO fail
-7 means DATA fail
-8 means mail data send fail

### 16.4.1 Example E-mail Log

An "End of Log" message displays for each mail in which a complete log has been sent. The following is an example of a log sent by e-mail.

You may edit the subject title.

"End of Log" message shows that a complete log has been sent.

**Figure 125** E-mail Log Example

```

Subject:
      Firewall Alert From
Date:
      Fri, 07 Apr 2000 10:05:42
From:
      user@zyxel.com
To:
      user@zyxel.com
1|Apr  7 00 |From:192.168.1.1      To:192.168.1.255  |default policy
|forward
  | 09:54:03 |UDP      src port:00520 dest port:00520  |<1,00>
|
2|Apr  7 00 |From:192.168.1.131   To:192.168.1.255  |default policy
|forward
  | 09:54:17 |UDP      src port:00520 dest port:00520  |<1,00>
|
3|Apr  7 00 |From:192.168.1.6     To:10.10.10.10   |match
|forward
  | 09:54:19 |UDP      src port:03516 dest port:00053  |<1,01>
|
.....{snip}.....
.....{snip}.....
126|Apr  7 00 |From:192.168.1.1     To:192.168.1.255  |match
|forward
  | 10:05:00 |UDP      src port:00520 dest port:00520  |<1,02>
|
127|Apr  7 00 |From:192.168.1.131   To:192.168.1.255  |match
|forward
  | 10:05:17 |UDP      src port:00520 dest port:00520  |<1,02>
|
128|Apr  7 00 |From:192.168.1.1     To:192.168.1.255  |match
|forward
  | 10:05:30 |UDP      src port:00520 dest port:00520  |<1,02>
|
End of Firewall Log

```

## 16.5 Log Descriptions

This section provides descriptions of example log messages.

**Table 74** System Maintenance Logs

LOG MESSAGE	DESCRIPTION
Time calibration is successful	The router has adjusted its time based on information from the time server.
Time calibration failed	The router failed to get information from the time server.
WAN interface gets IP: %s	A WAN interface got a new IP address from the DHCP, PPPoE, or dial-up server.
DHCP client IP expired	A DHCP client's IP address has expired.
DHCP server assigns %s	The DHCP server assigned an IP address to a client.
Successful WEB login	Someone has logged on to the router's web configurator interface.
WEB login failed	Someone has failed to log on to the router's web configurator interface.
Successful TELNET login	Someone has logged on to the router via telnet.
TELNET login failed	Someone has failed to log on to the router via telnet.
Successful FTP login	Someone has logged on to the router via ftp.
FTP login failed	Someone has failed to log on to the router via ftp.
NAT Session Table is Full!	The maximum number of NAT session table entries has been exceeded and the table is full.
Starting Connectivity Monitor	Starting Connectivity Monitor.
Time initialized by Daytime Server	The router got the time and date from the Daytime server.
Time initialized by Time server	The router got the time and date from the time server.
Time initialized by NTP server	The router got the time and date from the NTP server.
Connect to Daytime server fail	The router was not able to connect to the Daytime server.
Connect to Time server fail	The router was not able to connect to the Time server.
Connect to NTP server fail	The router was not able to connect to the NTP server.
Too large ICMP packet has been dropped	The router dropped an ICMP packet that was too large.
Configuration Change: PC = 0x%x, Task ID = 0x%x	The router is saving configuration changes.
Successful SSH login	Someone has logged on to the router's SSH server.
SSH login failed	Someone has failed to log on to the router's SSH server.
Successful HTTPS login	Someone has logged on to the router's web configurator interface using HTTPS protocol.
HTTPS login failed	Someone has failed to log on to the router's web configurator interface using HTTPS protocol.

**Table 75** System Error Logs

LOG MESSAGE	DESCRIPTION
%s exceeds the max. number of session per host!	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.
setNetBIOSFilter: calloc error	The router failed to allocate memory for the NetBIOS filter settings.
readNetBIOSFilter: calloc error	The router failed to allocate memory for the NetBIOS filter settings.
WAN connection is down.	A WAN connection is down. You cannot access the network through this interface.

**Table 76** Access Control Logs

LOG MESSAGE	DESCRIPTION
Firewall default policy: [ TCP   UDP   IGMP   ESP   GRE   OSPF ] <Packet Direction>	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched the default policy and was blocked or forwarded according to the default policy's setting.
Firewall rule [NOT] match:[ TCP   UDP   IGMP   ESP   GRE   OSPF ] <Packet Direction>, <rule:%d>	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched (or did not match) a configured firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
Triangle route packet forwarded: [ TCP   UDP   IGMP   ESP   GRE   OSPF ]	The firewall allowed a triangle route session to pass through.
Packet without a NAT table entry blocked: [ TCP   UDP   IGMP   ESP   GRE   OSPF ]	The router blocked a packet that didn't have a corresponding NAT table entry.
Router sent blocked web site message: TCP	The router sent a message to notify a user that the router blocked access to a web site that the user requested.

**Table 77** TCP Reset Logs

LOG MESSAGE	DESCRIPTION
Under SYN flood attack, sent TCP RST	The router sent a TCP reset packet when a host was under a SYN flood attack (the TCP incomplete count is per destination host.)
Exceed TCP MAX incomplete, sent TCP RST	The router sent a TCP reset packet when the number of TCP incomplete connections exceeded the user configured threshold. (the TCP incomplete count is per destination host.) Note: Refer to <b>TCP Maximum Incomplete</b> in the <b>Firewall Attack Alerts</b> screen.
Peer TCP state out of order, sent TCP RST	The router sent a TCP reset packet when a TCP connection state was out of order. Note: The firewall refers to RFC793 Figure 6 to check the TCP state.
Firewall session time out, sent TCP RST	The router sent a TCP reset packet when a dynamic firewall session timed out. Default timeout values: ICMP idle timeout (s): 60 UDP idle timeout (s): 60 TCP connection (three way handshaking) timeout (s): 30 TCP FIN-wait timeout (s): 60 TCP idle (established) timeout (s): 3600

LOG MESSAGE	DESCRIPTION
Exceed MAX incomplete, sent TCP RST	The router sent a TCP reset packet when the number of incomplete connections (TCP and UDP) exceeded the user-configured threshold. (Incomplete count is for all TCP and UDP connections through the firewall.)Note: When the number of incomplete connections (TCP + UDP) > "Maximum Incomplete High", the router sends TCP RST packets for TCP connections and destroys TOS (firewall dynamic sessions) until incomplete connections < "Maximum Incomplete Low".
Access block, sent TCP RST	The router sends a TCP RST packet and generates this log if you turn on the firewall TCP reset mechanism (via CLI command: "sys firewall tcprst").

**Table 78** Packet Filter Logs

LOG MESSAGE	DESCRIPTION
[ TCP   UDP   ICMP   IGMP   Generic ] packet filter matched (set: %d, rule: %d)	Attempted access matched a configured filter rule (denoted by its set and rule number) and was blocked or forwarded according to the rule.

**Table 79** ICMP Logs

LOG MESSAGE	DESCRIPTION
Firewall default policy: ICMP <Packet Direction>, <type:%d>, <code:%d>	ICMP access matched the default policy and was blocked or forwarded according to the user's setting.
Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>	ICMP access matched (or didn't match) a firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
Triangle route packet forwarded: ICMP	The firewall allowed a triangle route session to pass through.
Packet without a NAT table entry blocked: ICMP	The router blocked a packet that didn't have a corresponding NAT table entry.
Unsupported/out-of-order ICMP: ICMP	The firewall does not support this kind of ICMP packets or the ICMP packets are out of order.
Router reply ICMP packet: ICMP	The router sent an ICMP reply packet to the sender.

**Table 80** CDR Logs

LOG MESSAGE	DESCRIPTION
Firewall default policy: ICMP <Packet Direction>, <type:%d>, <code:%d>	ICMP access matched the default policy and was blocked or forwarded according to the user's setting.
Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>	ICMP access matched (or didn't match) a firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
Triangle route packet forwarded: ICMP	The firewall allowed a triangle route session to pass through.
Packet without a NAT table entry blocked: ICMP	The router blocked a packet that didn't have a corresponding NAT table entry.

LOG MESSAGE	DESCRIPTION
Unsupported/out-of-order ICMP: ICMP	The firewall does not support this kind of ICMP packets or the ICMP packets are out of order.
Router reply ICMP packet: ICMP	The router sent an ICMP reply packet to the sender.

**Table 81** PPP Logs

LOG MESSAGE	DESCRIPTION
ppp:LCP Starting	The PPP connection's Link Control Protocol stage has started.
ppp:LCP Opening	The PPP connection's Link Control Protocol stage is opening.
ppp:CHAP Opening	The PPP connection's Challenge Handshake Authentication Protocol stage is opening.
ppp:IPCP Starting	The PPP connection's Internet Protocol Control Protocol stage is starting.
ppp:IPCP Opening	The PPP connection's Internet Protocol Control Protocol stage is opening.
ppp:LCP Closing	The PPP connection's Link Control Protocol stage is closing.
ppp:IPCP Closing	The PPP connection's Internet Protocol Control Protocol stage is closing.

**Table 82** UPnP Logs

LOG MESSAGE	DESCRIPTION
UPnP pass through Firewall	UPnP packets can pass through the firewall.

**Table 83** Content Filtering Logs

LOG MESSAGE	DESCRIPTION
%s: block keyword	The content of a requested web page matched a user defined keyword.
%s	The system forwarded web content.

**Table 84** Attack Logs

LOG MESSAGE	DESCRIPTION
attack [ TCP   UDP   IGMP   ESP   GRE   OSPF ]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF attack.
attack ICMP (type:%d, code:%d)	The firewall detected an ICMP attack.
land [ TCP   UDP   IGMP   ESP   GRE   OSPF ]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF land attack.
land ICMP (type:%d, code:%d)	The firewall detected an ICMP land attack.
ip spoofing - WAN [ TCP   UDP   IGMP   ESP   GRE   OSPF ]	The firewall detected an IP spoofing attack on the WAN port.
ip spoofing - WAN ICMP (type:%d, code:%d)	The firewall detected an ICMP IP spoofing attack on the WAN port.
icmp echo : ICMP (type:%d, code:%d)	The firewall detected an ICMP echo attack.
syn flood TCP	The firewall detected a TCP syn flood attack.



LOG MESSAGE	DESCRIPTION
ports scan TCP	The firewall detected a TCP port scan attack.
teardrop TCP	The firewall detected a TCP teardrop attack.
teardrop UDP	The firewall detected an UDP teardrop attack.
teardrop ICMP (type:%d, code:%d)	The firewall detected an ICMP teardrop attack.
illegal command TCP	The firewall detected a TCP illegal command attack.
NetBIOS TCP	The firewall detected a TCP NetBIOS attack.
ip spoofing - no routing entry [ TCP   UDP   ICMP   ESP   GRE   OSPF ]	The firewall classified a packet with no source routing entry as an IP spoofing attack.
ip spoofing - no routing entry ICMP (type:%d, code:%d)	The firewall classified an ICMP packet with no source routing entry as an IP spoofing attack.
vulnerability ICMP (type:%d, code:%d)	The firewall detected an ICMP vulnerability attack.
traceroute ICMP (type:%d, code:%d)	The firewall detected an ICMP traceroute attack.

**Table 85** 802.1X Logs

LOG MESSAGE	DESCRIPTION
RADIUS accepts user.	A user was authenticated by the RADIUS Server.
RADIUS rejects user. Pls check RADIUS Server.	A user was not authenticated by the RADIUS Server. Please check the RADIUS Server.
User logout because of session timeout expired.	The router logged out a user whose session expired.
User logout because of user deassociation.	The router logged out a user who ended the session.
User logout because of no authentication response from user.	The router logged out a user from which there was no authentication response.
User logout because of idle timeout expired.	The router logged out a user whose idle timeout period expired.
User logout because of user request.	A user logged out.
No response from RADIUS. Pls check RADIUS Server.	There is no response message from the RADIUS server, please check the RADIUS server.
Use RADIUS to authenticate user.	The RADIUS server is operating as the authentication server.
No Server to authenticate user.	There is no authentication server to authenticate a user.

