P-660W-Tx v2

ADSL Router over POTS/ISDN

User's Guide

Version 3.40
03/2008
Edition 2

DEFAULT LOGIN	
IP Address	**http://192.168.1.1**
Password	**1234**

ZyXEL

www.zyxel.com

About This User's Guide

Intended Audience

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

Related Documentation

- Quick Start Guide

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

  Embedded web help for descriptions of individual screens and supplementary information.
- Command Reference Guide

  The Command Reference Guide explains how to use the Command-Line Interface (CLI) and CLI commands to configure the ZyXEL Device.

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

- Supporting Disk

  Refer to the included CD for support documents.
- ZyXEL Web Site

  Please refer to www.zyxel.com for additional support documentation and product certifications.

User’s Guide Feedback

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

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

E-mail: techwriters@zyxel.com.tw

Document Conventions

Warnings and Notes

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

Warnings tell you about things that could harm you or your ZyXEL Device.

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

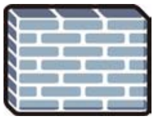
Syntax Conventions

- The P-660W-T1 v2 and the P-660W-T3 v2 may be referred to as the “ZyXEL Device”, the “P-660W-Tx v2”, 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 upper case 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 ZyXEL Device.

Table 1 Common Icons

ZyXEL Device 	Computer 	Notebook
Server 	Printer 	Telephone
Switch 	Router 	Internet Cloud
Firewall 	Modem 	Wireless Signal
Television 	DSLAM 	

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.
- ONLY qualified service personnel should service or disassemble this device.
- 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 it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Use ONLY power wires of the appropriate wire gauge (see Chapter 20 on page 201 for details) for your device. Connect it to a power supply of the correct voltage (see Chapter 20 on page 201 for details).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

This product is recyclable. Dispose of it properly.

Contents Overview

Table of Contents

Chapter 11

Chapter 12

List of Figures

List of Tables

PART I
Introduction

Introducing the ZyXEL Device

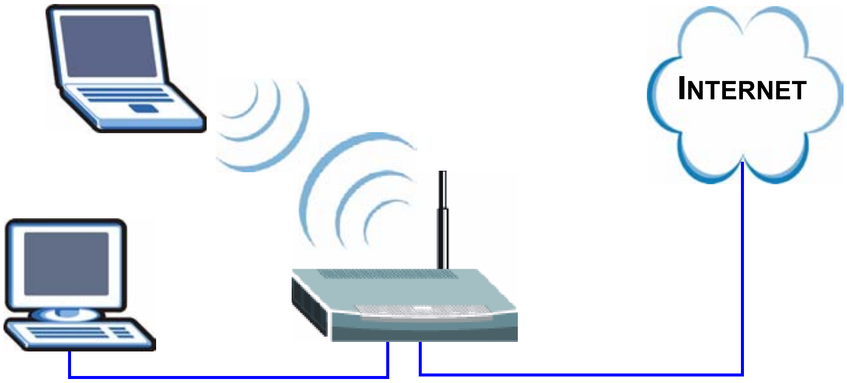
This chapter introduces the main applications and features of the ZyXEL Device. It also introduces the ways you can manage the ZyXEL Device.

1.1 Overview

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

The ZyXEL Device is an ADSL (Asymmetric Digital Subscriber Line) router and modem with wireless capability. See Chapter 20 on page 201 for a complete list of features.

Figure 1 High-speed Internet Access with the ZyXEL Device



Connect your computer(s) to the ZyXEL Device. The ZyXEL Device uses the phone line to provide high-speed Internet access to the computer(s). You can continue to use the phone line for regular phone calls as well. See the Quick Start Guide for instructions on making these connections.

1.2 Ways to Manage the ZyXEL Device

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

- Web Configurator. This is recommended for everyday management of the ZyXEL Device using a (supported) web browser. See Chapter 2 on page 33.
- Command Line Interface. Line commands are mostly used for troubleshooting by service engineers. See the CLI Reference Guide.

- FTP. Use File Transfer Protocol for firmware upgrades and configuration backup/restore. See Chapter 18 on page 190.

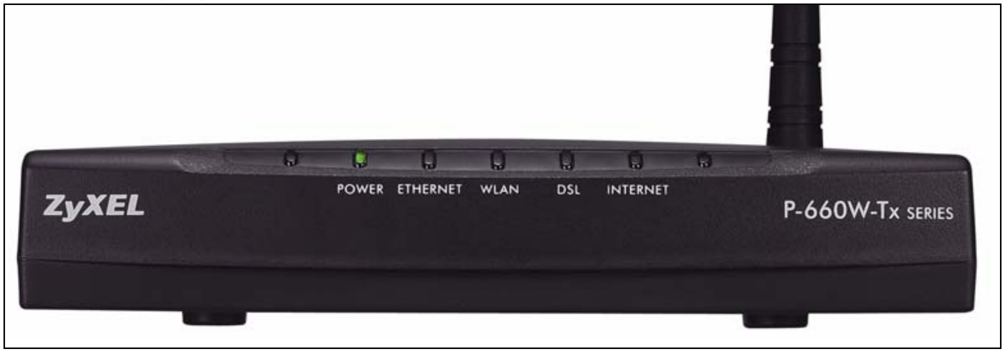
1.3 Good Habits for Managing the ZyXEL Device

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

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

1.4 LEDs

The following figure shows the front panel LEDs.



The following table describes the LEDs.

Table 2 Front Panel LEDs

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The ZyXEL Device is receiving power and functioning properly.
		Blinking	The ZyXEL Device is rebooting or performing diagnostics.
		Off	The system is not ready or has malfunctioned.
ETHERNET	Green	On	The ZyXEL Device has a successful 10/100 Mb Ethernet connection.
		Blinking	The ZyXEL Device is sending/receiving data.
		Off	The ZyXEL Device does not have an Ethernet connection.

Table 2 Front Panel LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
WLAN	Green	On	The ZyXEL Device is ready, but is not sending/receiving data through the wireless LAN.
		Blinking	The ZyXEL Device is sending/receiving data through the wireless LAN.
		Off	The wireless LAN is not ready or has failed.
DSL	Green	Fast Blinking	The ZyXEL Device is trying to detect the DSL signal.
		Slow Blinking	The ZyXEL Device is initializing the DSL line.
		On	The DSL link is successful.
		Off	The DSL link is down.
INTERNET	Green	On	The ZyXEL Device has a successful connection to the Internet.
		Blinking	There is data traffic on the ZyXEL Device’s Internet connection.
		Off	The ZyXEL Device has no connection with the Internet.

2

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).

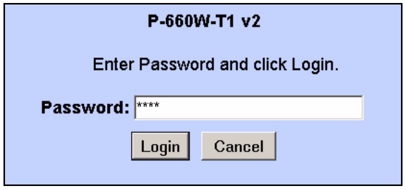
See the chapter on troubleshooting if you need to make sure these functions are allowed in Internet Explorer.

2.1.1 Accessing the Web Configurator

Note: Even though you can connect to the ZyXEL Device wirelessly, it is recommended that you connect your computer to a LAN port for initial configuration.

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.The **Password** field already contains the default password “1234”. Click **Login** to proceed to a screen asking you to change your password or click **Cancel** to revert to the default password.

Figure 2 Password Screen



P-660W-T1 v2

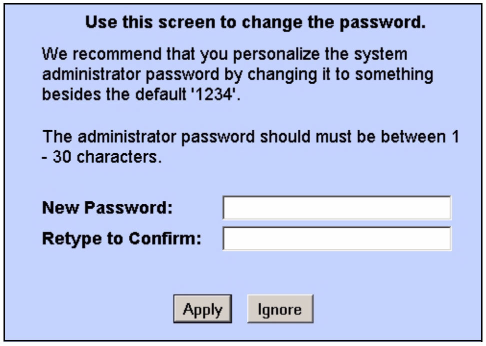
Enter Password and click Login.

Password: ****

6 It is highly recommended you change the default 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.

Figure 3 Change Password at Login



Use this screen to change the password.

We recommend that you personalize the system administrator password by changing it to something besides the default '1234'.

The administrator password should must be between 1 - 30 characters.

New Password:

Retype to Confirm:

7 You should now see the **SITE MAP** screen.

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

2.1.2 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”.

2.1.2.1 Using the Reset Button

1 Make sure the **POWER** LED is on (not blinking).

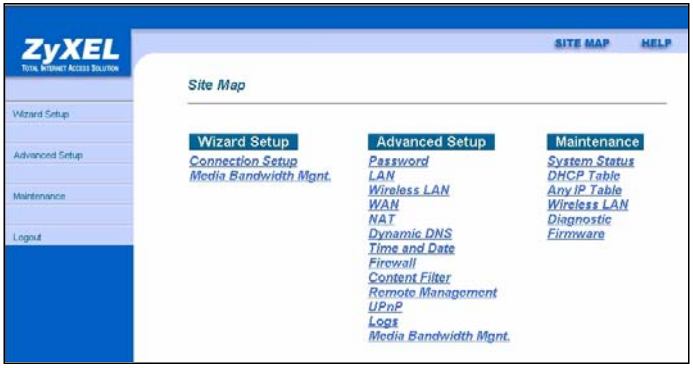
2 Press the **RESET** button for ten seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the ZyXEL Device restarts.

2.1.3 Navigating the Web Configurator

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

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

Figure 4 Web Configurator: Site Map Screen



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

Table 3 Web Configurator Screens Summary

LINK	SUB-LINK	FUNCTION
Wizard Setup	Connection Setup	Use these screens for initial configuration including general setup, ISP parameters for Internet Access and WAN IP/DNS Server/MAC address assignment.
	Media Bandwidth Mgnt	Use these screens to limit bandwidth usage by application.
Advanced Setup		
Password		Use this screen to change your password.
LAN	LAN Setup	Use this screen to configure LAN settings.
	Static DHCP	Use this screen to configure static DHCP settings on your LAN.
Wireless LAN	Wireless	Use this screen to configure the wireless LAN settings.
	MAC Filter	Use this screen to change MAC filter settings on the ZyXEL Device.
WAN	WAN Setup	Use this screen to change the ZyXEL Device’s WAN remote node settings.
	WAN Backup	Use this screen to configure your traffic redirect properties and WAN backup settings.
NAT		Use this screen to configure the NAT mode.
Dynamic DNS		Use this screen to set up dynamic DNS.
Time and Date		Use this screen to change your ZyXEL Device’s time and date.

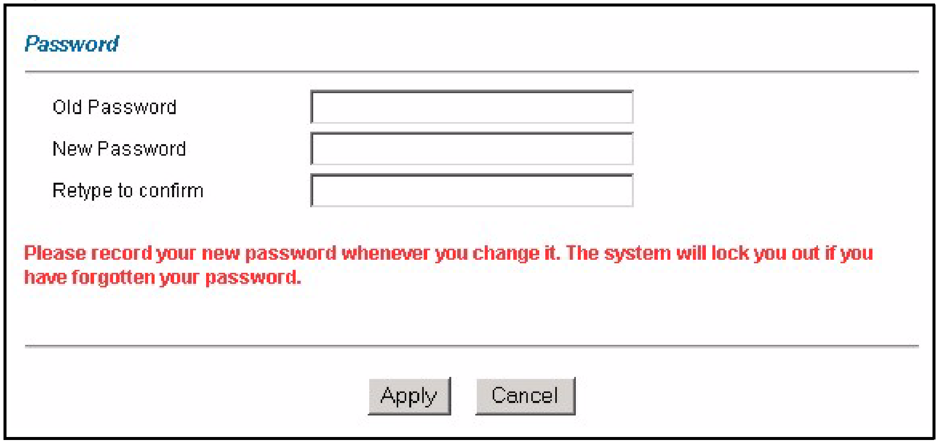
Table 3 Web Configurator Screens Summary (continued)

LINK	SUB-LINK	FUNCTION
Firewall	Default Policy	Use this screen to activate/deactivate the firewall and the direction of network traffic to which to apply the rule.
	Rule Summary	This screen shows a summary of the firewall rules, and allows you to edit/add a firewall rule.
	Anti Probing	Use this screen to change your anti-probing settings.
	Threshold	Use this screen to configure the threshold for DoS attacks.
Content Filter	Keyword	Use this screen to block sites containing certain keywords in the URL.
	Schedule	Use this screen to set the days and times for the ZyXEL Device to perform content filtering.
	Trusted	Use this screen to exclude a range of users on the LAN from content filtering on your ZyXEL Device.
Remote Management		Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet/FTP/Web to manage the ZyXEL Device.
UPnP		Use this screen to enable UPnP on the ZyXEL Device.
Logs	Log Settings	Use this screen to change your ZyXEL Device's log settings.
	View Log	Use this screen to view the logs for the categories that you selected.
Media Bandwidth Management	Summary	Use this screen to assign bandwidth limits to specific types of traffic.
	Class Setup	Use this screen to define a bandwidth class.
	Monitor	Use this screen to view bandwidth class statistics.
Maintenance		
System Status		This screen contains administrative and system-related information.
DHCP Table		This screen displays DHCP (Dynamic Host Configuration Protocol) related information and is READ-ONLY.
Any IP Table		Use this screen to view the IP and MAC addresses of LAN computers communicating with the ZyXEL Device.
Wireless LAN	Association List	This screen displays the MAC address(es) of the wireless stations that are currently associating with the ZyXEL Device.
Diagnostic	General	These screens display information to help you identify problems with the ZyXEL Device general connection.
	DSL Line	These screens display information to help you identify problems with the DSL line.
Firmware		Use this screen to upload firmware to your ZyXEL Device
LOGOUT		Click **Logout** to exit the web configurator.

2.2 Change 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 **Password** in the **Site Map** screen to display the screen as shown next.

Figure 5 Password



Password

Old Password

New Password

Retype to confirm

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

The following table describes the fields in this screen.

Table 4 Password

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

PART II
Setup Wizard

3

Connection Setup Wizard

The Connection Wizard assists you in setting up Internet access. This chapter provides information on the Connection Wizard screens in the web configurator.