**Table 86** ACL Setting N

PACKET DIRECTION	DIRECTION	DESCRIPTION
(L to W)	LAN to WAN	ACL set for packets traveling from the LAN to the WAN.
(W to L)	WAN to LAN	ACL set for packets traveling from the WAN to the LAN.

PACKET DIRECTION	DIRECTION	DESCRIPTION
(L to ZyXEL Device)	LAN to ZyXEL Device	ACL set for packets traveling from the LAN to the ZyXEL Device.
(W to ZyXEL Device)	WAN to ZyXEL Device	ACL set for packets traveling from the WAN to the ZyXEL Device.

**Table 87** ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message

TYPE	CODE	DESCRIPTION
16		Information Reply
	0	Information reply message

**Table 88** System Logs

LOG MESSAGE	DESCRIPTION
<pre>&lt;Facility*8 + Severity&gt;Mon dd hr:mm:ss hostname src="&lt;srcIP:srcPort&gt;" dst="&lt;dstIP:dstPort&gt;" msg="&lt;msg&gt;" note="&lt;note&gt;" devID="&lt;mac address last three numbers&gt;" cat="&lt;category&gt;</pre>	<p>"This message is sent by the system ("RAS" displays as the system name if you haven't configured one) when the router generates a syslog. The facility is defined in the web MAIN MENU-&gt;LOGS-&gt;Log Settings page. The severity is the log's syslog class. The definition of messages and notes are defined in the various log charts throughout this appendix. The "devID" is the last three characters of the MAC address of the router's LAN port. The "cat" is the same as the category in the router's logs.</p>

The following table shows RFC-2408 ISAKMP payload types that the log displays. Please refer to RFC 2408 for detailed information on each type.

**Table 89** RFC-2408 ISAKMP Payload Types

LOG DISPLAY	PAYLOAD TYPE
SA	Security Association
PROP	Proposal
TRANS	Transform
KE	Key Exchange
ID	Identification
CER	Certificate
CER_REQ	Certificate Request
HASH	Hash
SIG	Signature
NONCE	Nonce
NOTFY	Notification
DEL	Delete
VID	Vendor ID



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

## 17.1 Firmware Upgrade

Find firmware at [www.zyxel.com](http://www.zyxel.com) in a file that (usually) uses the system model name with a .bin extension, for example, "ZyXEL Device.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 **Maintenance > Tools** to open the **Firmware** screen. Follow the instructions in this screen to upload firmware to your ZyXEL Device.

**Figure 126** Firmware Upgrade

The following table describes the labels in this screen.

**Table 90** Firmware Upgrade

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

Note: 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.

**Figure 127** Firmware Upload In Progress



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

**Figure 128** Network Temporarily Disconnected



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

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

**Figure 129** Error Message



## 17.2 Configuration Screen

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

**Figure 130** Configuration

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

- Backup Configuration:** A text prompt 'Click **Backup** to save the current configuration to you computer.' followed by a 'Backup' button.
- Restore Configuration:** A text prompt 'To restore a previously saved configuration file on your computer to the Prestige, please type a location for storing the configuration file or click **Browse** to look for one, and then click **Upload**.' Below this is a 'File Path:' label, an input field, a 'Choose...' button, and an 'Upload' button.
- Reset to Factory Default Settings:** A text prompt 'Click **Reset** to clear all user-entered configuration and return the Prestige to the factory default settings.' Below this is a list of default settings: 'Password :1234', 'Lan IP : 192.168.1.1', and 'DHCP : Server .'. At the bottom is a 'Reset' button.

### 17.2.1 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

### 17.2.2 Restore Configuration

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

**Table 91** Maintenance Restore Configuration

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

Note: 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 131** Configuration Restore 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 132** 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.

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

**Figure 133** Configuration Restore Error



## 17.2.3 Back 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.



You can also press the **RESET** button on the rear panel to reset the factory defaults of your ZyXEL Device. Refer to the chapter about introducing the web configurator for more information on the **RESET** button.

## 17.3 Restart

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

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

**Figure 134** Restart Screen



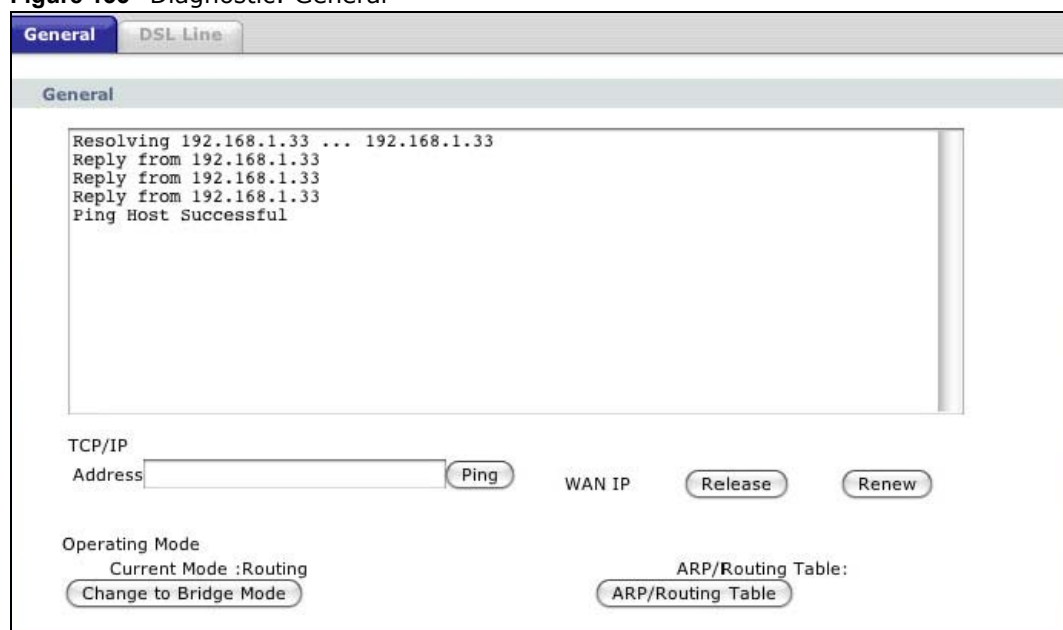
## Diagnostic

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

### 18.1 General Diagnostic

Click **Maintenance > Diagnostic** to open the screen shown next.

**Figure 135** Diagnostic: General



The following table describes the fields in this screen.

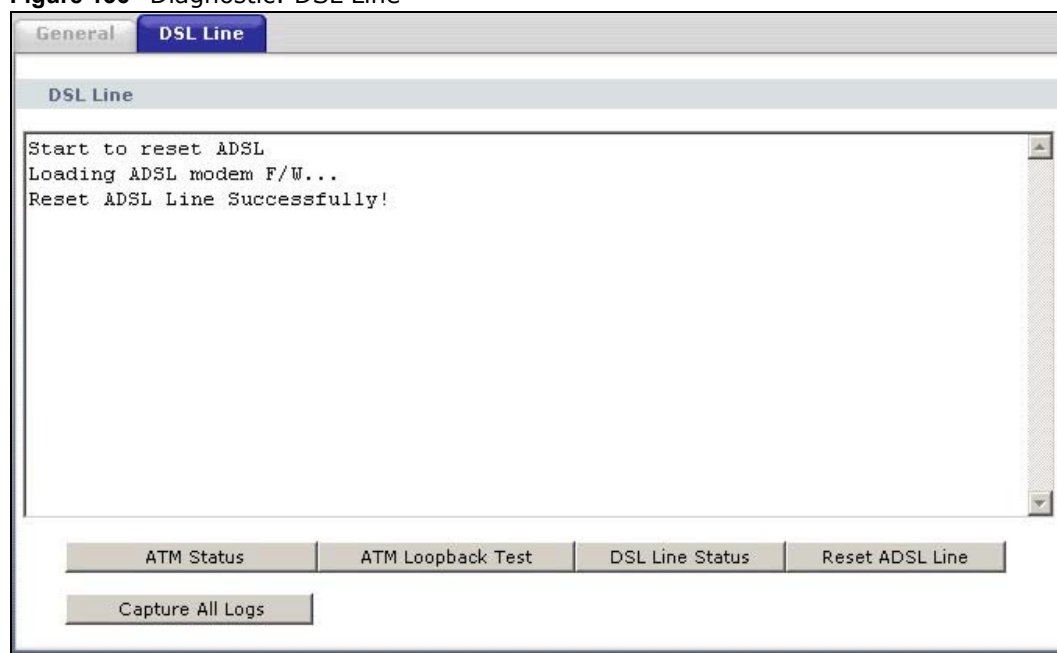
**Table 92** Diagnostic: General

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.
Change to Bridge/Routing Mode	Click this button to toggle between Routing and Bridge mode.
ARP/Routing Table	Click this button to view ARP table and Routing table information in the General display area.

## 18.2 DSL Line Diagnostic

Click **Maintenance > Diagnostic > DSL Line** to open the screen shown next.

**Figure 136** Diagnostic: DSL Line



The following table describes the fields in this screen.

**Table 93** Diagnostic: DSL Line

LABEL	DESCRIPTION
ATM Status	Click this button to view ATM status.
ATM Loopback Test	Click this button to start the ATM loopback test. Make sure you have configured at least one PVC with proper VPIs/VCIs before you begin this test. The ZyXEL Device sends an OAM F5 packet to the DSLAM/ATM switch and then returns it (loops it back) to the ZyXEL Device. The ATM loopback test is useful for troubleshooting problems with the DSLAM and ATM network.
DSL Line Status	Click this button to view the DSL port's line operating values and line bit allocation.
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!"
Capture All Logs	Click this button to display all logs generated with the DSL line.



# Troubleshooting

This chapter covers potential problems and the corresponding remedies.

## 19.1 Problems Starting Up the ZyXEL Device

**Table 94** Troubleshooting Starting Up Your ZyXEL Device

PROBLEM	CORRECTIVE ACTION
None of the lights turn on when I turn on the ZyXEL Device.	<p>Make sure that the ZyXEL Device's power adaptor is connected to the ZyXEL Device and plugged in to an appropriate power source. Make sure that the ZyXEL Device and the power source are both turned on.</p> <p>Turn the ZyXEL Device off and on.</p> <p>If the error persists, you may have a hardware problem. In this case, you should contact your vendor.</p>

## 19.2 Problems with the LAN

**Table 95** Troubleshooting the LAN

PROBLEM	CORRECTIVE ACTION
The LAN lights do not turn on.	<p>Check your Ethernet cable connections (refer to the Quick Start Guide for details).</p> <p>Check for faulty Ethernet cables.</p> <p>Make sure your computer's Ethernet Card is working properly.</p>
I cannot access the ZyXEL Device from the LAN.	If <b>Any IP</b> is disabled, make sure that the IP address and the subnet mask of the ZyXEL Device and your computer(s) are on the same subnet.

## 19.3 Problems with the WAN

**Table 96** Troubleshooting the WAN

PROBLEM	CORRECTIVE ACTION
The DSL light is off.	Check the telephone wire and connections between the ZyXEL Device DSL port and the wall jack.
	Make sure that the telephone company has checked your phone line and set it up for DSL service.
	Reset your ADSL line to reinitialize your link to the DSLAM. For details, refer to <a href="#">Table 93 on page 211</a> .
I cannot get a WAN IP address from the ISP.	<p>The ISP provides the WAN IP address after authenticating you. Authentication may be through the user name and password, the MAC address or the host name.</p> <p>The username and password apply to PPPoE and PPPoA encapsulation only. Make sure that you have entered the correct <b>Service Type</b>, <b>User Name</b> and <b>Password</b> (be sure to use the correct casing). Refer to the WAN Setup chapter.</p>
I cannot access the Internet.	<p>Make sure the ZyXEL Device is turned on and connected to the network.</p> <p>Verify your WAN settings. Refer to the chapter on WAN setup.</p> <p>Make sure you entered the correct user name and password.</p> <p>If you use PPPoE pass through, make sure that bridge mode is turned on.</p>
The Internet connection disconnects.	<p>Check the schedule rules.</p> <p>If you use PPPoA or PPPoE encapsulation, check the idle time-out setting. Refer to <a href="#">Chapter 4 on page 43</a>.</p> <p>Contact your ISP.</p>

## 19.4 Problems Accessing the ZyXEL Device

**Table 97** Troubleshooting Accessing the ZyXEL Device

PROBLEM	CORRECTIVE ACTION
I cannot access the ZyXEL Device.	<p>The default user password is "user" and admin password is "1234". The <b>Password</b> field is case-sensitive. Make sure that you enter the correct password using the proper case.</p> <p>If you have changed the password and have now forgotten it, you will need to upload the default configuration file. This restores all of the factory defaults including the password.</p>
I cannot access the web configurator.	<p>Make sure that there is not a Telnet session running.</p> <p>Use the ZyXEL Device's WAN IP address when configuring from the WAN. Refer to the instructions on checking your WAN connection.</p> <p>Use the ZyXEL Device's LAN IP address when configuring from the LAN. Refer to for instructions on checking your LAN connection.</p> <p>Check that you have enabled web service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on remote management for details.</p> <p>Your computer's and the ZyXEL Device's IP addresses must be on the same subnet for LAN access.</p> <p>If you changed the ZyXEL Device's LAN IP address, then enter the new one as the URL.</p> <p>Make sure that pop-up windows, JavaScripts and Java permissions are allowed. See the appendix for how to enable them.</p>





# Product Specifications

See also the Introduction chapter for a general overview of the key features.

## Specification Tables

**Table 98** Device

Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	administrator: 1234 user: user
DHCP Pool	192.168.1.33 to 192.168.1.64
Dimensions (W x D x H)	105 x 105 x 31 mm
Power Specification	9VAC 1A
Ethernet port	auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet port
Operation Temperature	0° C ~ 40° C
Storage Temperature	-30° ~ 60° C
Operation Humidity	20% ~ 85% RH
Storage Humidity	20% ~ 90% RH
Distance between the centers of the holes on the device's back.	75 mm
Screw size for wall-mounting	M3*10

**Table 99** Firmware

ADSL Standards	<p>Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt(G.992.1); G.lite(G.992.2)).</p> <p>ADSL2 G.dmt.bis (G.992.3)</p> <p>ADSL2+ (G.992.5)</p> <p>Reach-Extended ADSL (RE ADSL)</p> <p>SRA (Seamless Rate Adaptation)</p> <p>Auto-negotiating rate adaptation</p> <p>ADSL physical connection ATM AAL5 (ATM Adaptation Layer type 5)</p> <p>Multi-protocol over AAL5 (RFC2684/1483)</p> <p>PPP over ATM AAL5 (RFC 2364)</p> <p>PPP over Ethernet (RFC 2516)</p> <p>RFC 1483 encapsulation over ATM</p> <p>MAC encapsulated routing (ENET encapsulation)</p> <p>VC-based and LLC-based multiplexing</p> <p>Up to 8 PVCs (Permanent Virtual Circuits)</p> <p>I.610 F4/F5 OAM</p>
Other Protocol Support	<p>PPP (Point-to-Point Protocol) link layer protocol.</p> <p>Transparent bridging for unsupported network layer protocols.</p> <p>DHCP Server/Client/Relay</p> <p>RIP I/RIP II</p> <p>ICMP</p> <p>SNMP v1 and v2c with MIB II support (RFC 1213)</p> <p>IP Multicasting IGMP v1 and v2</p> <p>IGMP Proxy</p> <p>UPnP</p>
Management	<p>Embedded Web Configurator</p> <p>CLI (Command Line Interpreter)</p> <p>Remote Management via Telnet or Web</p> <p>SNMP manageable</p> <p>FTP/TFTP for firmware downloading, configuration backup and restoration.</p> <p>Built-in Diagnostic Tools for FLASH memory, ADSL circuitry, RAM and LAN port</p> <p>MAP - "Multimedia Auto Provisioner" (multimedia installation tutorial and automatic configurator)</p>
NAT/SUA	<p>Port Forwarding</p> <p>1024 NAT sessions</p> <p>Multimedia application</p> <p>PPTP under NAT/SUA</p>

---

**Table 99** Firmware (continued)

Static Routes	16 IP and 4 Bridge
Other Features	Any IP Zero Configuration (VC auto-hunting) Traffic Redirect Dynamic DNS IP Alias



## Wall-mounting Instructions

Do the following to hang your ZyXEL Device on a wall.

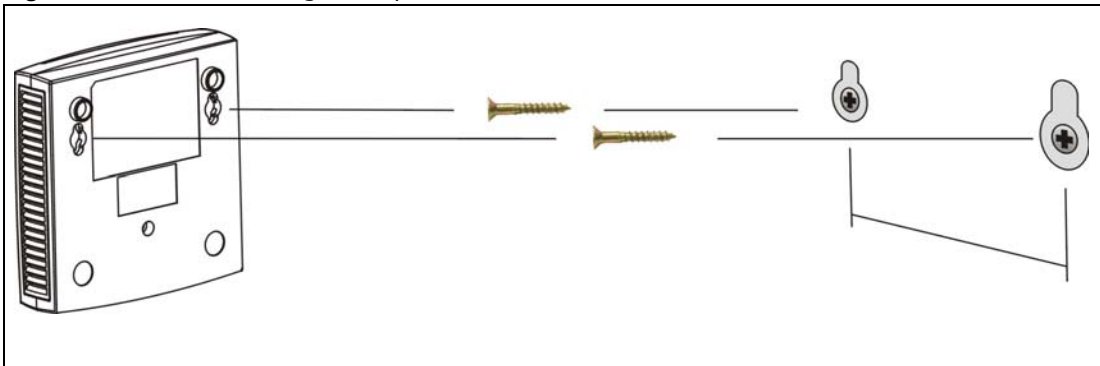
Note: See the product specifications appendix for the size of screws to use and how far apart to place them.

- 1 Locate a high position on wall that is free of obstructions. Use a sturdy wall.
- 2 Drill two holes for the screws. Make sure the distance between the centers of the holes matches what is listed in the product specifications appendix.

Note: Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

- 3 Do not screw the screws all the way into the wall. Leave a small gap of about 0.5 cm between the heads of the screws and the wall.
- 4 Make sure the screws are snugly fastened to the wall. They need to hold the weight of the ZyXEL Device with the connection cables.
- 5 Align the holes on the back of the ZyXEL Device with the screws on the wall. Hang the ZyXEL Device on the screws.

**Figure 137** Wall-mounting Example





# 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.

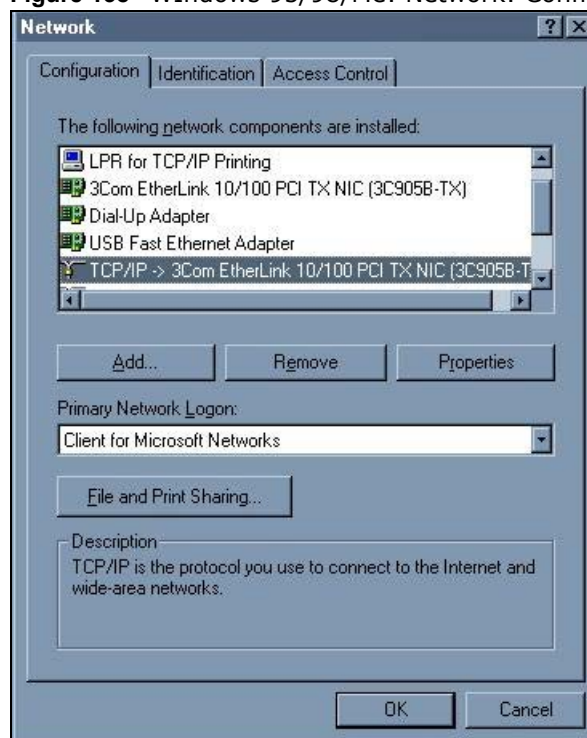
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

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 138** 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.

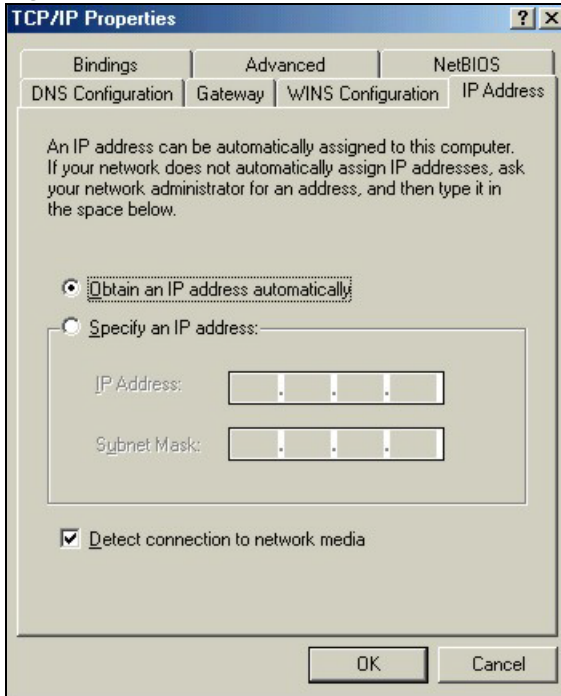
## Configuring

- 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.

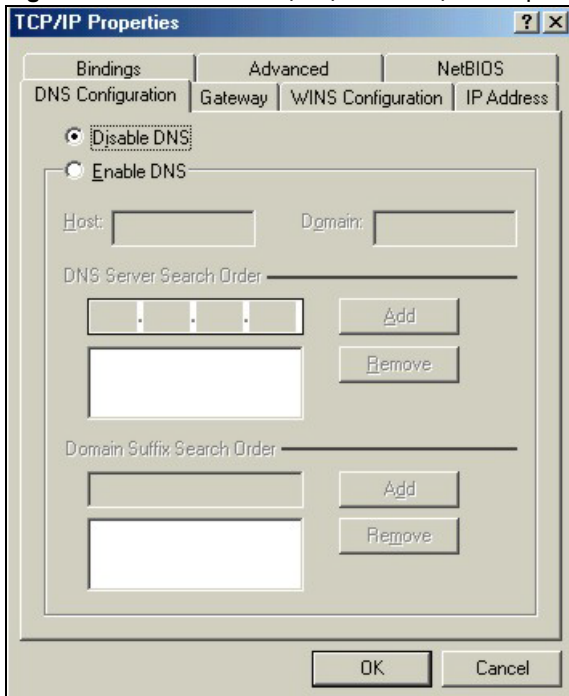
**Figure 139** Windows 95/98/Me: TCP/IP Properties: IP Address



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 140** 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