3.1 Introduction

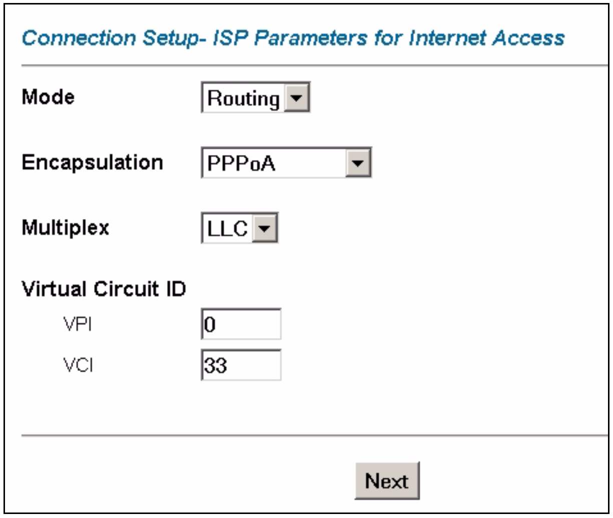
Use the Connection Wizard screens to configure your system for Internet access with the information given to you by your ISP (Internet Service Provider).

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

3.1.1 Internet Access Wizard Setup

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

Figure 6 Internet Access Wizard Setup: ISP Parameters



Connection Setup- ISP Parameters for Internet Access

Mode: Routing

Encapsulation: PPPoA

Multiplex: LLC

Virtual Circuit ID

VPI: 0

VCI: 33

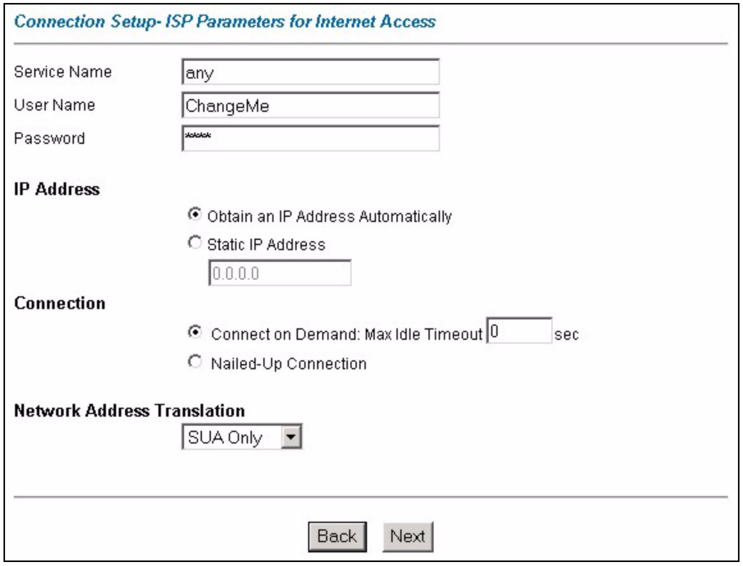
The following table describes the fields in this screen.

Table 5 Internet Access Wizard Setup: ISP Parameters

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

2 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 7 Internet Connection with PPPoE



Connection Setup- ISP Parameters for Internet Access

Service Name: any

User Name: ChangeMe

Password: ****

IP Address

● Obtain an IP Address Automatically

○ Static IP Address: 0.0.0.0

Connection

● Connect on Demand: Max Idle Timeout 0 sec

○ Nailed-Up Connection

Network Address Translation

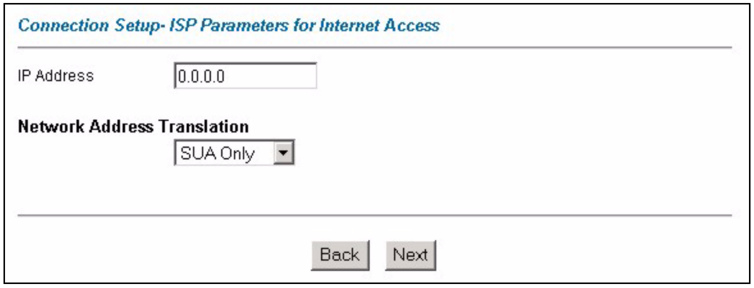
SUA Only

The following table describes the fields in this screen.

Table 6 Internet Connection with PPPoE

LABEL	DESCRIPTION
Service Name	Type the name of your PPPoE service here.
User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
IP Address	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select **Obtain an IP Address Automatically** if you have a dynamic IP address; otherwise select **Static IP Address** and type your ISP assigned IP address in the text box below.
Connection	Select **Connect on Demand** when you don't want the connection up all the time and specify an idle time-out (in seconds) in the **Max. Idle Timeout** field. The default setting selects **Connection on Demand** with 0 as the idle time-out, which means the Internet session will not timeout. Select **Nailed-Up Connection** when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
Network Address Translation	Select **None**, **SUA Only** or **Full Feature** from the drop-down list box. Refer to the NAT chapter for more details.
Back	Click **Back** to go back to the first wizard screen.
Next	Click **Next** to continue to the next wizard screen.

Figure 8 Internet Connection with RFC 1483



Connection Setup- ISP Parameters for Internet Access

IP Address 0.0.0.0

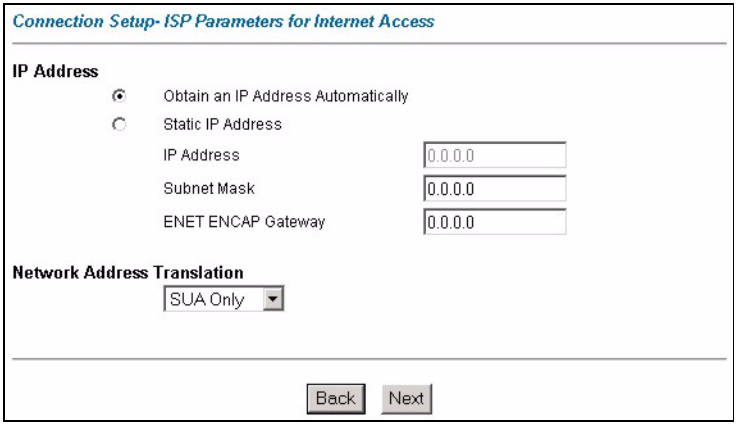
Network Address Translation SUA Only

The following table describes the fields in this screen.

Table 7 Internet Connection with RFC 1483

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

Figure 9 Internet Connection with ENET ENCAP



Connection Setup- ISP Parameters for Internet Access

IP Address

● Obtain an IP Address Automatically

○ Static IP Address

IP Address 0.0.0.0

Subnet Mask 0.0.0.0

ENET ENCAP Gateway 0.0.0.0

Network Address Translation SUA Only

The following table describes the fields in this screen.

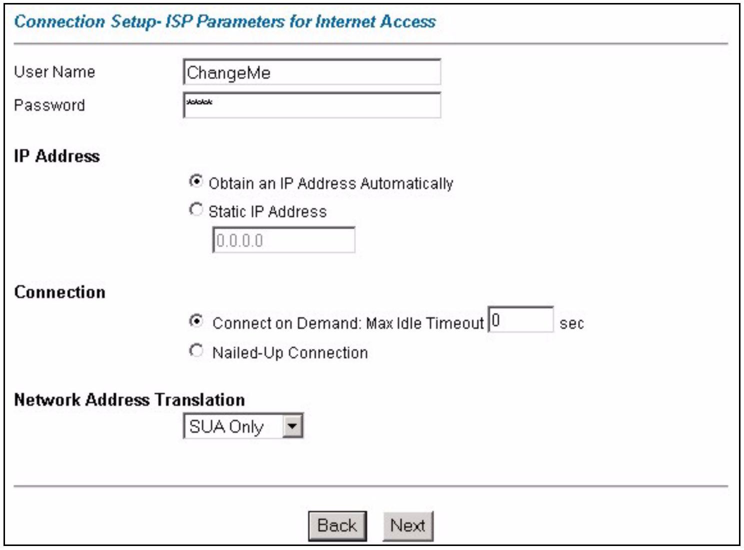
Table 8 Internet Connection with ENET ENCAP

LABEL	DESCRIPTION
IP Address	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select **Obtain an IP Address Automatically** if you have a dynamic IP address; otherwise select **Static IP Address** and type your ISP assigned IP address in the IP Address text box below.
Subnet Mask	Enter a subnet mask in dotted decimal notation. Refer to the appendices to calculate a subnet mask If you are implementing subnetting.

Table 8 Internet Connection with ENET ENCAP (continued)

LABEL	DESCRIPTION
ENET ENCAP Gateway	You must specify a gateway IP address (supplied by your ISP) when you use **ENET ENCAP** in the **Encapsulation** field in the previous screen.
Network Address Translation	Select **None**, **SUA Only** or **Full Feature** from the drop-sown list box. Refer to the NAT chapter for more details.
Back	Click **Back** to go back to the first wizard screen.
Next	Click **Next** to continue to the next wizard screen.

Figure 10 Internet Connection with PPPoA



Connection Setup- ISP Parameters for Internet Access

User Name: ChangeMe

Password: *****

IP Address

● Obtain an IP Address Automatically

○ Static IP Address

0.0.0.0

Connection

● Connect on Demand: Max Idle Timeout 0 sec

○ Nailed-Up Connection

Network Address Translation

SUA Only

The following table describes the fields in this screen.

Table 9 Internet Connection with PPPoA

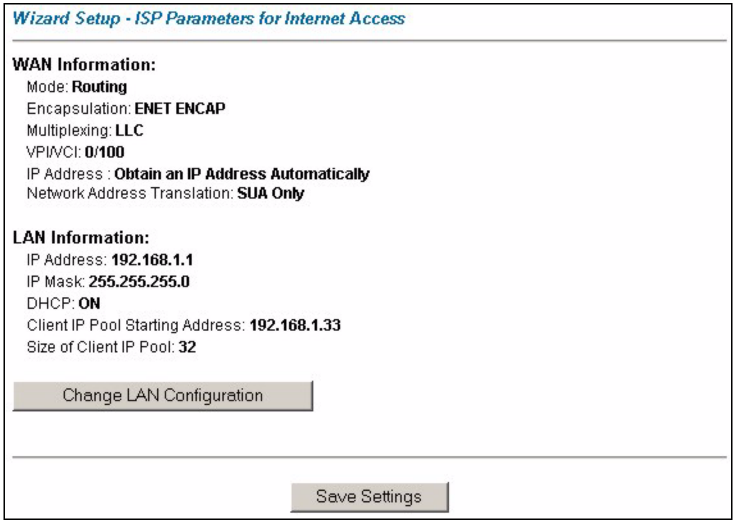
LABEL	DESCRIPTION
User Name	Enter the login name that your ISP gives you.
Password	Enter the password associated with the user name above.
IP Address	This option is available if you select **Routing** in the **Mode** field. A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Click **Obtain an IP Address Automatically** if you have a dynamic IP address; otherwise click **Static IP Address** and type your ISP assigned IP address in the IP Address text box below.
Connection	Select **Connect on Demand** when you don't want the connection up all the time and specify an idle time-out (in seconds) in the **Max. Idle Timeout** field. The default setting selects **Connection on Demand** with 0 as the idle time-out, which means the Internet session will not timeout. Select **Nailed-Up Connection** when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.

Table 9 Internet Connection with PPPoA (continued)

LABEL	DESCRIPTION
Network Address Translation	This option is available if you select **Routing** in the **Mode** field. Select **None**, **SUA Only** or **Full Feature** from the drop-sown list box. Refer to the NAT chapter for more details.
Back	Click **Back** to go back to the first wizard screen.
Next	Click **Next** to continue to the next wizard screen.

3 Verify the settings in the screen shown next. To change the LAN information on the ZyXEL Device, click **Change LAN Configurations**. Otherwise click **Save Settings** to save the configuration and skip to the section 3.13.

Figure 11 Internet Access Wizard Setup: Third Screen



Wizard Setup - ISP Parameters for Internet Access

WAN Information:

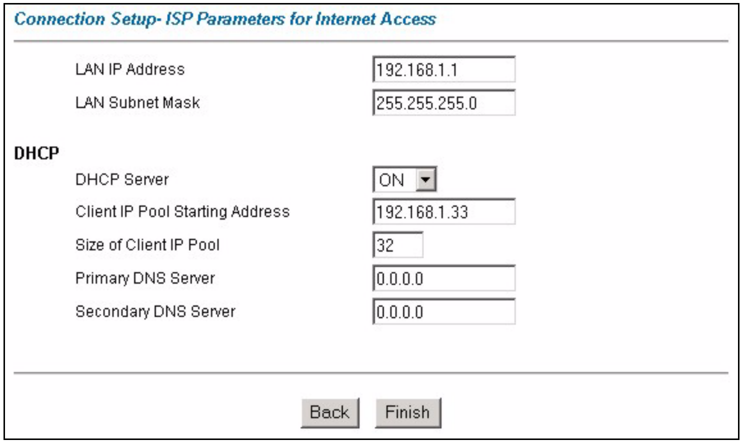
Mode: **Routing**
Encapsulation: **ENET ENCAP**
Multiplexing: **LLC**
VPI/VCI: **0/100**
IP Address : **Obtain an IP Address Automatically**
Network Address Translation: **SUA Only**

LAN Information:

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

If you want to change your ZyXEL Device LAN settings, click **Change LAN Configuration** to display the screen as shown next.

Figure 12 Internet Access Wizard Setup: LAN Configuration



Connection Setup- ISP Parameters for Internet Access

LAN IP Address: 192.168.1.1
LAN Subnet Mask: 255.255.255.0

DHCP

DHCP Server: ON
Client IP Pool Starting Address: 192.168.1.33
Size of Client IP Pool: 32
Primary DNS Server: 0.0.0.0
Secondary DNS Server: 0.0.0.0

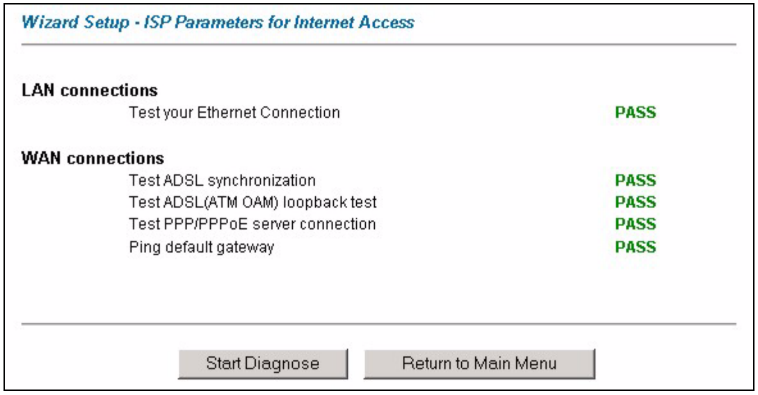
The following table describes the fields in this screen.

Table 10 Internet Access Wizard Setup: LAN Configuration

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

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

Figure 13 Internet Access Wizard Setup: Connection Tests



Wizard Setup - ISP Parameters for Internet Access

LAN connections

Test your Ethernet Connection PASS

WAN connections

Test ADSL synchronization PASS

Test ADSL(ATM OAM) loopback test PASS

Test PPP/PPPoE server connection PASS

Ping default gateway PASS

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

4

Media Bandwidth Management Wizard

4.1 Introduction

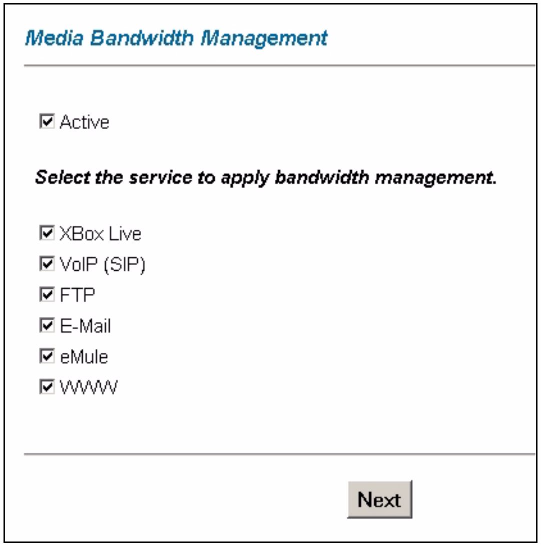
Bandwidth management allows you to allocate priority to different kinds of traffic on your network to ensure the smoother flow of network traffic. For example, you can allocate a high priority to XBox Live traffic. Use the Media Bandwidth Management (MBM) Wizard screens to configure bandwidth management on your ZyXEL Device.

See Chapter 17 on page 165 for background information on Media Bandwidth Management.

4.1.1 Media Bandwidth Management Wizard

1 In the **SITE MAP** screen click **Media Bandwidth Management Wizard** to display the first wizard screen.

Figure 14 MBM Wizard: Media Bandwidth Management



Media Bandwidth Management

☑ Active

Select the service to apply bandwidth management.

☑ XBox Live
☑ VoIP (SIP)
☑ FTP
☑ E-Mail
☑ eMule
☑ WWW

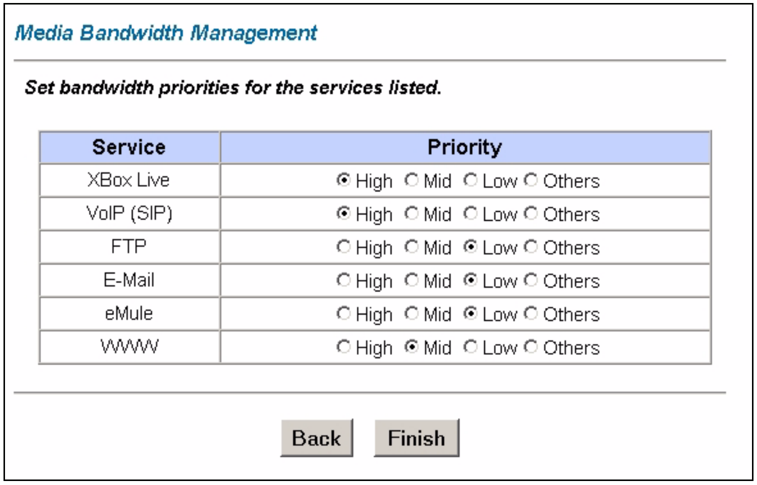
The following table describes the fields in this screen.

Table 11 MBM Wizard: Media Bandwidth Management

LABEL	DESCRIPTION
Active	Select **Active** to enable the Media Bandwidth Management feature on your ZyXEL Device.
Select the service to apply bandwidth management	Select the traffic type(s) to which you want to allocate priority. You can select the following: **XBox Live** - a game playing device used for gaming on the Internet, as well as playing media files such as videos. **VoIP (SIP)** - Voice over IP, this allows you to make calls over the Internet using a SIP server. **FTP** - File Transfer Protocol, a service used for downloading files. **E-Mail** - the email application used on your computer, rather than web-based email. **eMule** - a file-sharing application **WWW** - the World Wide Web If you do not use a service, it is not necessary to set a priority for that service.
Next	Click **Next** to continue with the Wizard.

2 Configure levels of priority for the services you have selected in the next screen.

Figure 15 MBM Wizard: Media Bandwidth Management



Media Bandwidth Management

Set bandwidth priorities for the services listed.

Service	Priority
XBox Live	● High ○ Mid ○ Low ○ Others
VoIP (SIP)	● High ○ Mid ○ Low ○ Others
FTP	○ High ○ Mid ● Low ○ Others
E-Mail	○ High ○ Mid ● Low ○ Others
eMule	○ High ○ Mid ● Low ○ Others
WWW	○ High ● Mid ○ Low ○ Others

The following table describes the fields in this screen.

Table 12 MBM Wizard: Media Bandwidth Management

LABEL	DESCRIPTION
Service	This field lists the services selected in the previous screen
Priority	Select a priority level for each service you have specified in the previous screen. The options are **High**, **Mid**, **Low** and **Others**. Give voice and video applications a high priority, as quality is affected by transmission delays. **VoIP** is a voice service and **XBox Live** is a video service, so they should receive a high priority. Give Internet browsing a medium level priority as quality is not noticeably affected by brief delays. Give data transfer services such as **eMule**, **FTP** or **E-Mail** a low priority as quality is not affected by delays in transmission. Select **Others** for applications to which you do not want to apply QoS.
Back	Click **Back** to return to the previous screen.
Finish	Click **Finish** to save your settings and return to the main menu.

PART III
Advanced Setup

5

LAN Setup

This chapter describes how to configure LAN settings.

5.1 LAN Overview

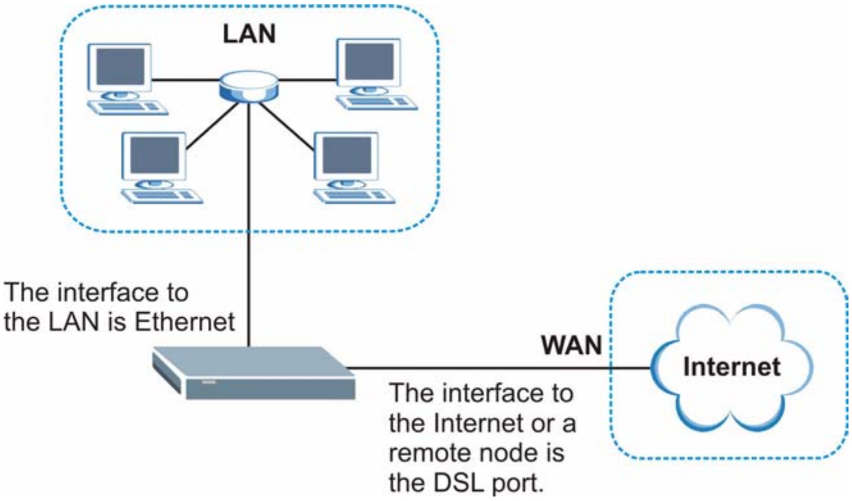
A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

See Section 5.3 on page 60 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 16 LAN and WAN IP Addresses


LAN
The interface to the LAN is Ethernet
WAN
Internet
The interface to the Internet or a remote node is the DSL port.

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

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.

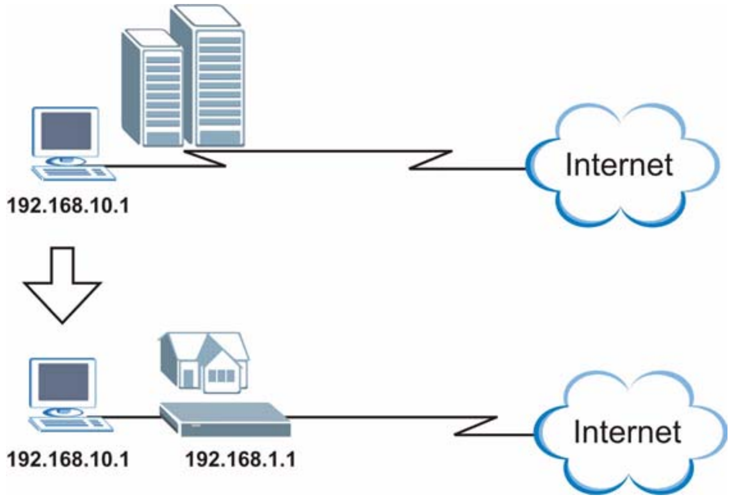
5.2.4 Any IP

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 17 Any IP Example



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

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

5.2.4.1 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.

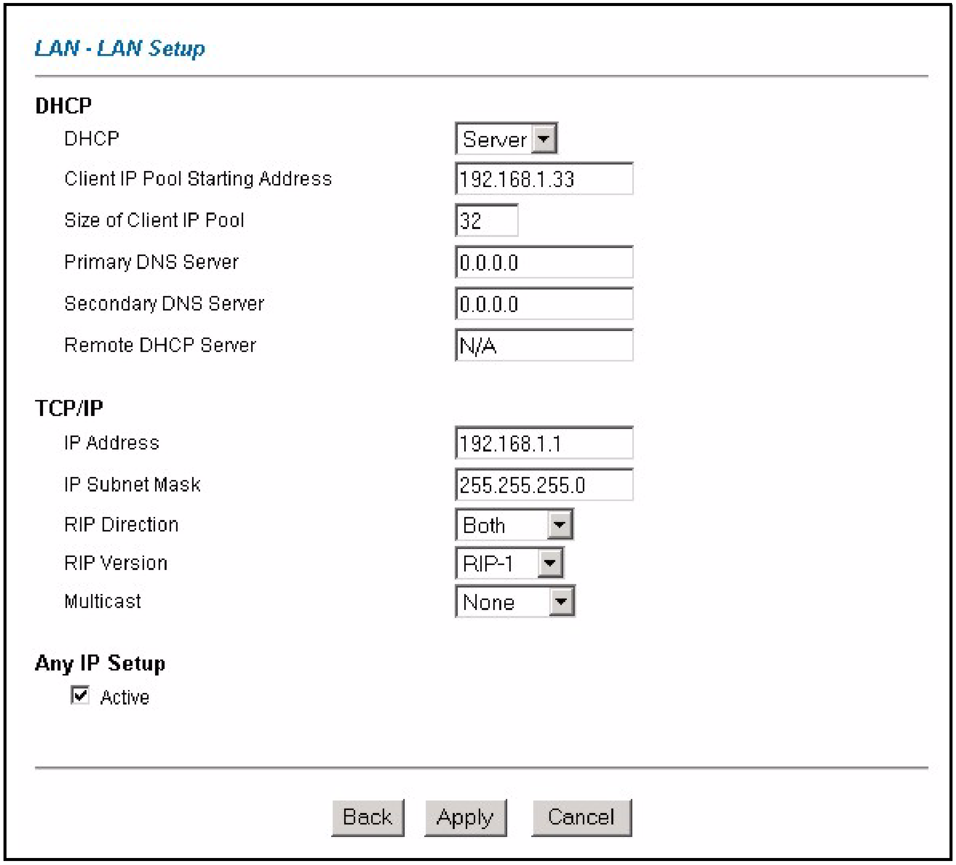
1. When a computer (which is in a different subnet) first attempts to access the Internet, it sends packets to its default gateway (which is not the ZyXEL Device) by looking at the MAC address in its ARP table.
2. When the computer cannot locate the default gateway, an ARP request is broadcast on the 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

Click **LAN** > LAN Setup to open the **LAN Setup** screen. See Section 5.1 on page 55 for background information.

Figure 18 LAN Setup



LAN - LAN Setup

DHCP

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

TCP/IP

IP Address	192.168.1.1
IP Subnet Mask	255.255.255.0
RIP Direction	Both
RIP Version	RIP-1
Multicast	None

Any IP Setup

☑ Active

The following table describes the fields in this screen.

Table 13 LAN Setup

LABEL	DESCRIPTION
DHCP	
DHCP	If set to **Server**, your ZyXEL Device can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client. If set to **None**, the DHCP server will be disabled. If set to **Relay**, the ZyXEL Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the **Remote DHCP Server** field in this case. When DHCP is used, the following items need to be set:
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	This field specifies the size or count of the IP address pool.
Primary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Secondary DNS Server	As above.
Remote DHCP Server	If **Relay** is selected in the **DHCP** field above then enter the IP address of the actual remote DHCP server here.
TCP/IP	

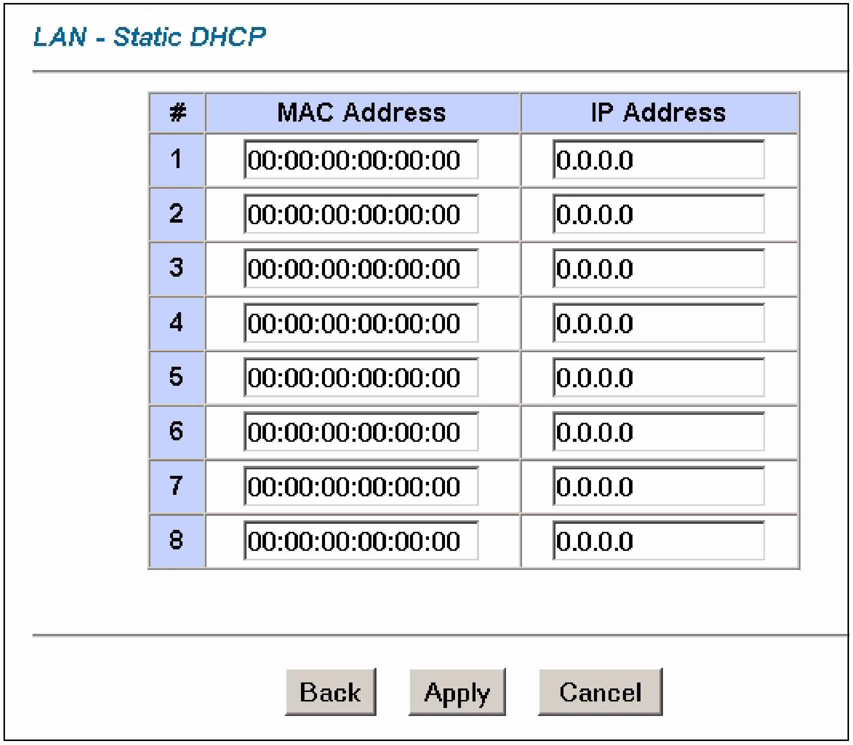
Table 13 LAN Setup (continued)

LABEL	DESCRIPTION
IP Address	Enter the IP address of your ZyXEL Device in dotted decimal notation, for example, 192.168.1.1 (factory default).
IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
RIP Direction	Select the RIP direction from **None**, **Both**, **In Only** and **Out Only**.
RIP Version	Select the RIP version from **RIP-1**, **RIP-2B** and **RIP-2M**.
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 (**IGMP-v1**) and **IGMP-v2**. Select **None** to disable it.
Any IP Setup	Select the **Active** 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.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

5.4 Configuring Static DHCP

Click **LAN** > **Static DHCP** to open the **Static DHCP** screen. See Section 5.1.2 on page 56 for background information.