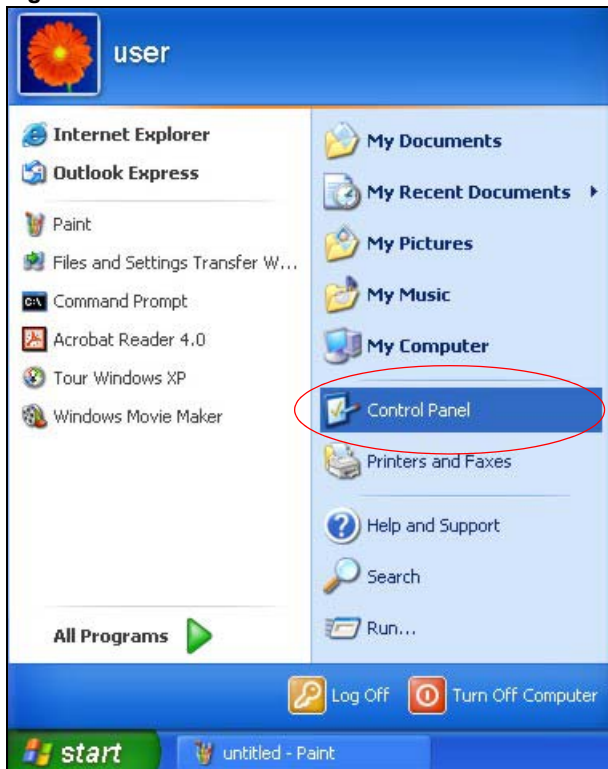
- 1 Click **Start** and then **Run**.
- 2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
- 3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

## 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 141 Windows XP: Start Menu



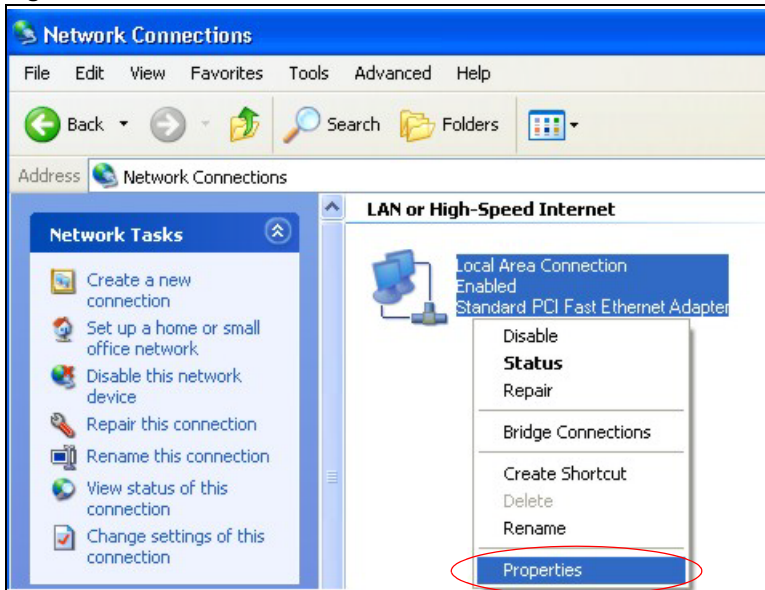
- 2 In the **Control Panel**, double-click **Network Connections (Network and Dial-up Connections)** in Windows 2000/NT).

**Figure 142** Windows XP: Control Panel



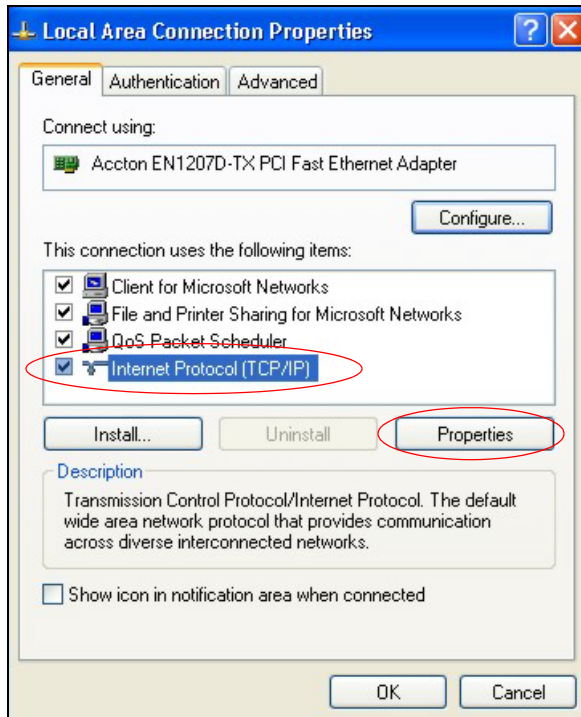
- 3 Right-click **Local Area Connection** and then click **Properties**.

**Figure 143** 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 144** Windows XP: Local Area Connection Properties

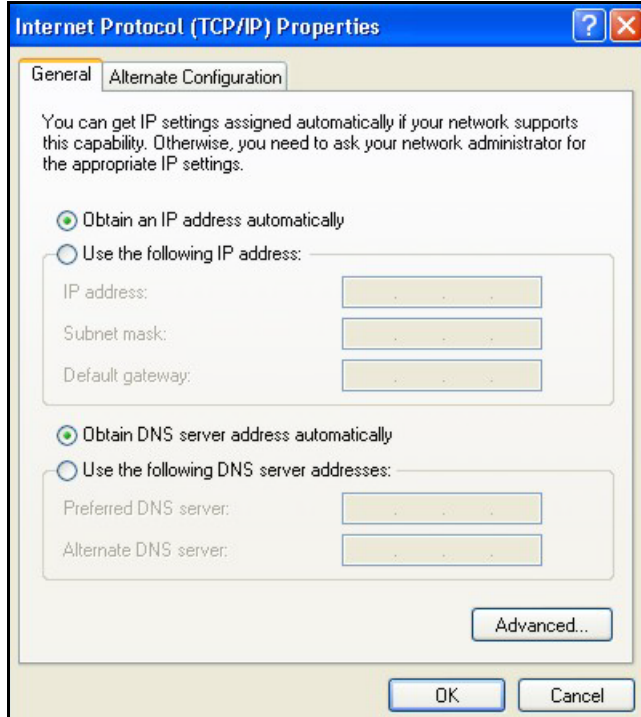


- 5 The **Internet Protocol TCP/IP Properties** window opens (the **General** tab in Windows XP).

- 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 145** Windows XP: Internet Protocol (TCP/IP) Properties



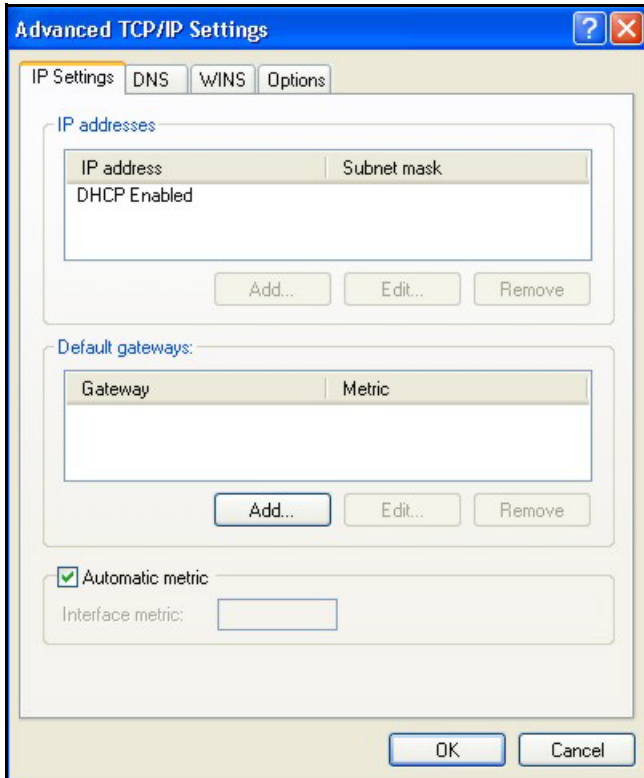
- 6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

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 146** Windows XP: Advanced TCP/IP Properties

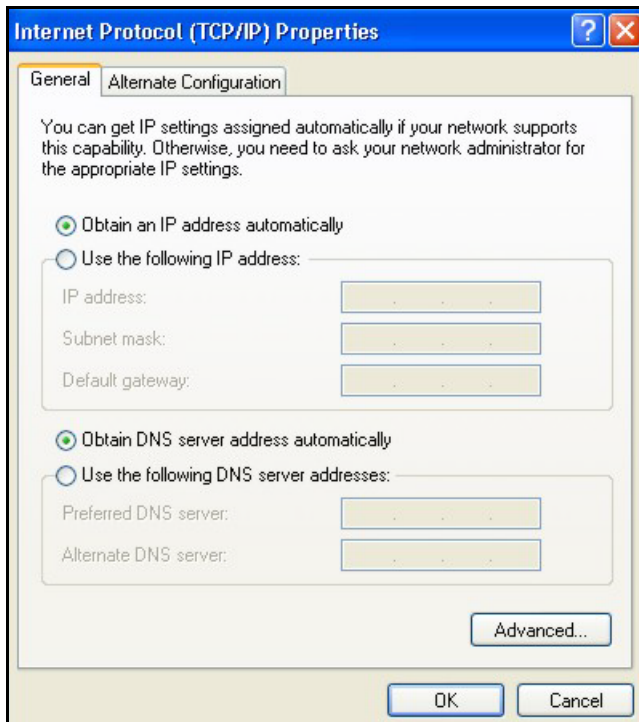


7 In the **Internet Protocol TCP/IP Properties** window (the **General tab** in Windows XP):

- 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 147** 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).

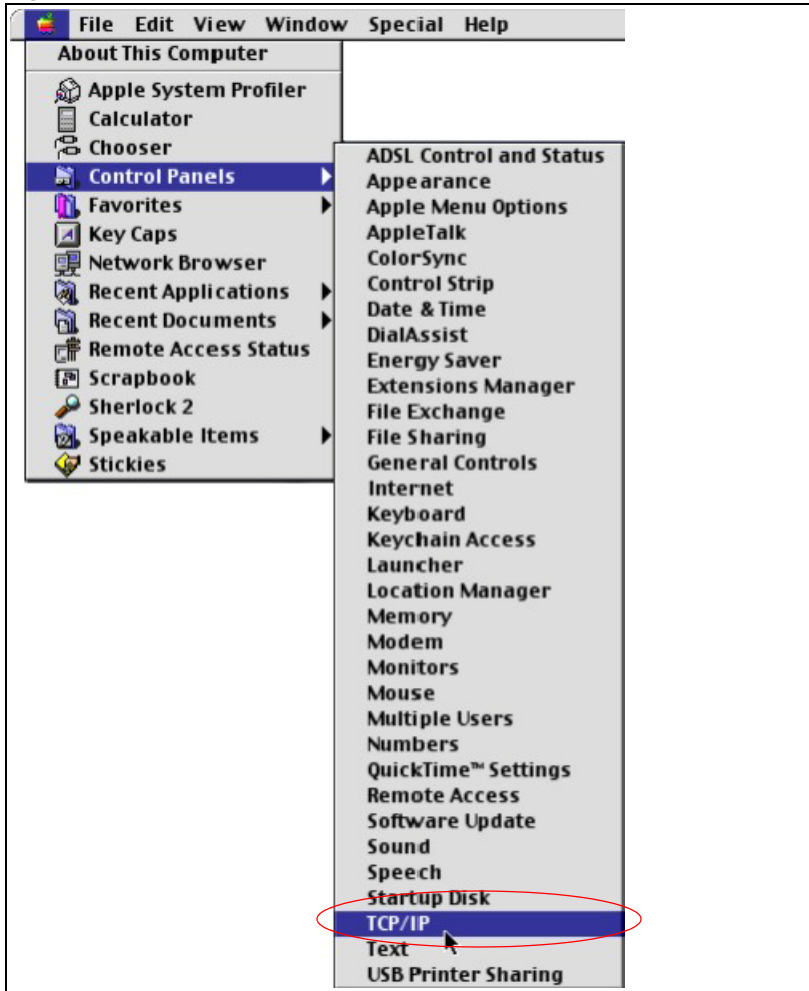
## Verifying Settings

- 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**.