Figure 19 LAN > Static DHCP



#	MAC Address	IP Address
1	00:00:00:00:00:00	0.0.0.0
2	00:00:00:00:00:00	0.0.0.0
3	00:00:00:00:00:00	0.0.0.0
4	00:00:00:00:00:00	0.0.0.0
5	00:00:00:00:00:00	0.0.0.0
6	00:00:00:00:00:00	0.0.0.0
7	00:00:00:00:00:00	0.0.0.0
8	00:00:00:00:00:00	0.0.0.0

The following table describes the fields in this screen.

Table 14 LAN Setup

LABEL	DESCRIPTION
#	This is the index number for the entries in this table.
MAC Address	Type the MAC address of the device for which you are configuring the IP address. Use hexadecimal characters in the following format: "0A:A0:00:BB:CC:DD"
IP Address	Type the IP address for the device you are configuring in dotted decimal notation, for example, "150.222.0.1".
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

6

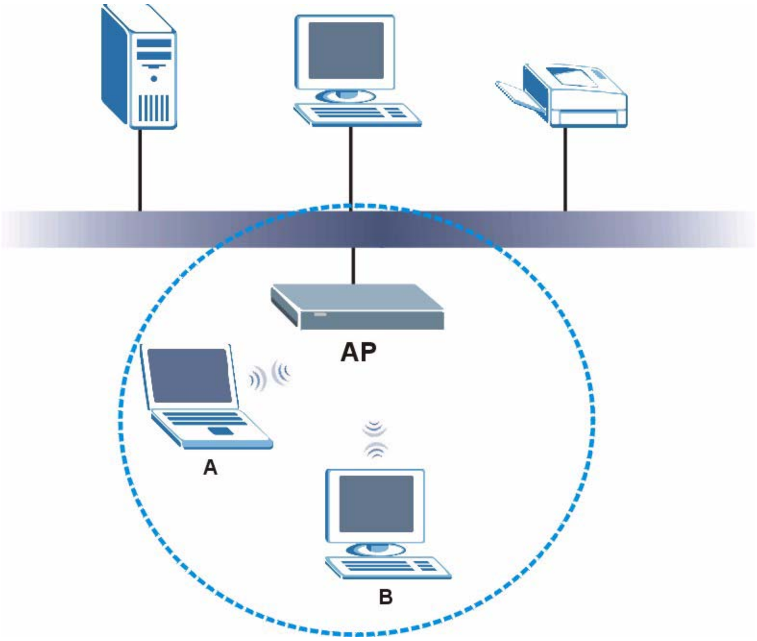
Wireless LAN

This chapter discusses how to configure the wireless network settings in your ZyXEL Device. See the appendices for more detailed information about wireless networks.

6.1 Wireless Network Overview

The following figure provides an example of a wireless network.

Figure 20 Example of a Wireless Network



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

Every wireless network must follow these basic guidelines.

- Every wireless client in the same wireless network must use the same SSID.
  The SSID is the name of the wireless network. It stands for Service Set IDentity.
- If two wireless networks overlap, they should use different channels.
  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.

- Every wireless client in the same wireless network must use security compatible with the AP.

  Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

6.2 Wireless Security Overview

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

6.2.1 SSID

Normally, the AP acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the AP does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized devices to get the SSID. In addition, unauthorized devices can still see the information that is sent in the wireless network.

6.2.2 MAC Address Filter

Every wireless client has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each wireless client, see the appropriate User's Guide or other documentation.

You can use the MAC address filter to tell the AP which wireless clients are allowed or not allowed to use the wireless network. If a wireless client is allowed to use the wireless network, it still has to have the correct settings (SSID, channel, and security). If a wireless client is not allowed to use the wireless network, it does not matter if it has the correct settings.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized devices to get the MAC address of an authorized wireless client. Then, they can use that MAC address to use the wireless network.

6.2.3 User Authentication

You can make every user log in to the wireless network before they can use it. This is called user authentication. However, every wireless client in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, there are two typical places to store the user names and passwords for each user.

- In the AP: this feature is called a local user database or a local database.
- In a RADIUS server: this is a server used in businesses more than in homes.

[1] Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.

[2] Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

If your AP does not provide a local user database and if you do not have a RADIUS server, you cannot set up user names and passwords for your users.

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

Local user databases also have an additional limitation that is explained in the next section.

6.2.4 Encryption

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

The types of encryption you can choose depend on the type of user authentication. (See Section 6.2.3 on page 66 for information about this.)

Table 15 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest	No Security	WPA
↕	Static WEP	
	WPA-PSK	
Strongest	WPA2-PSK	WPA2

For example, if the wireless network has a RADIUS server, you can choose **WPA** or **WPA2**. If users do not have to log in with a user name and password in order to access the wireless network, you can choose no encryption, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every wireless client in the wireless network supports. For example, suppose the AP does not have a local user database, and you do not have a RADIUS server. Therefore, there is no user authentication. Suppose the wireless network has two wireless clients. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.

It is recommended that wireless networks use **WPA-PSK**, **WPA**, or stronger encryption. IEEE 802.1x and WEP encryption are better than none at all, but it is still possible for unauthorized devices to figure out the original information pretty quickly.

It is not possible to use **WPA-PSK**, **WPA** or stronger encryption with a local user database. In this case, it is better to set up stronger encryption with no authentication than to set up weaker encryption with the local user database.

When you select **WPA2** or **WPA2-PSK** in your ZyXEL Device, you can also select an option (**WPA Compatible**) to support WPA as well. In this case, if some wireless clients support WPA and some support WPA2, you should set up **WPA2-PSK** or **WPA2** (depending on the type of wireless network login) and select the **WPA Compatible** option in the ZyXEL Device.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every wireless client in the wireless network must have the same key.

6.3 Additional Wireless Terms

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

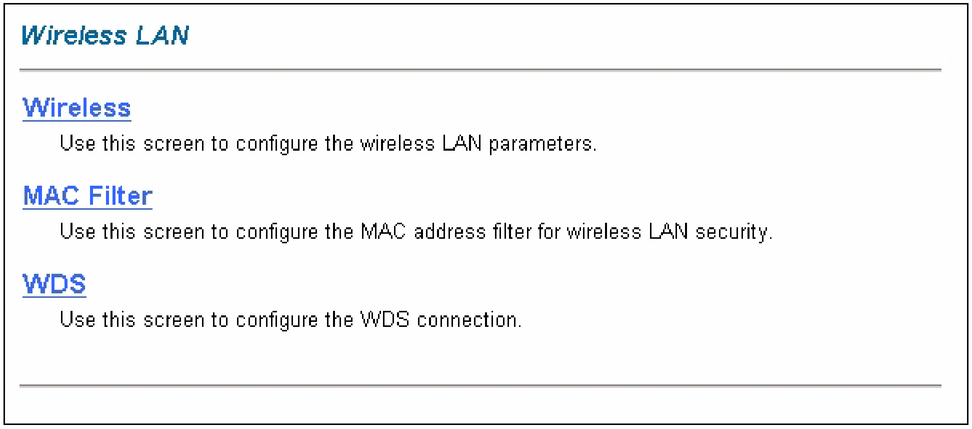
Table 16 Additional Wireless Terms

TERM	DESCRIPTION
Intra-BSS Traffic	This describes direct communication (not through the ZyXEL Device) between two wireless devices within a wireless network. You might disable this kind of communication to enhance security within your wireless network.
RTS/CTS Threshold	In a wireless network which covers a large area, wireless devices are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through. By setting this value lower than the default value, the wireless devices must sometimes get permission to send information to the ZyXEL Device. The lower the value, the more often the devices must get permission. If this value is greater than the fragmentation threshold value (see below), then wireless devices never have to get permission to send information to the ZyXEL Device.
Preamble	A preamble affects the timing in your wireless network. There are two preamble modes: long and short. If a device uses a different preamble mode than the ZyXEL Device does, it cannot communicate with the ZyXEL Device.
Authentication	The process of verifying whether a wireless device is allowed to use the wireless network.
Max. Frame Burst	Enable this to improve the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. Maximum Frame Burst sets the maximum time that the ZyXEL Device transmits IEEE 802.11g wireless traffic only.
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.
Roaming	If you have two or more ZyXEL Devices (or other wireless access points) on your wireless network, you can enable this option so that wireless devices can change locations without having to log in again. This is useful for devices, such as notebooks, that move around a lot.

6.4 The Main Wireless LAN Screen

Click **Wireless LAN** in the navigation panel to display the main **Wireless LAN** screen.

Figure 21 Wireless LAN



Wireless LAN

Wireless

Use this screen to configure the wireless LAN parameters.

MAC Filter

Use this screen to configure the MAC address filter for wireless LAN security.

WDS

Use this screen to configure the WDS connection.

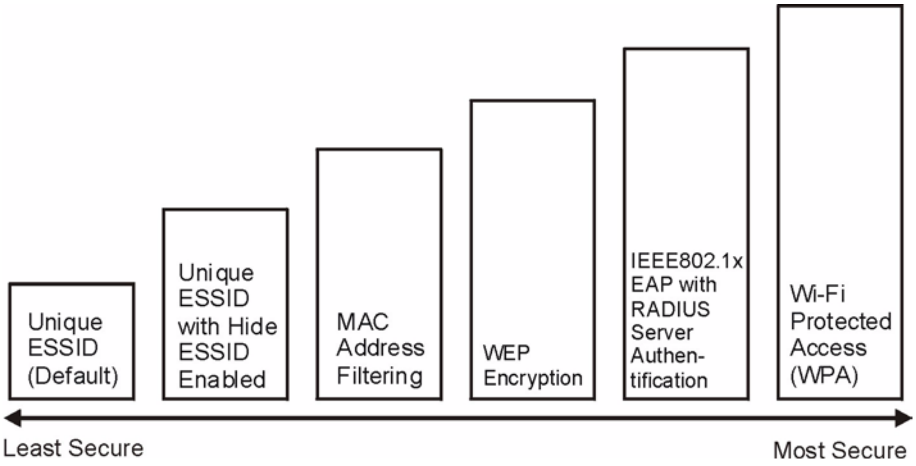
The following table describes the links in this screen.

Table 17 Wireless LAN

LINK	DESCRIPTION
Wireless	Click this link to go to a screen where you can configure wireless settings.
MAC Filter	Click this link to go to a screen where you can restrict access to your wireless network by MAC address.
WDS	Click this link to go to a screen where you can set up a WDS (Wireless Distribution System) connection between your AP's (access points).

The following figure shows the relative effectiveness of these wireless security methods available on your ZyXEL Device.

Figure 22 Wireless Security Methods


Unique ESSID (Default)
Unique ESSID with Hide ESSID Enabled
MAC Address Filtering
WEP Encryption
IEEE802.1x EAP with RADIUS Server Authen- tification
Wi-Fi Protected Access (WPA)
Least Secure
Most Secure

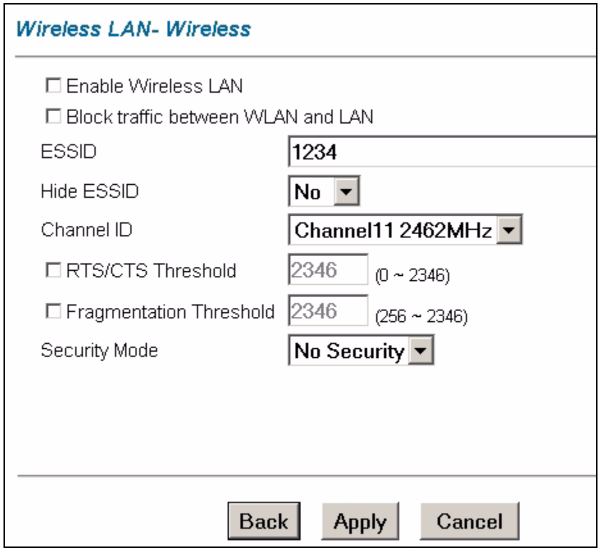
You must enable the same wireless security settings on the ZyXEL Device and on all wireless clients that you want to associate with it.

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

6.5 Configuring the Wireless Screen

Click **Advanced Setup** > **Wireless LAN** to open the **Wireless LAN** screen.

Figure 23 Network > Wireless LAN



Wireless LAN- Wireless

□ Enable Wireless LAN

□ Block traffic between WLAN and LAN

ESSID: 1234

Hide ESSID: No

Channel ID: Channel11 2462MHz

□ RTS/CTS Threshold: 2346 (0 ~ 2346)

□ Fragmentation Threshold: 2346 (256 ~ 2346)

Security Mode: No Security

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

Table 18 Network > Wireless LAN > General

LABEL	DESCRIPTION
Enable Wireless LAN	Click the check box to activate the wireless feature on your ZyXEL Device.
Block Traffic between WLAN and LAN	
ESSID	The **ESSID** (Extended Service Set IDentity) identifies your wireless network. Enter a descriptive name (up to 32 printable characters including spaces; alphabetic characters are case-sensitive) for the wireless LAN.
Hide ESSID	Select **Yes** to hide the **ESSID** from unauthorized individuals scanning for ESSIDs using a site survey tool or select **No**.to make it visible to wireless devices in range.
Channel ID	The range of radio frequencies used by wireless devices is called a channel. Select a wireless channel if interference from other nearby devices is a problem. The ZyXEL Device and other wireless devices in your wireless network must use the same channel.

Table 18 Network > Wireless LAN > General

LABEL	DESCRIPTION
RTS/CTS Threshold	The RTS (Request To Send) threshold (number of bytes) is for enabling RTS/CTS. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this value to be larger than the maximum MSDU (MAC service data unit) size turns off RTS/CTS. Setting this value to zero turns on RTS/CTS. Select the check box to change the default value and enter a new value between 0 and 2432.
Fragmentation Threshold	This is the threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Select the check box to change the default value and enter a value between 256 and 2432.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to reload the previous configuration for this screen.

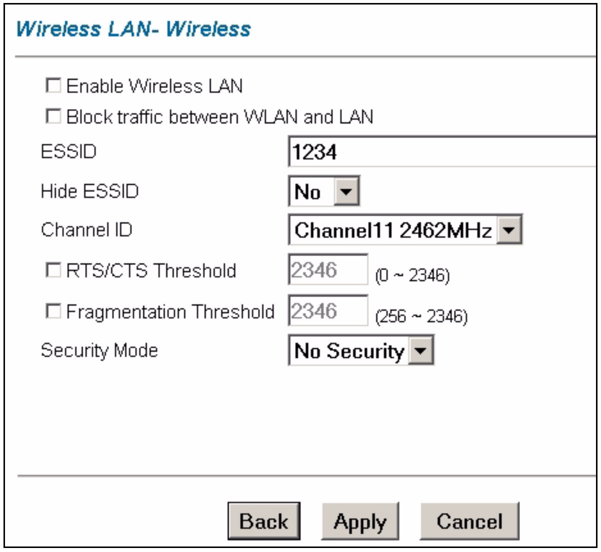
See the rest of this chapter for information on the other labels in this screen.

6.5.1 No Security

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

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

Figure 24 Network > Wireless LAN: No Security



Wireless LAN- Wireless

□ Enable Wireless LAN
□ Block traffic between WLAN and LAN

ESSID	1234
Hide ESSID	No
Channel ID	Channel11 2462MHz
□ RTS/CTS Threshold	2346 (0 ~ 2346)
□ Fragmentation Threshold	2346 (256 ~ 2346)
Security Mode	No Security

The following table describes the labels in this screen.

Table 19 Wireless No Security

LABEL	DESCRIPTION
Security Mode	Choose **No Security** from the drop-down list box.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to reload the previous configuration for this screen.

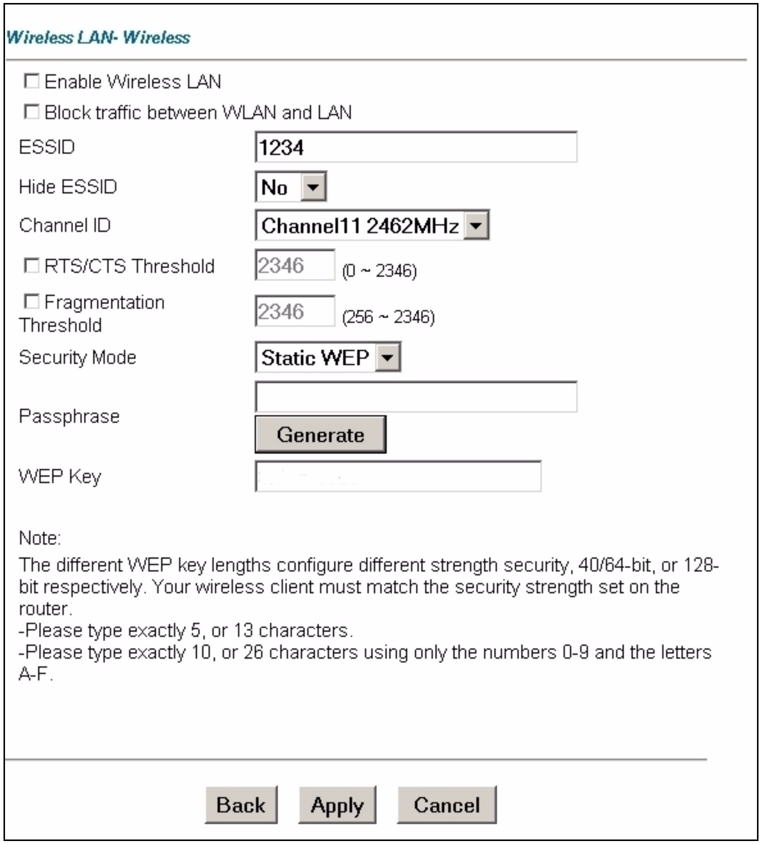
6.5.2 WEP Encryption

WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the access points must use the same WEP key.

Your ZyXEL Device allows you to configure up to four 64-bit, 128-bit or 256-bit WEP keys but only one key can be enabled at any one time.

In order to configure and enable WEP encryption; click **Wireless LAN** and **Wireless** to the display the **Wireless** screen.

Figure 25 Wireless Screen



Wireless LAN- Wireless

☐ Enable Wireless LAN

☐ Block traffic between WLAN and LAN

ESSID	1234
Hide ESSID	No
Channel ID	Channel11 2462MHz
☐ RTS/CTS Threshold	2346 (0 ~ 2346)
☐ Fragmentation Threshold	2346 (256 ~ 2346)
Security Mode	Static WEP
Passphrase	
WEP Key	

Note:
The different WEP key lengths configure different strength security, 40/64-bit, or 128-bit respectively. Your wireless client must match the security strength set on the router.
-Please type exactly 5, or 13 characters.
-Please type exactly 10, or 26 characters using only the numbers 0-9 and the letters A-F.

The following table describes the labels in this screen.

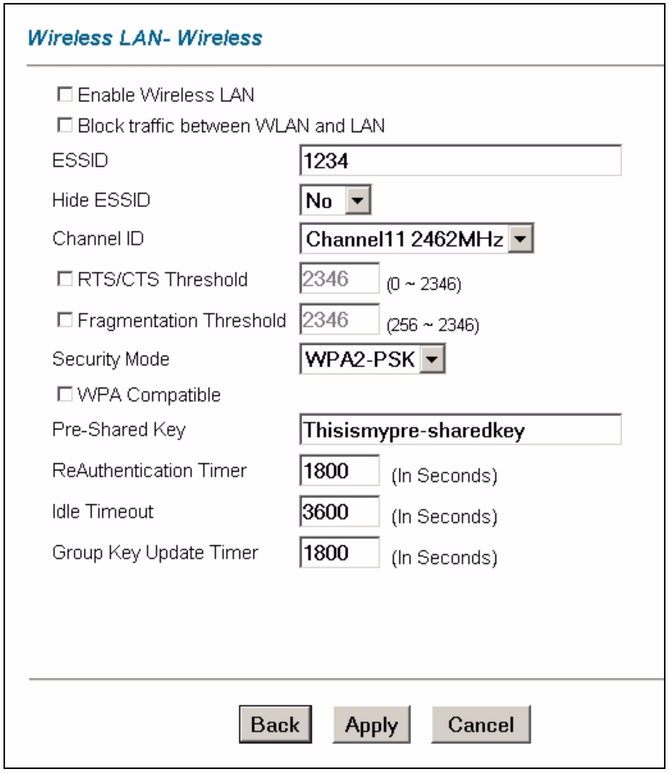
Table 20 Wireless LAN

LABEL	DESCRIPTION
Security Mode	Select **Static WEP** from the drop-down list.
You won't see the following WEP-related fields if you have **WPA** or **WPA-PSK** enabled.	
Passphrase	Enter a "passphrase" (password phrase) of up to 63 case-sensitive printable characters and click **Generate** to have the ZyXEL Device create four different WEP keys. At the time of writing, you cannot use passphrase to generate 256-bit WEP keys.
Generate	After you enter the passphrase, click **Generate** to have the ZyXEL Device generate a WEP key automatically. The key displays in the **WEP Key** field.
WEP Key	The **WEP Key** is used to encrypt data. Both the ZyXEL Device and other wireless devices on your network must use the same WEP key. If you want to manually set the WEP keys, type the key in this field. The length of the key corresponds to the security strength. For 64-bit security, type 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). For 128-bit security, type13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").
Back	Click **Back** to go to the main wireless LAN setup screen.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

6.5.3 WPA-PSK/WPA2-PSK

Click **Advanced Setup** > **Wireless LAN** to display the **Wireless LAN** screen. Select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 26 Network > Wireless LAN: WPA-PSK/



Wireless LAN- Wireless

□ Enable Wireless LAN

□ Block traffic between WLAN and LAN

ESSID: 1234

Hide ESSID: No

Channel ID: Channel11 2462MHz

□ RTS/CTS Threshold: 2346 (0 ~ 2346)

□ Fragmentation Threshold: 2346 (256 ~ 2346)

Security Mode: WPA2-PSK

□ WPA Compatible

Pre-Shared Key: Thisismypre-sharedkey

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

Group Key Update Timer: 1800 (In Seconds)

The following table describes the labels in this screen.

Table 21 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
Security Mode	Select **WPA-PSK** or **WPA2-PSK** from the drop-down box.
WPA Compatible	This check box is available only when you select **WPA2-PSK** or **WPA2** in the **Security Mode** field. Select the check box to have both WPA2 and WPA wireless clients be able to communicate with the ZyXEL Device even when the ZyXEL Device is using WPA2-PSK or WPA2.
Pre-Shared Key	The encryption mechanisms used for **WPA/WPA2** and **WPA-PSK/WPA2-PSK** are the same. The only difference between the two is that **WPA-PSK/WPA2-PSK** uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
ReAuthentication Timer (in seconds)	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes). Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).

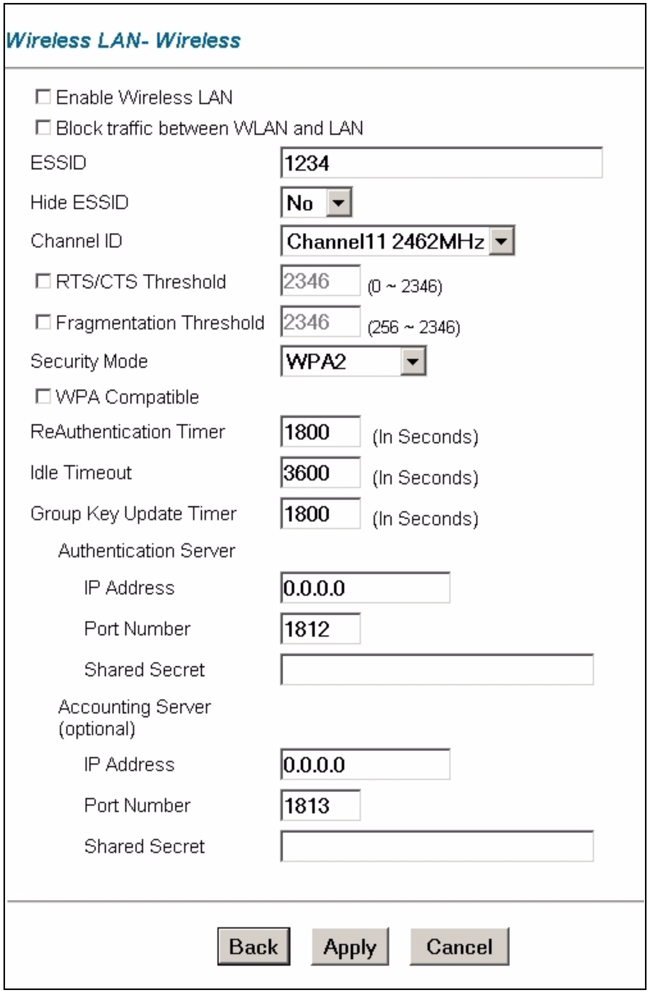
Table 21 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP (if using **WPA-PSK/ WPA2-PSK** key management) or RADIUS server (if using **WPA/WPA2** key management) sends a new group key out to all clients. The re-keying process is the WPA/WPA2 equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in **WPA-PSK/WPA2-PSK** mode. The default is **1800** seconds (30 minutes).
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Reset	Click **Reset** to reload the previous configuration for this screen.

6.5.4 WPA/WPA2

Click **Advanced Setup** > **Wireless LAN** to display the **Wireless LAN** screen. Select **WPA** or **WPA2** from the **Security Mode** list.

Figure 27 Network > Wireless LAN > General: WPA/WPA2



Wireless LAN- Wireless

☐ Enable Wireless LAN
☐ Block traffic between WLAN and LAN

ESSID	1234	
Hide ESSID	No	
Channel ID	Channel11 2462MHz	
☐ RTS/CTS Threshold	2346	(0 ~ 2346)
☐ Fragmentation Threshold	2346	(256 ~ 2346)
Security Mode	WPA2	
☐ WPA Compatible		
ReAuthentication Timer	1800	(In Seconds)
Idle Timeout	3600	(In Seconds)
Group Key Update Timer	1800	(In Seconds)
Authentication Server		
IP Address	0.0.0.0	
Port Number	1812	
Shared Secret		
Accounting Server (optional)		
IP Address	0.0.0.0	
Port Number	1813	
Shared Secret		

The following table describes the labels in this screen.

Table 22 Network > Wireless LAN > General: WPA/WPA2

LABEL	DESCRIPTION
WPA Compatible	This check box is available only when you select **WPA2-PSK** or **WPA2** in the **Security Mode** field. Select the check box to have both WPA2 and WPA wireless clients be able to communicate with the ZyXEL Device even when the ZyXEL Device is using WPA2-PSK or WPA2.
ReAuthentication Timer	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes). Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP (if using **WPA-PSK/ WPA2-PSK** key management) or RADIUS server (if using **WPA/WPA2** key management) sends a new group key out to all clients. The re-keying process is the WPA/WPA2 equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in **WPA-PSK/WPA2-PSK** mode. The ZyXEL Device default is **1800** seconds (30 minutes).
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the ZyXEL Device. The key must be the same on the external authentication server and your ZyXEL Device. The key is not sent over the network.
Accounting Server	
Active	Select **Yes** from the drop down list box to enable user accounting through an external authentication server.
IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	Enter the port number of the external accounting server. The default port number is **1813**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the ZyXEL Device. The key must be the same on the external accounting server and your ZyXEL Device. The key is not sent over the network.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Reset	Click **Reset** to reload the previous configuration for this screen.