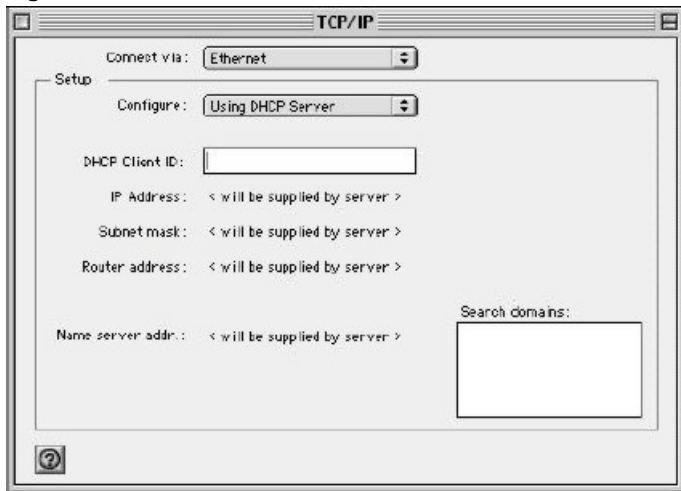
Figure 148 Macintosh OS 8/9: Apple Menu





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

**Figure 149** 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).

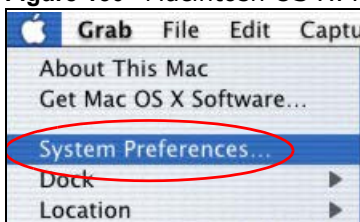
## Verifying Settings

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.

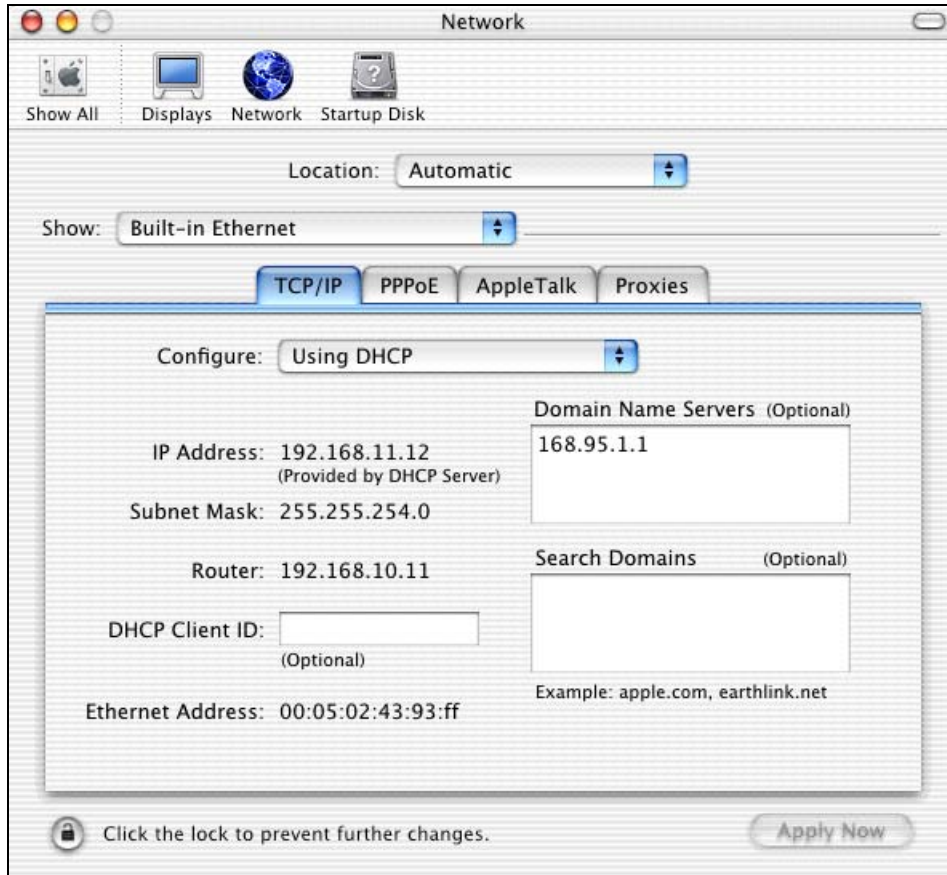
**Figure 150** Macintosh OS X: Apple Menu



- 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 151** 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.

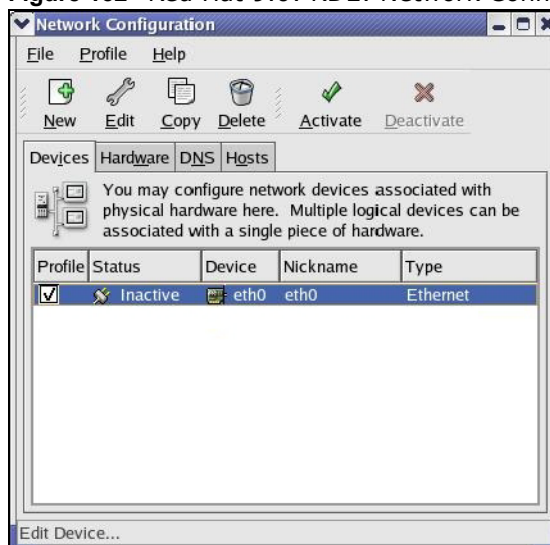
Note: Make sure you are logged in as the root administrator.

### 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 152** 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.

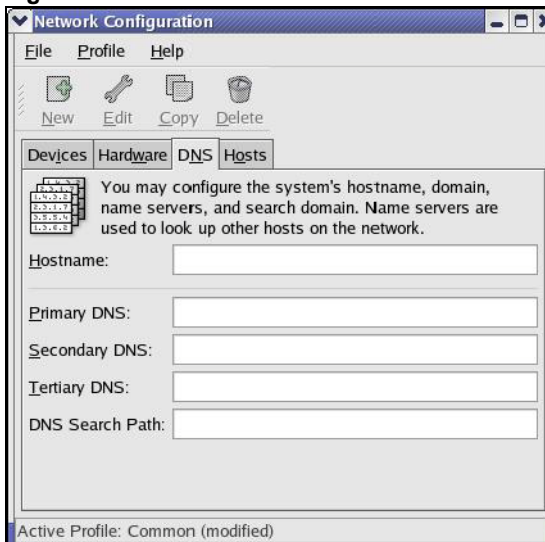
**Figure 153** Red Hat 9.0: KDE: Ethernet Device: General



- 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 154** 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 155** 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 156** 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 157** 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 158** 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 159** 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 160** 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, IP address classes and subnet masks. You use subnet masks to subdivide a network into smaller logical networks.

## Introduction to IP Addresses

An IP address has two parts: the network number and the host ID. Routers use the network number to send packets to the correct network, while the host ID identifies a single device on the network.

An IP address is made up of four octets, written in dotted decimal notation, for example, 192.168.1.1. (An octet is an 8-digit binary number. Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.)

There are several classes of IP addresses. The first network number (192 in the above example) defines the class of IP address. These are defined as follows:

- Class A: 0 to 127
- Class B: 128 to 191
- Class C: 192 to 223
- Class D: 224 to 239
- Class E: 240 to 255

## IP Address Classes and Hosts

The class of an IP address determines the number of hosts you can have on your network.

- In a class A address the first octet is the network number, and the remaining three octets are the host ID.
- In a class B address the first two octets make up the network number, and the two remaining octets make up the host ID.
- In a class C address the first three octets make up the network number, and the last octet is the host ID.

The following table shows the network number and host ID arrangement for classes A, B and C.

**Table 100** Classes of IP Addresses

IP ADDRESS	OCTET 1	OCTET 2	OCTET 3	OCTET 4
Class A	<b>Network number</b>	Host ID	Host ID	Host ID
Class B	<b>Network number</b>	<b>Network number</b>	Host ID	Host ID
Class C	<b>Network number</b>	<b>Network number</b>	<b>Network number</b>	Host ID

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 for example). Therefore, to determine the total number of hosts allowed in a network, deduct two as shown next:

- A class C address (1 host octet: 8 host bits) can have  $2^8 - 2$ , or 254 hosts.
- A class B address (2 host octets: 16 host bits) can have  $2^{16} - 2$ , or 65534 hosts.

A class A address (3 host octets: 24 host bits) can have  $2^{24} - 2$  hosts, or approximately 16 million hosts.

#### IP Address Classes and Network ID

The value of the first octet of an IP address determines the class of an address.

- Class A addresses have a **0** in the leftmost bit.
- Class B addresses have a **1** in the leftmost bit and a **0** in the next leftmost bit.
- Class C addresses start with **1 1 0** in the first three leftmost bits.
- Class D addresses begin with **1 1 1 0**. Class D addresses are used for multicasting, which is used to send information to groups of computers.
- There is also a class E. It is reserved for future use.

The following table shows the allowed ranges for the first octet of each class. This range determines the number of subnets you can have in a network.

**Table 101** Allowed IP Address Range By Class

CLASS	ALLOWED RANGE OF FIRST OCTET (BINARY)	ALLOWED RANGE OF FIRST OCTET (DECIMAL)
Class A	00000000 to 01111111	0 to 127
Class B	10000000 to 10111111	128 to 191
Class C	11000000 to 11011111	192 to 223
Class D	11100000 to 11101111	224 to 239
Class E (reserved)	11110000 to 11111111	240 to 255

### 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).

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.



---

Subnet masks are expressed in dotted decimal notation just like IP addresses. The “natural” masks for class A, B and C IP addresses are as follows.

**Table 102** “Natural” Masks

CLASS	NATURAL MASK
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

## Subnetting

With subnetting, the class arrangement of an IP address is ignored. For example, a class C address no longer has to have 24 bits of network number and 8 bits of host ID. With subnetting, some of the host ID bits are converted into network number bits.

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.

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 mask 255.255.255.128.

The following table shows all possible subnet masks for a class “C” address using both notations.

**Table 103** Alternative Subnet Mask Notation

SUBNET MASK	SUBNET MASK “1” BITS	LAST OCTET BIT VALUE	DECIMAL
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

The first mask shown is the class “C” natural mask. Normally if no mask is specified it is understood that the natural mask is being used.

## Example: Two Subnets

As an example, you have a class "C" address 192.168.1.0 with subnet mask of 255.255.255.0.

**Table 104** Two Subnets Example

IP/SUBNET MASK	NETWORK NUMBER	HOST ID
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask	255.255.255.	0
Subnet Mask (Binary)	11111111.11111111.11111111.	00000000

The first three octets of the address make up the network number (class "C").

To make two networks, divide the network 192.168.1.0 into two separate subnets by converting one of the host ID bits of the IP address to a network number bit. The "borrowed" host ID bit can be either "0" or "1" thus giving two subnets; 192.168.1.0 with mask 255.255.255.128 and 192.168.1.128 with mask 255.255.255.128.

Note: In the following charts, shaded/bolded last octet bit values indicate host ID bits "borrowed" to make network ID bits. The number of "borrowed" host ID bits determines the number of subnets you can have. The remaining number of host ID bits (after "borrowing") determines the number of hosts you can have on each subnet.

**Table 105** Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	<b>0</b> 0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	<b>1</b> 0000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

**Table 106** Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	<b>1</b> 0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	<b>1</b> 0000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Host IDs of all zeros represent the subnet itself and host IDs of all ones are the broadcast address for that subnet, so the actual number of hosts available on each subnet in the example above is  $2^7 - 2$  or 126 hosts for each subnet.

192.168.1.0 with mask 255.255.255.128 is the subnet itself, and 192.168.1.127 with mask 255.255.255.128 is the directed broadcast address for the first subnet. Therefore, the lowest IP address that can be assigned to an actual host for the first subnet is 192.168.1.1 and the highest is 192.168.1.126. Similarly the host ID range for the second subnet is 192.168.1.129 to 192.168.1.254.

## Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class "C" address space into two subnets. Similarly to divide a class "C" 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 (all zeroes is the subnet itself, all ones is the broadcast address on the subnet).

**Table 107** Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	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 108** 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 109** 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 110** Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	<b>11000000</b>
Subnet Mask (Binary)	11111111.11111111.11111111.	<b>11000000</b>
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 class C IP address last octet values for each subnet.