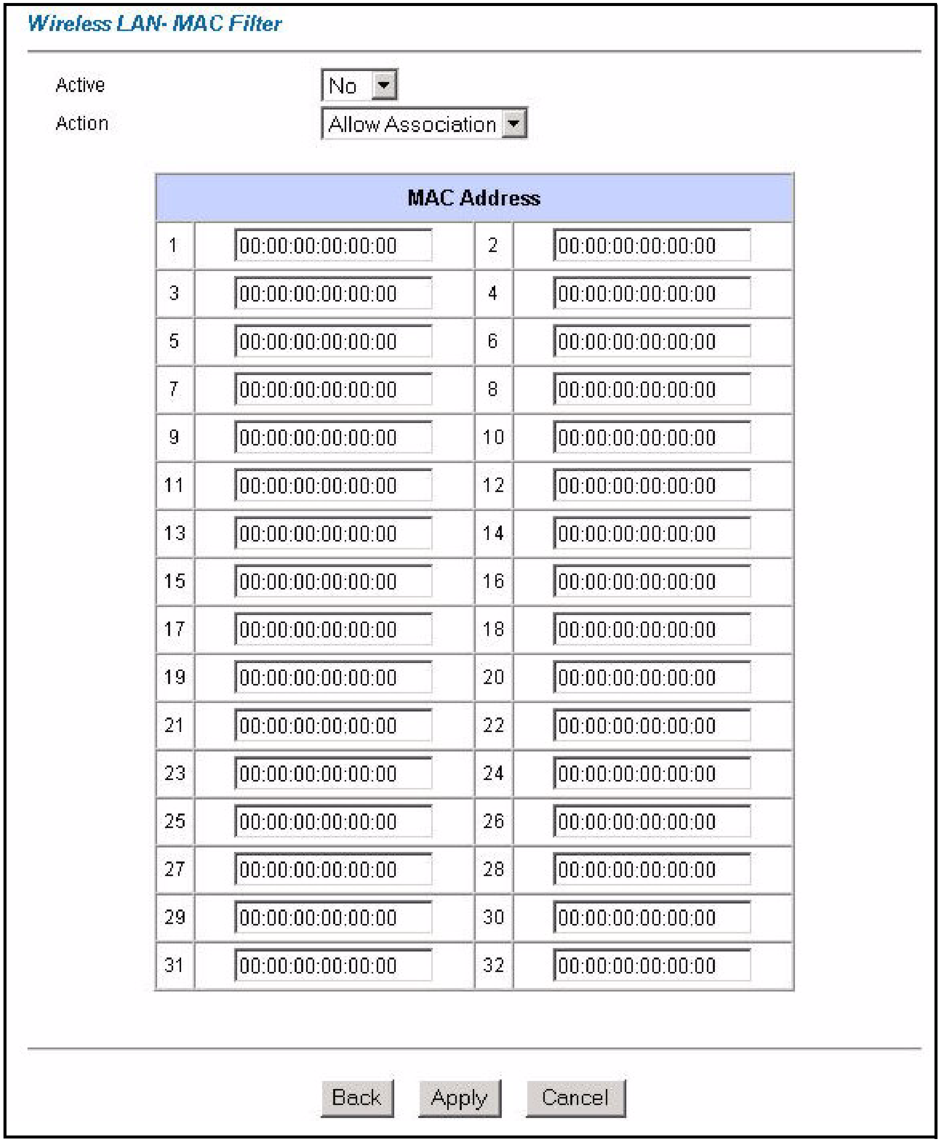
If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's ESSID or security settings (see Figure 22 on page 69), you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the ZyXEL Device's new settings.

6.6 Configuring MAC Filters

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the devices to configure this screen. To change your ZyXEL Device's MAC filter settings, click **Advanced Setup** > **Wireless LAN** > **MAC Filter** to open the **MAC Filter** screen. The screen appears as shown.

Be careful not to list your computer's MAC address and set the **Action** field to **Deny Association** when managing the ZyXEL Device via a wireless connection. This would lock you out.

Figure 28 MAC Filter



Wireless LAN- MAC Filter

Active: No

Action: Allow Association

MAC Address			
1	00:00:00:00:00:00	2	00:00:00:00:00:00
3	00:00:00:00:00:00	4	00:00:00:00:00:00
5	00:00:00:00:00:00	6	00:00:00:00:00:00
7	00:00:00:00:00:00	8	00:00:00:00:00:00
9	00:00:00:00:00:00	10	00:00:00:00:00:00
11	00:00:00:00:00:00	12	00:00:00:00:00:00
13	00:00:00:00:00:00	14	00:00:00:00:00:00
15	00:00:00:00:00:00	16	00:00:00:00:00:00
17	00:00:00:00:00:00	18	00:00:00:00:00:00
19	00:00:00:00:00:00	20	00:00:00:00:00:00
21	00:00:00:00:00:00	22	00:00:00:00:00:00
23	00:00:00:00:00:00	24	00:00:00:00:00:00
25	00:00:00:00:00:00	26	00:00:00:00:00:00
27	00:00:00:00:00:00	28	00:00:00:00:00:00
29	00:00:00:00:00:00	30	00:00:00:00:00:00
31	00:00:00:00:00:00	32	00:00:00:00:00:00

The following table describes the fields in this menu.

Table 23 MAC Filter

LABEL	DESCRIPTION
Active	Select **Yes** from the drop down list box to enable MAC address filtering.
Action	Define the filter action for the list of MAC addresses in the **MAC Address** table. Select **Deny Association** to block access to the router, MAC addresses not listed will be allowed to access the ZyXEL Device. Select **Allow Association** to permit access to the router, MAC addresses not listed will be denied access to the ZyXEL Device.
MAC Address	Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc of the wireless stations that are allowed or denied access to the ZyXEL Device in these address fields.
Back	Click **Back** to go to the main wireless LAN setup screen.

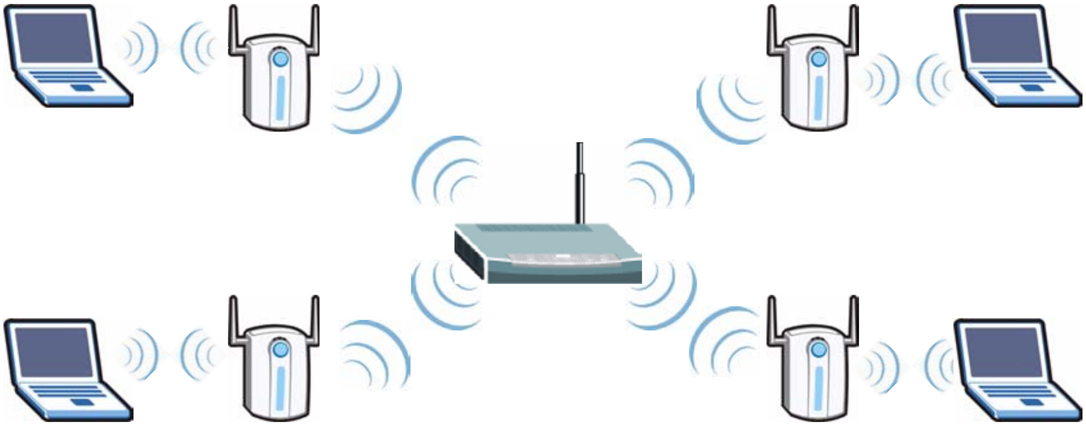
Table 23 MAC Filter (continued)

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

6.7 WDS Screen

The WDS (Wireless Distribution System) allows you to configure the ZyXEL Device to connect to two or more APs via wireless when WDS is enabled. An AP using WDS can function as a wireless network bridge allowing you to wirelessly connect two wired network segments.

Figure 29 Connecting Wireless Networks Using WDS

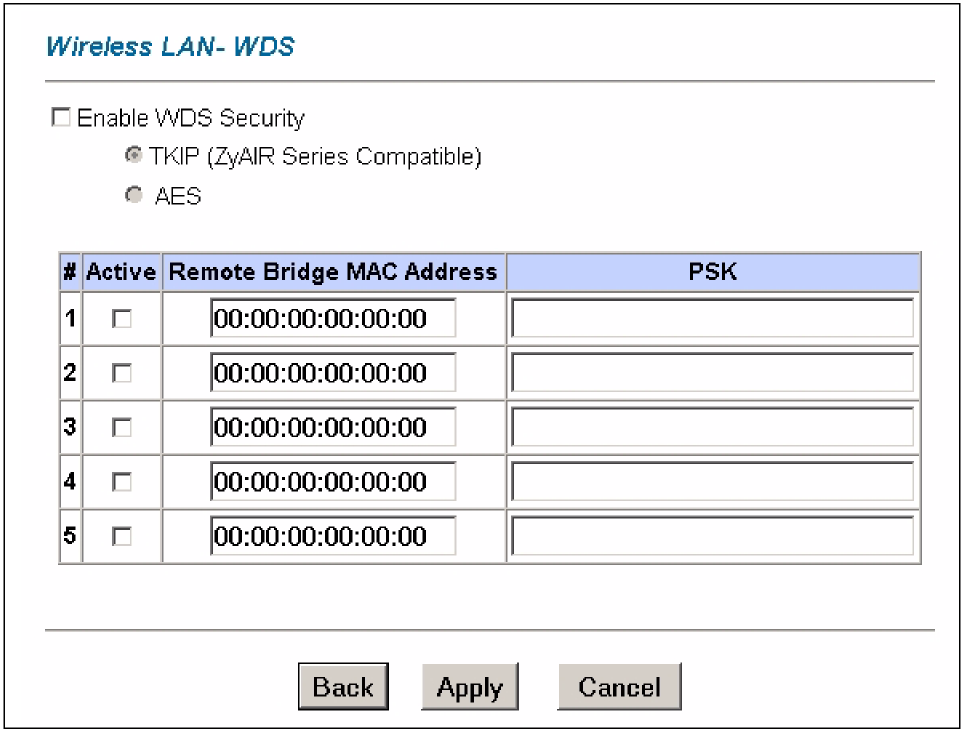


Use this screen to set up WDS between your ZyXEL Device and another AP.

WDS security is independent of the security settings between the ZyXEL Device and any wireless clients.

At the time of writing, WDS is compatible with other ZyXEL APs only. Not all models support WDS links. Check your other AP's documentation.

Figure 30 Advanced Setup > Wireless LAN > WDS



Wireless LAN- WDS

□ Enable WDS Security

● TKIP (ZyAIR Series Compatible)

○ AES

#	Active	Remote Bridge MAC Address	PSK
1	□	00:00:00:00:00:00	
2	□	00:00:00:00:00:00	
3	□	00:00:00:00:00:00	
4	□	00:00:00:00:00:00	
5	□	00:00:00:00:00:00	

The following table describes the labels in this screen.

Table 24 Advanced Setup > Wireless LAN > WDS

LABEL	DESCRIPTION
Enable WDS Security	Select this to set up security on your ZyXEL Device’s bridged connection with an AP. Select **AES** (Advanced Encryption Standard) as your security method if the AP’s on your network support it. Otherwise select **TKIP Security (ZyAIR Series Compatible)** (Temporal Key Integrity Protocol). If you de-select this option, the data sent between APs is not encrypted. Anyone can read it.
#	This is the index number of the access point (AP) with which you are setting up a WDS connection.
Active	Select this to enable a WDS connection with this AP.
Remote Bridge MAC Address	Type the MAC address of the AP with which you are setting up a WDS connection in a valid MAC address format (six hexadecimal character pairs, for example 12:34:56:78:9a:bc)..
PSK	Type a PSK (Pre-Shared Key) in this field between 8~63 characters long (A~Z, a~z,0~9).
Back	Click **Back** to return to the **Wireless LAN** menu screen.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to cancel your changes.

7

WAN Setup

This chapter describes how to configure WAN settings.

7.1 WAN Overview

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

7.1.1 Encapsulation

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

7.1.1.1 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.

7.1.1.2 PPP over Ethernet

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

7.1.1.3 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.

7.1.1.4 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.

7.1.2 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.

7.1.2.1 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.

7.1.2.2 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.

7.1.3 VPI and VCI

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

7.1.4 IP Address Assignment

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

7.1.4.1 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.

7.1.4.2 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.

7.1.4.3 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.

7.1.5 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.

7.1.6 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.

7.2 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 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 7.7 on page 86)
- Traffic-redirect route (see Section 7.8 on page 90)
- WAN-backup route, also called dial-backup (see Section 7.9 on page 90)

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.

7.3 PPPoE Encapsulation

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

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example Radius). PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new learning or procedures for Windows users.

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.

7.4 Traffic Shaping

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

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

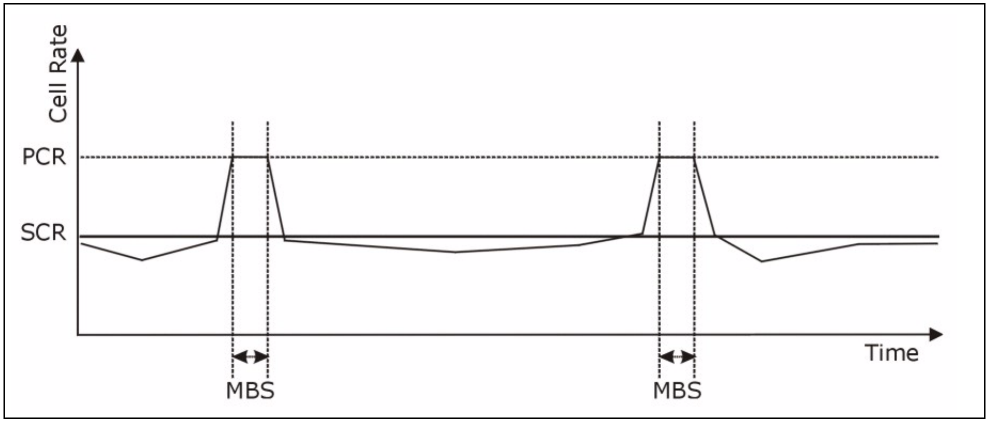
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

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

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

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

Figure 31 Example of Traffic Shaping



7.5 Zero Configuration Internet Access

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

Zero configuration for Internet access is disabled when

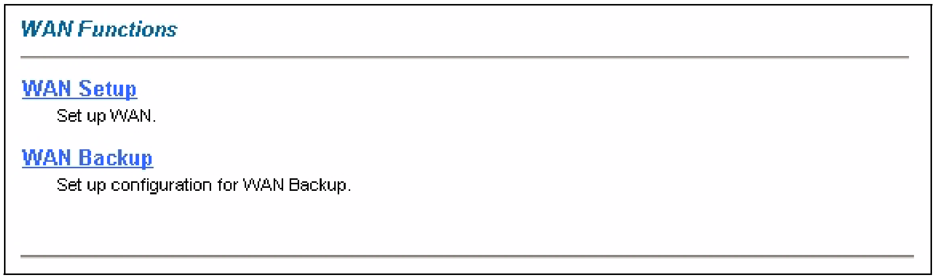
- the ZyXEL Device is in bridge mode
- you set the ZyXEL Device to use a static (fixed) WAN IP address.

7.6 The Main WAN Screen

Click **WAN** in the navigation panel to display the man **WAN** screen.

See Section 7.1 on page 81 for more information.

Figure 32 WAN



WAN Functions

WAN Setup

Set up WAN.

WAN Backup

Set up configuration for WAN Backup.

The following table describes the links in this screen.

Table 25 WAN

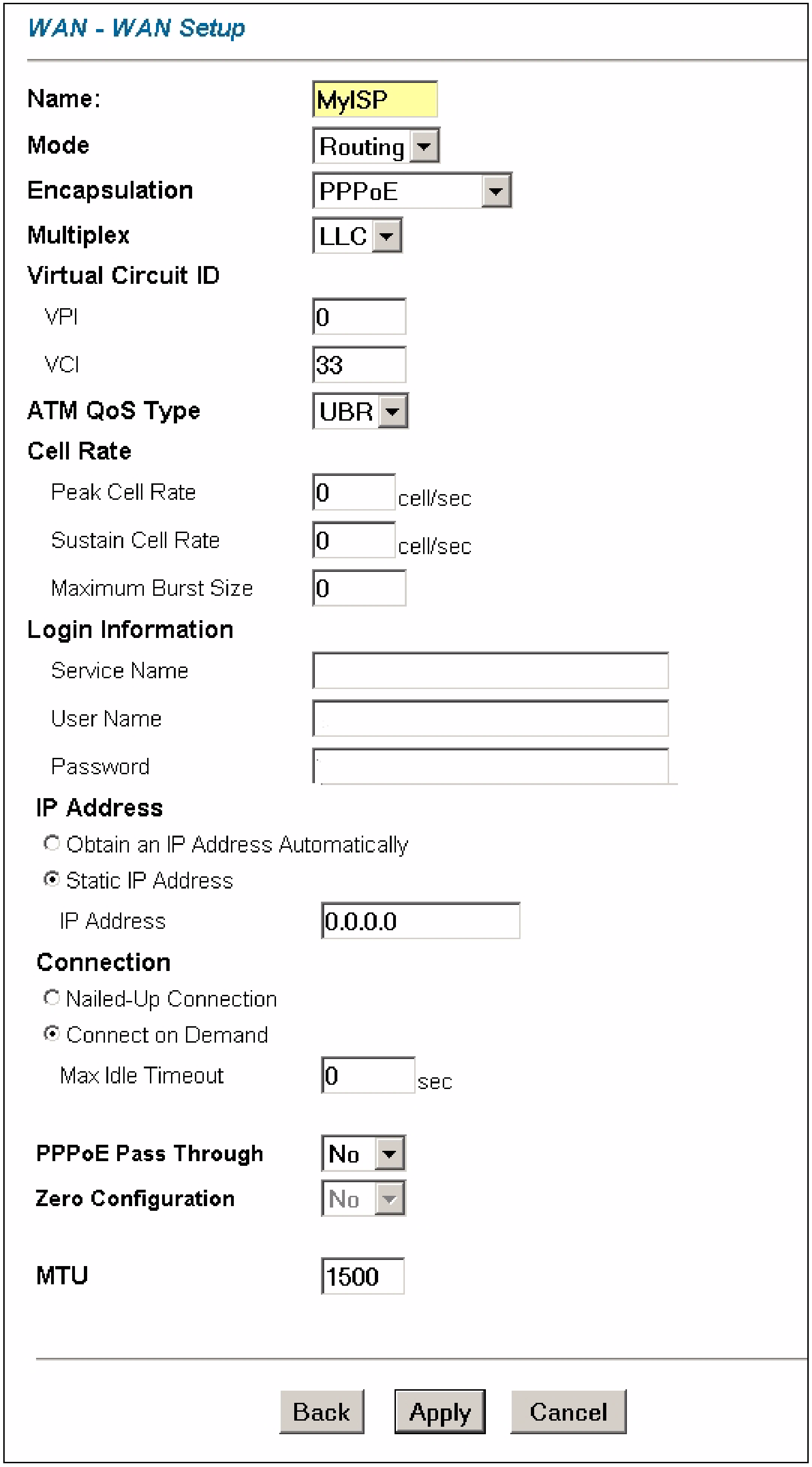
LINK	DESCRIPTION
WAN Setup	Click this link to go to the screen where you can configure your ZyXEL Device for an Internet connection.
WAN Backup	Click this link to go to the screen where you can configure WAN backup connections (traffic redirect and dial backup).

7.7 Configuring WAN Setup

To change your ZyXEL Device’s WAN remote node settings, click **WAN** and **WAN Setup**. The screen differs by the encapsulation.

See Section 7.1 on page 81 for more information.

Figure 33 WAN Setup (PPPoE)



WAN - WAN Setup

Name:	MyISP
Mode	Routing
Encapsulation	PPPoE
Multiplex	LLC
Virtual Circuit ID	
VPI	0
VCI	33
ATM QoS Type	UBR
Cell Rate	
Peak Cell Rate	0 cell/sec
Sustain Cell Rate	0 cell/sec
Maximum Burst Size	0
Login Information	
Service Name	
User Name	
Password	
IP Address	
○ Obtain an IP Address Automatically	
● Static IP Address	
IP Address	0.0.0.0
Connection	
○ Nailed-Up Connection	
● Connect on Demand	
Max Idle Timeout	0 sec
PPPoE Pass Through	No
Zero Configuration	No
MTU	1500

The following table describes the fields in this screen.

Table 26 WAN Setup

LABEL	DESCRIPTION
Name	Enter the name of your Internet Service Provider, e.g., MyISP. This information is for identification purposes only.
Mode	Select **Routing** (default) from the drop-down list box if your ISP allows multiple computers to share an Internet account. Otherwise select **Bridge**.
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the **Mode** field. If you select **Bridge** in the **Mode** field, select either **PPPoA** or **RFC 1483**. If you select **Routing** in the **Mode** field, select **PPPoA**, **RFC 1483**, **ENET ENCAP** or **PPPoE**.
Multiplex	Select the method of multiplexing used by your ISP from the drop-down list. Choices are **VC** or **LLC**.
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
ATM QoS Type	Select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **UBR** (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select **VBR** (Variable Bit Rate) for bursty traffic and bandwidth sharing with other applications.
Cell Rate	Cell rate configuration often helps eliminate traffic congestion that slows transmission of real time data such as audio and video connections.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustain Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
Login Information	(PPPoA and PPPoE encapsulation only)
Service Name	(PPPoE only) Type the name of your PPPoE service here.
User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
IP Address	This option is available if you select **Routing** in the **Mode** field. A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select **Obtain an IP Address Automatically** if you have a dynamic IP address; otherwise select **Static IP Address** and type your ISP assigned IP address in the **IP Address** field below.

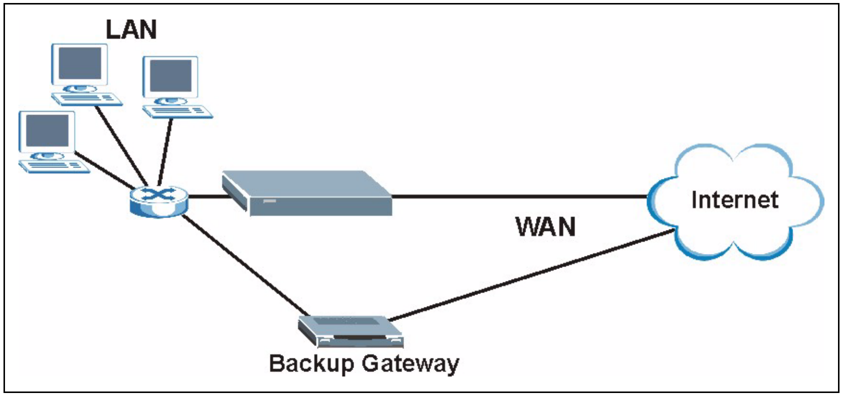
Table 26 WAN Setup (continued)

LABEL	DESCRIPTION
Connection (PPPoA and PPPoE encapsulation only)	
Nailed-Up Connection	Select **Nailed-Up Connection** when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select **Connect on Demand** when you don't want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field.
Max Idle Timeout	Specify an idle time-out in the **Max Idle Timeout** field when you select **Connect on Demand**. The default setting is 0, which means the Internet session will not timeout.
PPPoE Passthrough (PPPoE encapsulation only)	This field is available when you select **PPPoE** encapsulation. In addition to the ZyXEL Device's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the ZyXEL Device. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for application where NAT is not appropriate. Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
Subnet Mask (ENET ENCAP encapsulation only)	Enter a subnet mask in dotted decimal notation. Refer to the appendices to calculate a subnet mask If you are implementing subnetting.
ENET ENCAP Gateway (ENET ENCAP encapsulation only)	You must specify a gateway IP address (supplied by your ISP) when you select **ENET ENCAP** in the **Encapsulation** field.
Zero Configuration	This feature is not applicable/available when you configure the ZyXEL Device to use a static WAN IP address or in bridge mode. Select **Yes** to set the ZyXEL Device to automatically detect the Internet connection settings (such as the VCI/VPI numbers and the encapsulation method) from the ISP and make the necessary configuration changes. Select **No** to disable this feature. You must manually configure the ZyXEL Device for Internet access.
MTU	The **MTU** (Maximum Transmission Unit, measured in bytes) sets the largest frame size your ZyXEL Device can send. Setting a high MTU allows larger frames to be sent from your device resulting in the more efficient use of bandwidth. However, the size of frames on your network may be limited by the Ethernet maximum frame size limit of 1500 bytes. Furthermore, if other devices have a smaller MTU setting, they must fragment packets received from the ZyXEL Device, resulting in slower overall transmission speeds. Type the **MTU** in this field if your ISP gave you it. Otherwise leave it at its default setting.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

7.8 Traffic Redirect

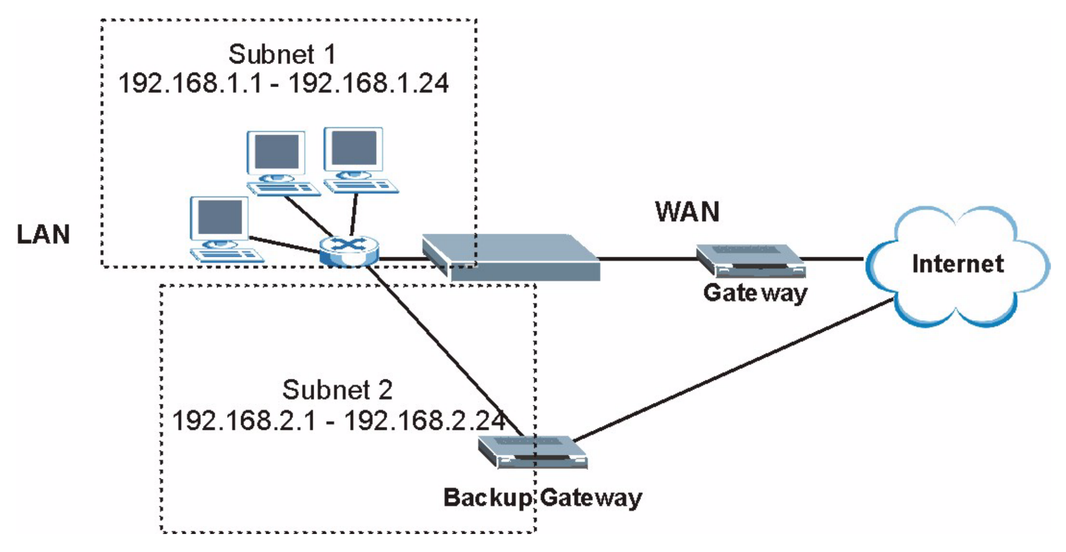
Traffic redirect forwards traffic to a backup gateway when the ZyXEL Device cannot connect to the Internet. An example is shown in the figure below.

Figure 34 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).

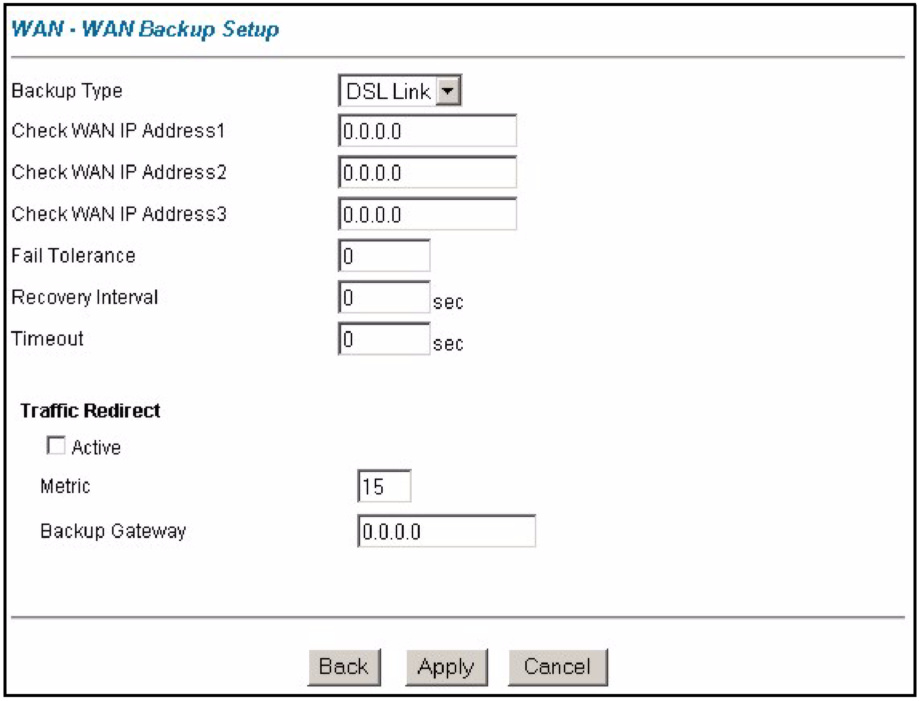
Figure 35 Traffic Redirect LAN Setup



7.9 Configuring WAN Backup

Click **WAN**, then **WAN Backup**. The screen appears as shown. Use this screen to change your ZyXEL Device's WAN backup settings.

Figure 36 WAN Backup



WAN - WAN Backup Setup

Backup Type: DSL Link ▾

Check WAN IP Address1: 0.0.0.0

Check WAN IP Address2: 0.0.0.0

Check WAN IP Address3: 0.0.0.0

Fail Tolerance: 0

Recovery Interval: 0 sec

Timeout: 0 sec

Traffic Redirect

□ Active

Metric: 15

Backup Gateway: 0.0.0.0

The following table describes the fields in this screen.