**Table 111** Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

The following table is a summary for class "C" subnet planning.

**Table 112** Class C 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

### Subnetting With Class A and Class B Networks.

For class "A" and class "B" addresses the subnet mask also determines which bits are part of the network number and which are part of the host ID.

---

A class "B" address has two host ID octets available for subnetting and a class "A" address has three host ID octets (see [Table 100 on page 239](#)) available for subnetting.

The following table is a summary for class "B" subnet planning.

**Table 113** Class B Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1



## Splitters and Microfilters

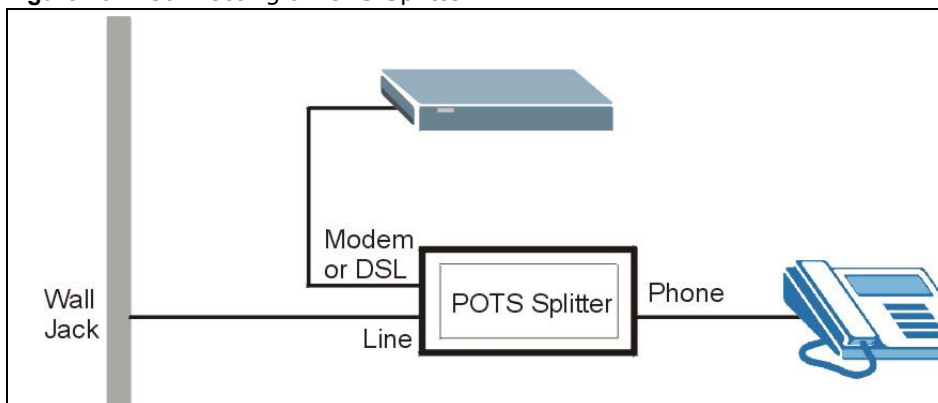
This appendix tells you how to install a POTS splitter or a telephone microfilter.

### Connecting a POTS Splitter

When you use the Full Rate (G.dmt) ADSL standard, you can use a POTS (Plain Old Telephone Service) splitter to separate the telephone and ADSL signals. This allows simultaneous Internet access and telephone service on the same line. A splitter also eliminates the destructive interference conditions caused by telephone sets.

Install the POTS splitter at the point where the telephone line enters your residence, as shown in the following figure.

**Figure 161** Connecting a POTS Splitter



- 1 Connect the side labeled "Phone" or "TEL" to your telephone.
- 2 Connect the side labeled "Modem" or "DSL" to your ZyXEL Device.
- 3 Connect the side labeled "Line" to the telephone wall jack.

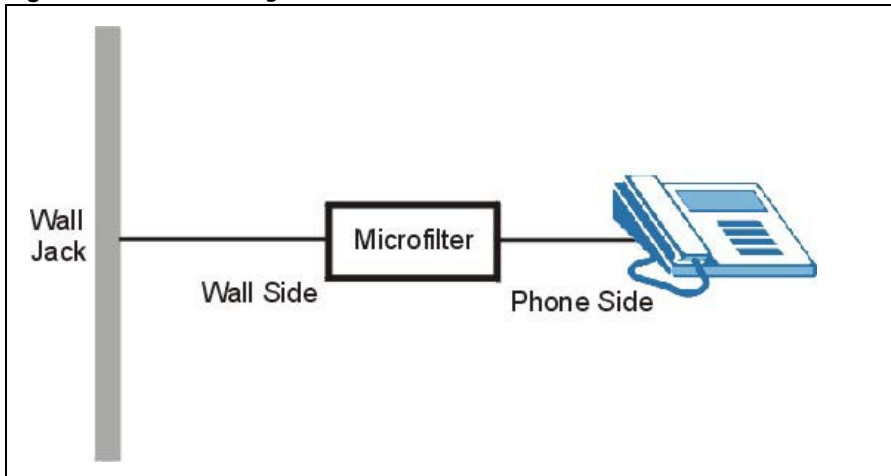
### Telephone Microfilters

Telephone voice transmissions take place in the lower frequency range, 0 - 4KHz, while ADSL transmissions take place in the higher bandwidth range, above 4KHz. A microfilter acts as a low-pass filter, for your telephone, to ensure that ADSL transmissions do not interfere with your telephone voice transmissions. The use of a telephone microfilter is optional.

- 1 Locate and disconnect each telephone.
- 2 Connect a cable from the wall jack to the "wall side" of the microfilter.
- 3 Connect the "phone side" of the microfilter to your telephone as shown in the following figure.

- 4 After you are done, make sure that your telephone works. If your telephone does not work, disconnect the microfilter and contact either your local telephone company or the provider of the microfilter.

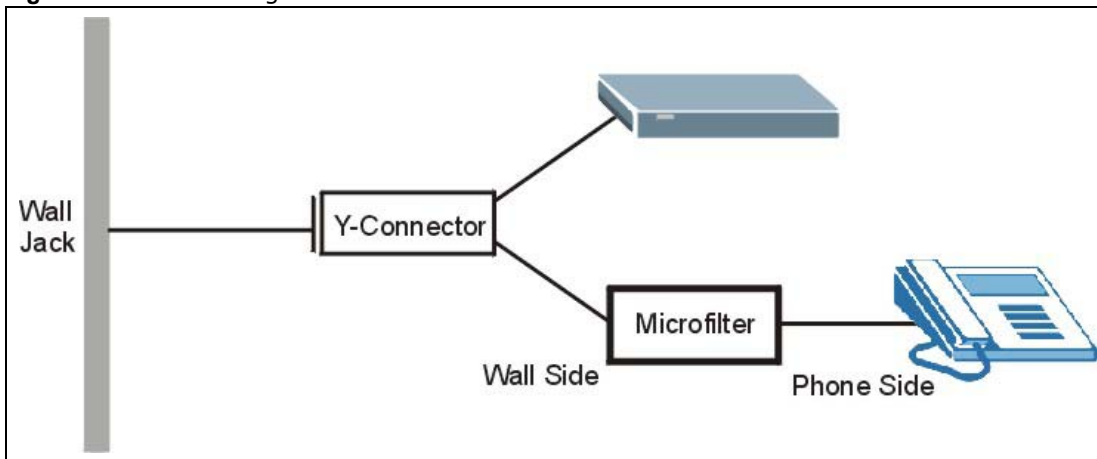
**Figure 162** Connecting a Microfilter



You can also use a Y-Connector with a microfilter in order to connect both your modem and a telephone to the same wall jack without using a POTS splitter.

- 1 Connect a phone cable from the wall jack to the single jack end of the Y-Connector.
- 2 Connect a cable from the double jack end of the Y-Connector to the "wall side" of the microfilter.
- 3 Connect another cable from the double jack end of the Y-Connector to the ZyXEL Device.
- 4 Connect the "phone side" of the microfilter to your telephone as shown in the following figure.

**Figure 163** Connecting a Microfilter and Y-Connector

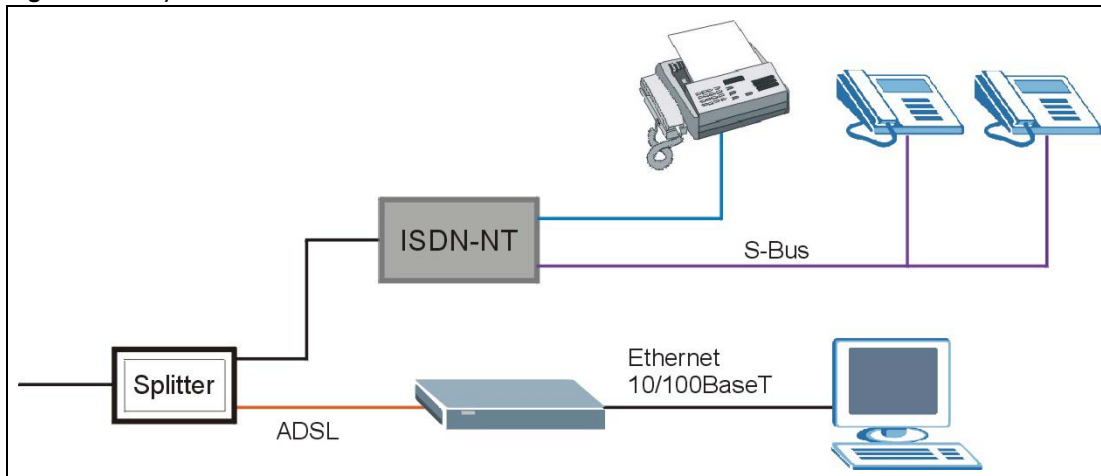




## ZyXEL Device With ISDN

This section relates to people who use their ZyXEL Device with ADSL over ISDN (digital telephone service) only. The following is an example installation for the ZyXEL Device with ISDN.

**Figure 164** ZyXEL Device with ISDN





# Pop-up Windows, JavaScripts and Java Permissions

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

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

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

## Internet Explorer Pop-up Blockers

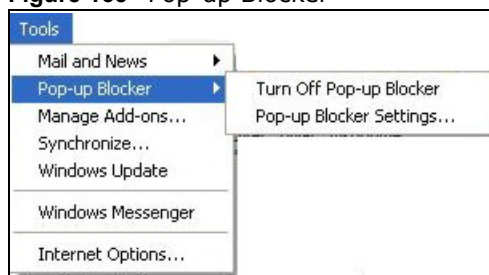
You may have to disable pop-up blocking to log into your device.

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

## Disable pop-up Blockers

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

Figure 165 Pop-up Blocker

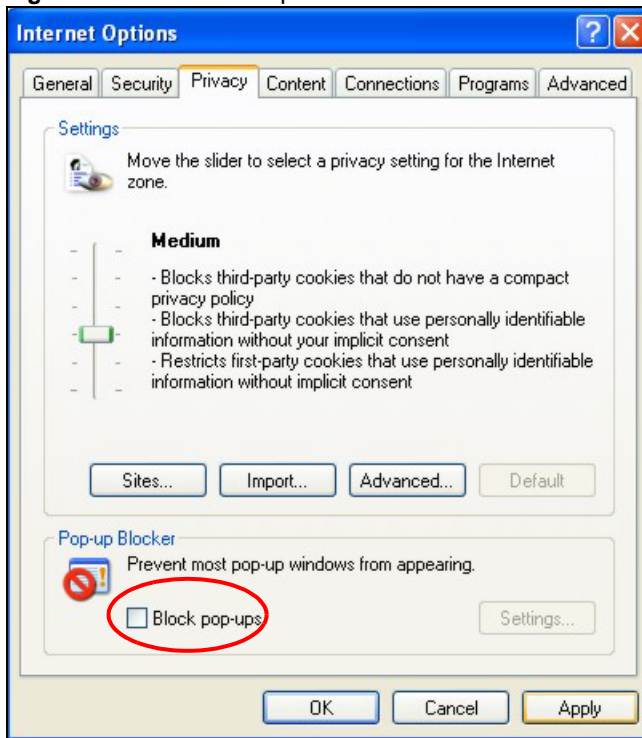


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

- 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 166** Internet Options



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

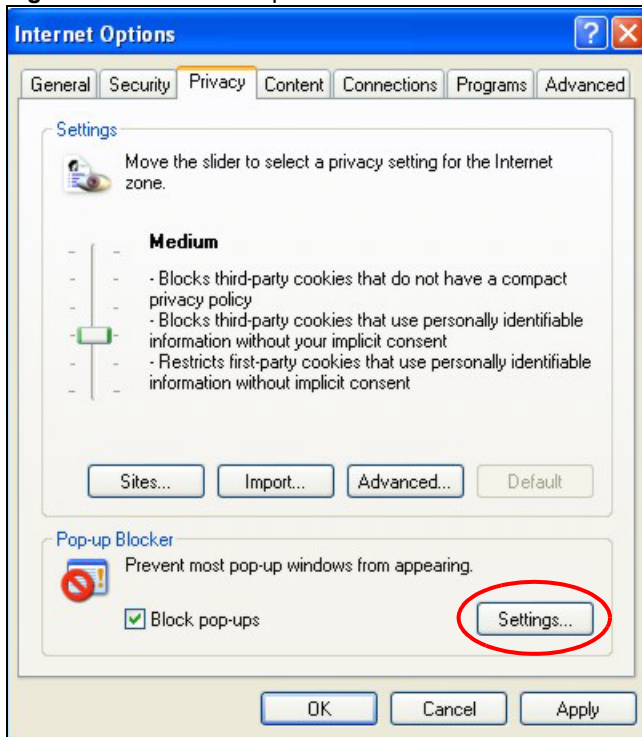
## Enable pop-up Blockers with Exceptions

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.

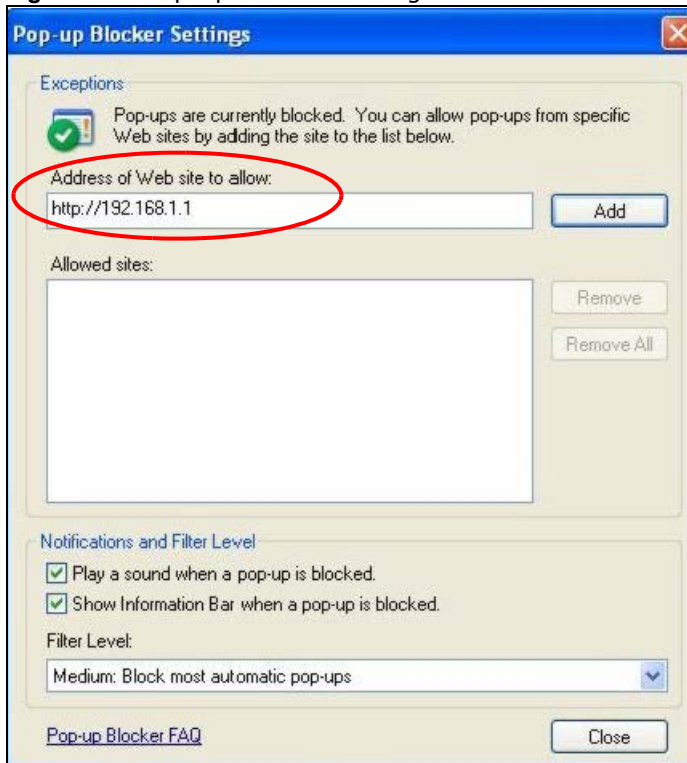
**Figure 167** Internet Options



- 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://192.168.1.1.

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

**Figure 168** Pop-up Blocker Settings



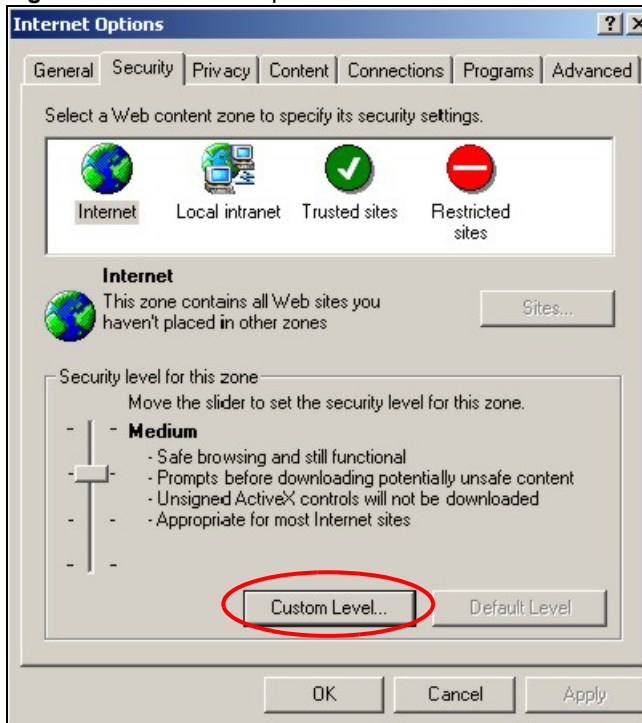
- 5 Click **Close** to return to the **Privacy** screen.
- 6 Click **Apply** to save this setting.

## 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.

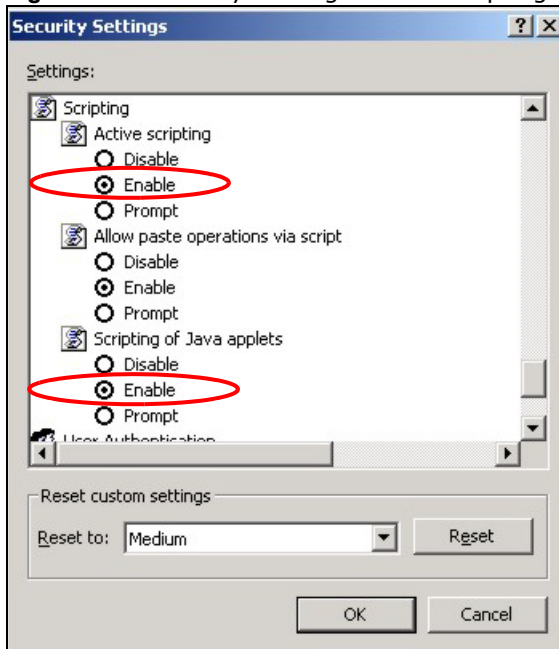
**Figure 169** Internet Options



- 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 170** Security Settings - Java Scripting



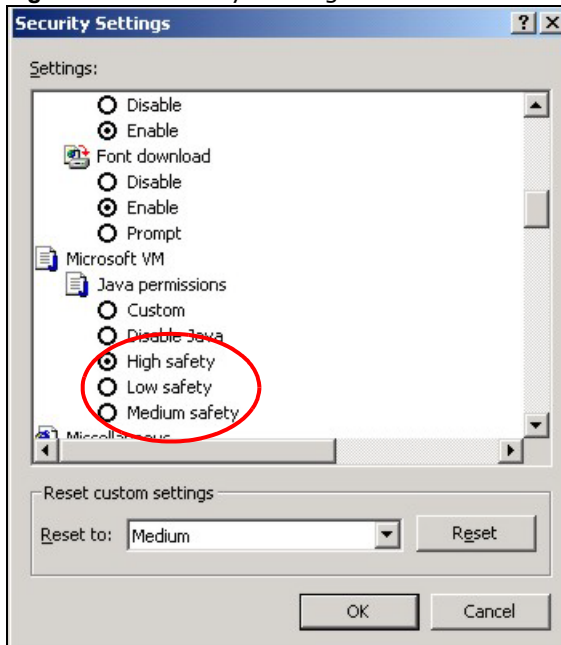
## Java Permissions

- 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 171** Security Settings - Java

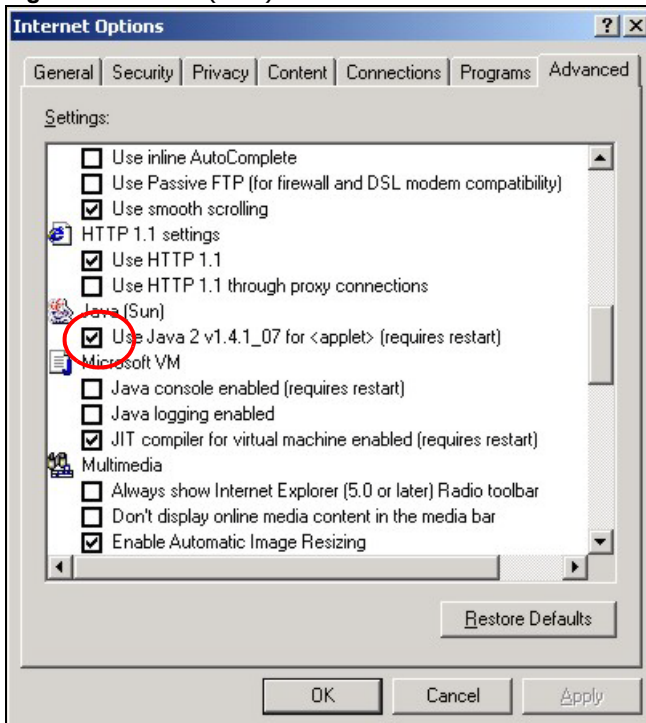


## JAVA (Sun)

- 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 172** Java (Sun)



## A

- activation
  - classifiers [151](#)
  - firewalls [90](#)
  - generic filters [110](#)
  - protocol filters [107](#)
  - SIP ALG [84](#)
- address assignment [64](#)
- Address Resolution Protocol (ARP) [67](#)
- ADSL standards [20](#), [218](#)
- alerts
  - firewalls [94](#)
- algorithm, certificates [124](#), [129](#)
  - MD5 fingerprint [125](#), [130](#), [134](#)
  - remote hosts [134](#)
  - SHA1 fingerprint [125](#), [130](#), [134](#)
- alternative subnet mask notation [241](#)
- anti-probing [86](#)
- Any IP [20](#)
  - and NAT [67](#)
  - how it works [67](#)
  - setup [69](#)
- applications
  - Internet access [22](#)
- asymmetrical routes [90](#)
- ATM Adaptation Layer 5 (AAL5) [44](#)

## B

- backup [207](#)
- backup gateway [60](#)
- backup type [60](#)
- bandwidth management [150](#)

## C

- CA [121](#)

- algorithm [129](#)
- CRL [129](#)
  - enrollment protocols [121](#)
  - property [128](#)
- CBR (Continuous Bit Rate) [52](#), [57](#)
- Certificate Management Protocol, see CMP
- certificates
  - algorithm [124](#), [129](#)
  - CA [121](#)
  - creation [118](#)
  - CRL [127](#), [128](#), [129](#)
  - deletion [118](#)
  - directory servers
    - LDAP [136](#)
    - login [137](#)
  - enrollment
    - options [121](#)
    - protocols [121](#)
  - exporting [130](#)
  - MD5 fingerprint [125](#)
  - modifications [118](#)
  - PEM [125](#), [130](#), [134](#)
  - property [123](#), [128](#)
  - SHA1 fingerprint [125](#)
  - types [117](#), [124](#)
- Certificates Revocation List, see CRL
- certifications [6](#)
  - Notice 1 [6](#)
- change password at login [25](#)
- classifiers
  - 802.1Q tags [153](#)
  - activation [151](#)
  - creation [151](#)
  - DSCP [153](#), [154](#)
  - FTP [154](#)
  - priority [152](#)
  - remote node [154](#)
  - routing policy [153](#)
  - SIP [154](#)
- client
  - DHCP [21](#)
- CMP [121](#)
- configuration

backup [207](#)  
firewalls [89, 93, 97](#)  
restore [207](#)  
copyright [5](#)  
cost of transmission [46](#)  
creation  
  certificates [118](#)  
  classifiers [151](#)  
CRL [127, 128, 129](#)  
customized services [94, 96](#)

## D

default LAN IP address [24](#)  
default settings [208](#)  
deletion, certificates [118](#)  
Denials of Service, see DoS  
DHCP [63, 65, 159, 185](#)  
  client [21](#)  
  configuration [63](#)  
  relay [21](#)  
  server [21](#)  
DHCP (Dynamic Host Configuration Protocol) [21](#)  
diagnostics [210](#)  
DiffServ Code Point, see DSCP  
directory servers  
  LDAP [136](#)  
  login [137](#)  
disclaimer [5](#)  
DNS [51](#)  
DNS (Domain Name System) [64](#)  
DNS and remote management [172](#)  
domain name [64, 185](#)  
  service type [80](#)  
domain name and DHCP clients [185](#)  
DoS [85](#)  
  three-way handshake [96](#)  
  thresholds [86, 96, 97, 98](#)  
DSCP [153, 154](#)  
DSL line, reinitialize [211](#)  
DSLAM (Digital Subscriber Line Access  
  Multiplexer) [22](#)  
dynamic DNS [21, 105, 145, 159](#)  
Dynamic Host Configuration Protocol [21](#)