Table 27 WAN Backup

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

Table 27 WAN Backup (continued)

LABEL	DESCRIPTION
Timeout	Type the number of seconds (3 recommended) for your ZyXEL Device to wait for a ping response from one of the IP addresses in the **Check WAN IP Address** field before timing out the request. The WAN connection is considered "down" after the ZyXEL Device times out the number of times specified in the **Fail Tolerance** field. Use a higher value in this field if your network is busy or congested.
Traffic Redirect	Traffic redirect forwards traffic to a backup gateway when the ZyXEL Device cannot connect to the Internet.
Active	Select this check box to have the ZyXEL Device use traffic redirect if the normal WAN connection goes down. If you activate traffic redirect, you must configure at least one Check WAN IP Address.
Metric	This field sets this route's priority among the routes the ZyXEL Device uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
Backup Gateway	Type the IP address of your backup gateway in dotted decimal notation. The ZyXEL Device automatically forwards traffic to this IP address if the ZyXEL Device's Internet connection terminates.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

8

Network Address Translation (NAT) Screens

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

8.1 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.

8.1.1 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 28 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.

8.1.2 What NAT Does

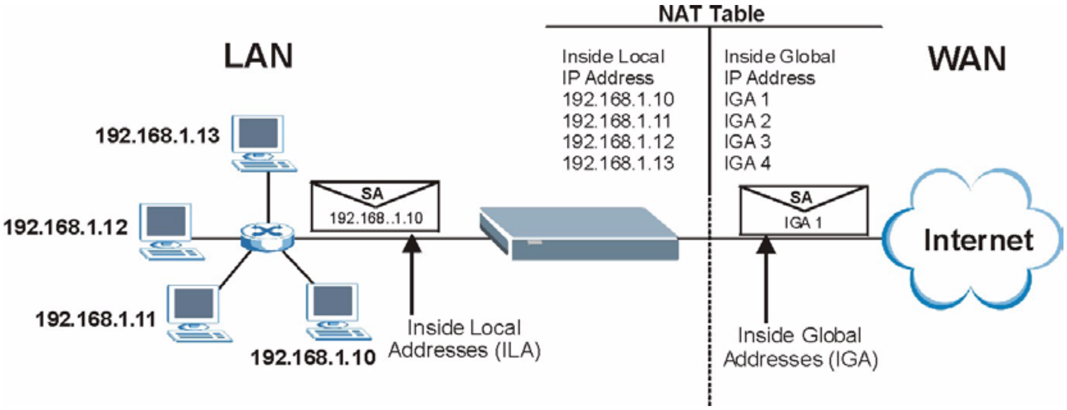
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) 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 29 on page 96), 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)*.

8.1.3 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.

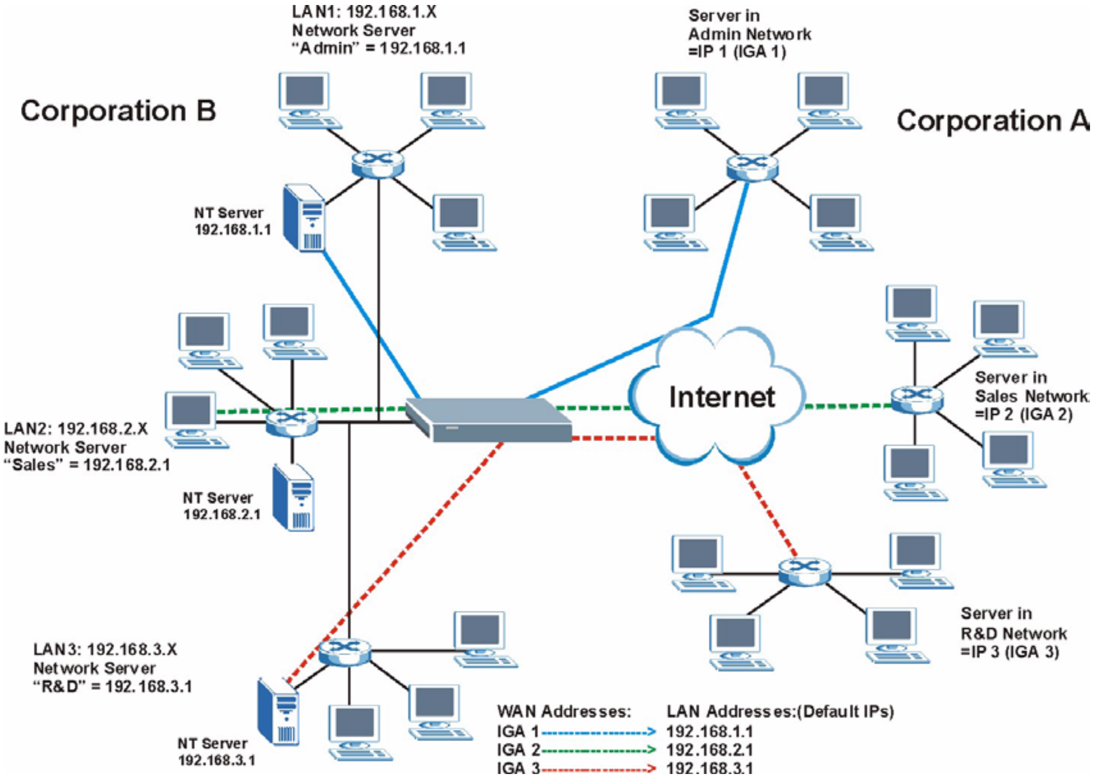
Figure 37 How NAT Works



8.1.4 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 38 NAT Application With IP Alias



8.1.5 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 29 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

8.2 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 29 on page 96.

- 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.

8.3 SUA Server

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

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

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

8.3.1 Default Server IP Address

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

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

8.3.2 Port Forwarding: Services and Port Numbers

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

Table 30 Services and Port Numbers

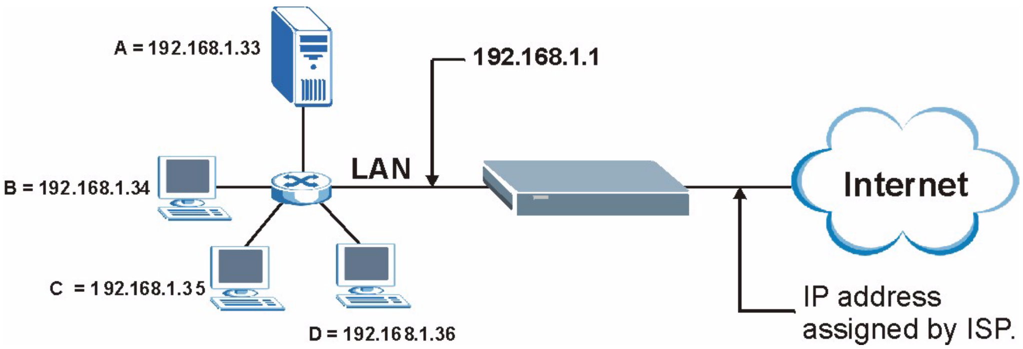
SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)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

8.3.3 Configuring Servers Behind SUA (Example)

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

IP address assigned by ISP.

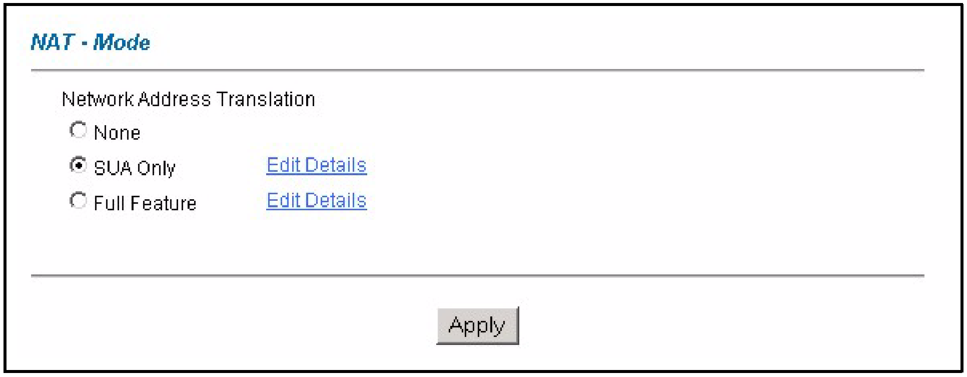
Figure 39 Multiple Servers Behind NAT Example



8.4 Selecting the NAT Mode

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 **NAT** to open the following screen.

Figure 40 NAT Mode



NAT - Mode

Network Address Translation

○ None

● SUA Only Edit Details

○ Full Feature Edit Details

The following table describes the labels in this screen.

Table 31 NAT Mode

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

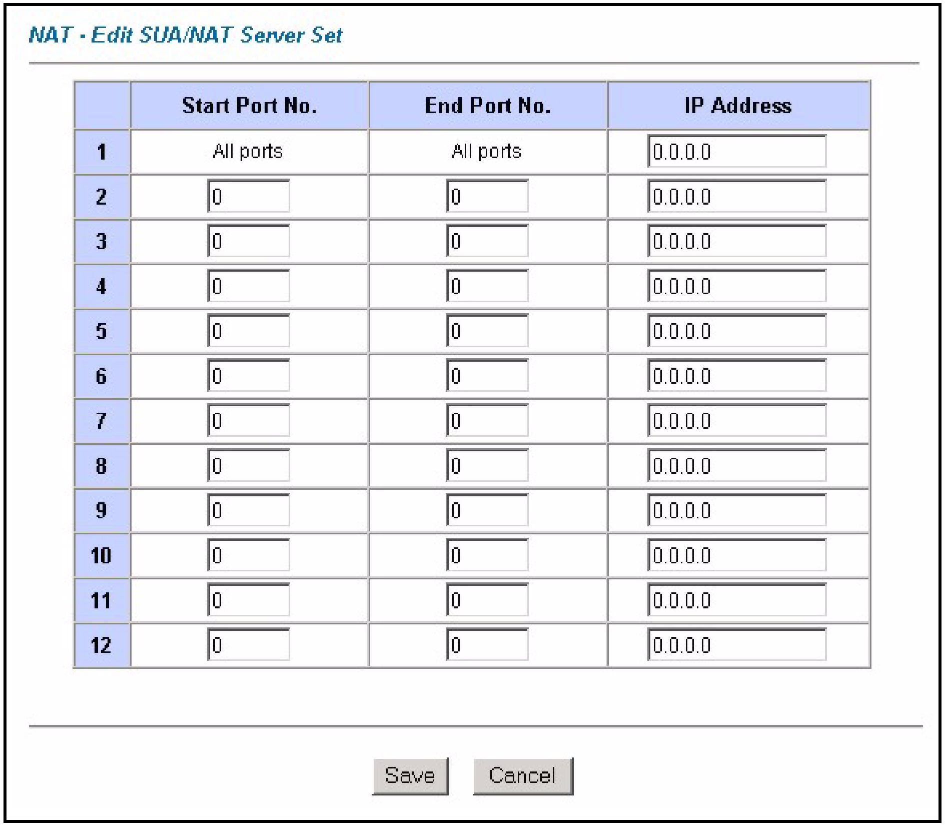
8.5 Configuring SUA Server Set

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

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

See Section 8.3 on page 96 for more information. See Table 30 on page 97 for port numbers commonly used for particular services.

Figure 41 Edit SUA/NAT Server Set



NAT - Edit SUA/NAT Server Set

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

The following table describes the fields in this screen.

Table 32 Edit SUA/NAT Server Set

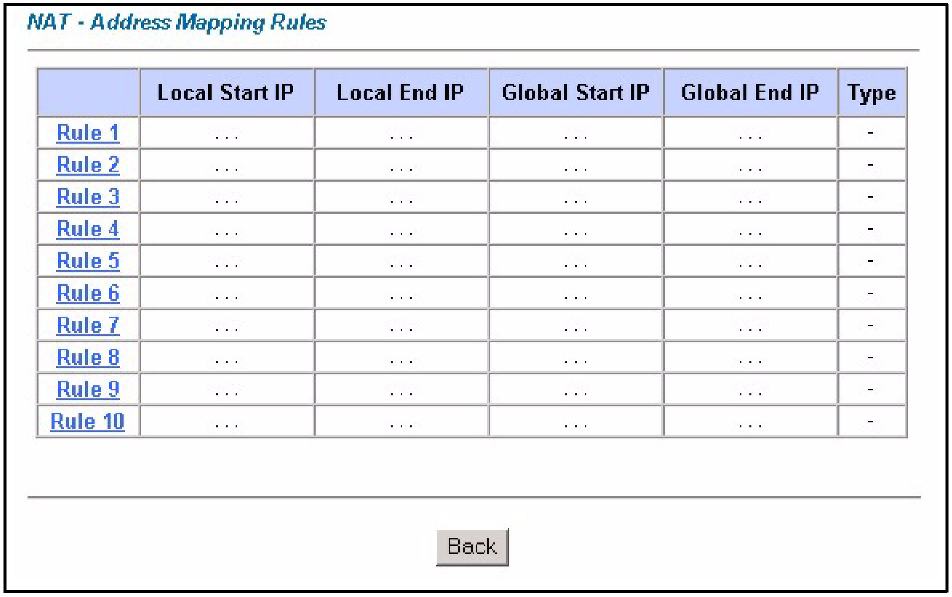
LABEL	DESCRIPTION
Start Port No.	Enter a port number in this field. To forward only one port, enter the port number again in the **End Port No.** field. To forward a series of ports, enter the start port number here and the end port number in the **End Port No.** field.
End Port No.	Enter a port number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

8.6 Configuring Address Mapping Rules

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

Click **NAT**, select **Full Feature** and click **Edit Details** to open the following screen. Use this screen to change your ZyXEL Device’s address mapping settings.

Figure 42 Address Mapping Rules



NAT - Address Mapping Rules

	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
Rule 1	...	...	...	...	-
Rule 2	...	...	...	...	-
Rule 3	...	...	...	...	-
Rule 4	...	...	...	...	-
Rule 5	...	...	...	...	-
Rule 6	...	...	...	...	-
Rule 7	...	...	...	...	-
Rule 8	...	...	...	...	-
Rule 9	...	...	...	...	-
Rule 10	...	...	...	...	-

The following table describes the fields in this screen.

Table 33 Address Mapping Rules

LABEL	DESCRIPTION
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-one** and **Server** mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for **Many-to-One** and **Server** mapping types.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is **N/A** for **One-to-one**, **Many-to-One** and **Server** mapping types.