DYNDNS wildcard [159](#)

## E

ECHO [80](#)  
e-mail logs [194](#)  
embedded help [27](#)  
Encapsulated Routing Link Protocol (ENET  
  ENCAP) [43](#)  
encapsulation [43, 44](#)  
  ENET ENCAP [43](#)  
  PPP over Ethernet [43](#)  
  PPPoA [44](#)  
  RFC 1483 [44](#)  
enrollment  
  options, certificates [121](#)  
  protocols, certificates [121](#)  
exporting  
  remote hosts, certificates [134](#)  
  trusted CA [130](#)

## F

factory default settings [208](#)  
FCC [6](#)  
FCC Rules [6](#)  
features [219](#)  
Federal Communications Commission [5](#)  
filters  
  packets  
    logs [109, 112](#)  
    types [106](#)  
Finger, protocol [80](#)  
firewalls [85](#)  
  actions [94](#)  
  activation [90](#)  
  address types [94](#)  
  alerts [94](#)  
  anti-probing [86](#)  
  asymmetrical routes [90](#)  
  configuration [89, 93, 97](#)  
  customized services [94, 96](#)  
  default action [90](#)  
  DoS [85](#)

- thresholds [86, 96, 97, 98](#)
- example [86](#)
- half-open sessions [98](#)
- ICMP [86](#)
- logs [94](#)
- maximum incomplete [98](#)
- P2P [97](#)
- packet direction [90](#)
- rules [91, 99](#)
- schedules [94](#)
- security [100](#)
- three-way handshake [96](#)
- triangle route [90, 101](#)
  - solutions [102](#)
- firmware [205](#)
  - upgrade [205](#)
  - upload [205](#)
  - upload error [206](#)
- FTP [80, 163, 168](#)
  - and NAT [80](#)
  - and remote management [168](#)
  - QoS [154](#)
- FTP restrictions [163](#)

## G

- general setup [185](#)
- generic filters
  - activation [110](#)
  - length [111](#)
  - logs [112](#)
  - mask [111](#)
  - offset [111](#)

## H

- half-open sessions [98](#)
- help, web configurator [27](#)
- HTTP [80](#)
  - and remote management [163](#)
- HTTP (Hypertext Transfer Protocol) [205](#)
- HTTPS [166](#)

## I

- IANA [65](#)
- ICMP [86](#)
- IGMP
  - and multicasting [66](#)
  - versions [66](#)
- IGMP (Internet Group Multicast Protocol) [66](#)
- importing
  - remote hosts [131](#)
  - trusted CA [127](#)
- Integrated Services Digital Network
  - See ISDN
- Interference Statement [6](#)
- Internet access [20, 22, 34](#)
  - setup [214](#)
  - troubleshooting [214](#)
  - wizard setup [34](#)
  - Zero Configuration [20](#)
- Internet Assigned Numbers AuthoritySee IANA [65](#)
- Internet Control Message Protocol, see ICMP
- IP

- address [65](#)
- address assignment [45](#)
- address assignment ENET ENCAP [45](#)
- address assignment PPPoA [45](#)
- address assignment PPPoE [45](#)
- address assignment RFC 1483 [45](#)
- address pool [64](#)
  - and static route [141](#)
- ANY IP feature [20](#)
- default LAN address [24](#)
- pool of addresses [70](#)
- IP address [80](#)
  - and NAT [82](#)
  - default server [80](#)
  - NAT [81](#)

- IP alias [21](#)

- IP Pool Setup [64](#)

- ISDN (Integrated Services Digital Network) [19](#)

## L

- LAN
  - DHCP [63](#)

---

- TCP/IP [65](#)
- LDAP [136](#)
- Lightweight Directory Access Protocol, see LDAP
- login [25](#)
  - directory servers [137](#)
- logs
  - e-mail [194](#)
  - firewalls [94](#)
  - generic filters [112](#)
  - protocol filters [109](#)
  - schedules [194](#)

## M

- management
  - types of [218](#)
- Management Information Base (MIB) [169](#)
- Maximum Burst Size (MBS) [47](#), [53](#), [58](#)
- maximum incomplete [98](#)
- MD5 fingerprint [125](#), [130](#), [134](#)
- metric [46](#)
- metric, cost of transmission [46](#)
- MIB (Management Information Base) [169](#)
- modifications, certificates [118](#)
- multicast [66](#)
- multiplexing [44](#)
  - LLC-based [44](#)
  - VC-based [44](#)
- multiprotocol encapsulation [44](#)

## N

- nailed-up connection [45](#)
- NAT [65](#), [80](#)
  - address mapping rule [84](#)
  - and servers [77](#)
  - application [77](#)
  - configuration [79](#)
  - definitions [75](#)
  - example [81](#)
  - how it works [76](#)
  - mapping types [77](#)
  - mode [79](#)
  - port forwarding [80](#)

- port numbers [80](#)
- SIP ALG
  - activation [84](#)
  - specifications [218](#)
  - what it does [76](#)
- NAT (Network Address Translation) [75](#)
- NAT Traversal [174](#)
- navigating the web configurator [26](#)
- Network Address Translation (NAT) [21](#)
- NNTP [80](#)

## P

- P2P [97](#)
- packet direction [90](#)
- packet filter
  - WAN [53](#), [58](#)
- packet filtering
  - types [106](#)
- packet filters
  - logs [109](#), [112](#)
- password
  - change at login [25](#)
- Peak Cell Rate (PCR) [46](#), [52](#), [57](#)
- PEM [125](#), [130](#), [134](#)
- Point to Point Protocol over ATM Adaptation Layer 5 (AAL5) [44](#)
- Point-to-Point Tunneling Protocol [80](#)
- POP3 [80](#)
- port number [80](#)
- PPPoA [44](#)
- PPPoE [43](#)
  - benefits [43](#)
- PPPoE (Point-to-Point Protocol over Ethernet) [21](#)
- PPTP [80](#)
- Privacy Enhanced Mail, see PEM
- probing, firewalls [86](#)
- product specifications [217](#)
  - dimensions [217](#)
  - operating conditions [217](#)
  - power [217](#)
- property, certificates [123](#)
- protocol filters
  - activation [107](#)

---

logs [109](#)  
protocols supported [218](#)

## Q

### QoS

802.1Q tags [153](#)  
bandwidth [150](#)  
classifiers  
    activation [151](#)  
    creation [151](#)  
    priority [152](#)  
DSCP [153](#), [154](#)  
FTP [154](#)  
remote node [154](#)  
routing policy [153](#)  
SIP [154](#)

### Quick Start Guide

hardware connections [24](#)

## R

reinitialize the ADSL line  
    diagnostics  
        ADSL line [211](#)

related documentation [3](#)

remote hosts, certificates  
    algorithm [134](#)  
    exporting [134](#)  
    importing [131](#)  
    MD5 fingerprint [134](#)  
    PEM [134](#)  
    SHA1 fingerprint [134](#)  
    types [133](#)

remote management [163](#)  
    and FTP [168](#)  
    and LAN [163](#)  
    and SNMP [169](#)  
    and WAN [163](#)  
    disabling [163](#)  
    enabling [163](#)  
    HTTPS [166](#)  
    types of sessions [163](#)

remote management and NAT [163](#)

remote management limitations [163](#)

remote node [154](#)

reset button [26](#)

resetting  
    and factory default settings [208](#)

resetting the ZyXEL Device [26](#)

restore configuration [207](#)

RFC 1483 [44](#)

RFC 1631 [75](#)

RFC-1483 [45](#)

RFC-2364 [44](#)

RFC2516, PPPoE [21](#)

### RIP

    direction [66](#)

    version [66](#)

RIP (Routing Information Protocol) [66](#)

Routing Information Protocol

    See also RIP [66](#)

Routing Information Protocol (RIP) [66](#)

routing policy [153](#)

## S

safety warnings [7](#)

SCEP [121](#)

### schedules

    firewalls [94](#)

    logs [194](#)

### security

    network [100](#)

### server

    DHCP [21](#)

### servers

    and NAT [78](#)

    time server [188](#)

service type, WAN [214](#)

### services

    and NAT [80](#)

    port numbers [80](#)

Session Initiation Protocol, see SIP

### setup

    firewalls [89](#), [93](#), [97](#)

SHA1 fingerprint [125](#), [130](#), [134](#)

Simple Certificate Enrollment Protocol, see SCEP

SIP ALG [154](#)

- activation [84](#)
- SMTP [80](#)
- SNMP [80](#), [169](#)
  - agent [169](#)
  - and remote management [169](#)
  - manager [169](#)
  - MIBs [170](#)
- SNMP (Simple Network Management Protocol) [169](#)
- SNMP manager [169](#)
- splitters [247](#)
- splitters and microfilters [247](#)
- standards, ADSL [218](#)
- static route
  - example [141](#)
  - how it works [141](#)
  - remote nodes [141](#)
- SUA [78](#)
- SUA (Single User Account) [78](#)
- SUA vs NAT
  - SUA (Single User Account) [78](#)
- subnet [239](#)
- subnet mask [65](#), [240](#)
- subnetting [241](#)
- supported protocols [218](#)
- Sustain Cell Rate (SCR) [53](#), [58](#)
- Sustained Cell Rate (SCR) [47](#)
- syntax conventions [4](#)
- system name [186](#)
- system timeout [164](#)

## T

- Telnet [167](#)
  - and remote management [163](#), [167](#)
- TFTP restrictions [163](#)
- three-way handshake [96](#)
- thresholds
  - DoS [86](#), [96](#), [97](#), [98](#)
  - P2P [97](#)
- trademarks [5](#)
- traffic redirect [20](#), [58](#), [59](#), [61](#)
  - example [58](#)
- traffic shaping [46](#)
- triangle route [90](#), [101](#)

- solutions [102](#)
- troubleshooting [214](#)
  - Internet access [214](#)
- trusted CA
  - algorithm [129](#)
  - CRL [127](#), [128](#), [129](#)
  - exporting [130](#)
  - importing [127](#)
  - MD5 fingerprint [130](#)
  - PEM [130](#)
  - SHA1 fingerprint [130](#)

## U

- UBR (Unspecified Bit Rate) [52](#), [57](#)
- Universal Plug and Play [174](#)
  - Application [174](#)
- Universal Plug and Play (UPnP) [20](#)
- UPnP [174](#)
  - Forum [175](#)
  - installation [176](#)
  - installation, Windows Me [176](#)
  - installation, Windows XP [177](#)
  - security issues [174](#)
- user name [160](#)

## V

- VBR (Variable Bit Rate) [52](#), [57](#)
- VC-based multiplexing [44](#)
- viewing certifications [6](#)
- Virtual Channel Identifier (VCI) [45](#)
- virtual circuit (VC) [44](#)
- Virtual Path Identifier (VPI) [45](#)
- VPI & VCI [45](#)

## W

- WAN
  - backup type [60](#)
  - DNS [51](#)
  - encapsulation [43](#)



---

- ENET ENCAP [43](#)
  - mode [50](#)
  - modulation [50](#)
  - packet filter [53, 58](#)
  - PPP over Ethernet [43](#)
  - PPPoA [44](#)
  - Setup [43](#)
  - troubleshooting [214](#)
- WAN (Wide Area Network) [43](#)
- WAN backup [60](#)
- web and remote management [164](#)
- web configurator [24, 26](#)
  - help [27](#)
  - main screen [26](#)
  - navigating [26](#)
  - screen summary [27](#)

## Z

- Zero Configuration Internet Access [20, 48](#)
- ZyNOS (ZyXEL Network Operating System) [5](#)
- ZyXEL Home Page [6](#)
- ZyXEL Network Operating System [5](#)





