P-870HN-51b

802.11n VDSL2 4-port Gateway

User's Guide

Default Login Details

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

Firmware Version 1.0
Edition 1, 9/2009

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.

Related Documentation

- Quick Start Guide

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

- Support Disc

  Refer to the included CD for support documents.

Documentation Feedback

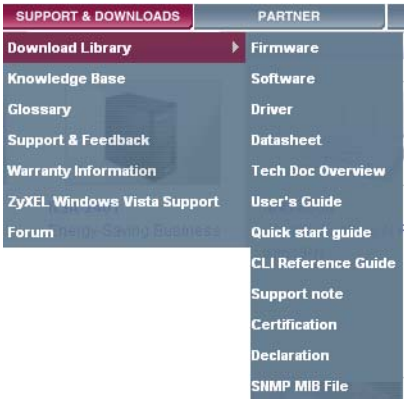
Send your comments, questions or suggestions to: techwriters@zyxel.com.tw

Thank you!

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

Need More Help?

More help is available at www.zyxel.com.



- Download Library

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

- Knowledge Base

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

- Forum

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

Customer Support

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

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

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

Document Conventions

Warnings and Notes

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

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

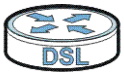
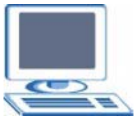
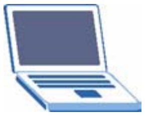
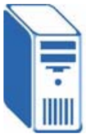
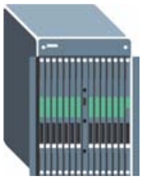
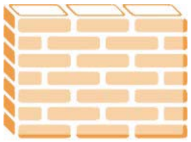
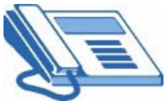
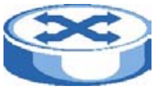
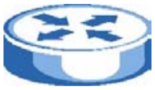
Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The P-870HN-51b may be referred to as the "ZyXEL Device", the "device", the "system" or the "product" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

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

ZyXEL Device  	Computer 	Notebook computer 
Server 	DSLAM 	Firewall 
Telephone 	Switch 	Router 

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

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

Contents Overview

Table of Contents

Chapter 14

Chapter 15

Chapter 16

Chapter 17

Chapter 18

PART I
Introduction

1

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 a VDSL2 gateway that allows super-fast, secure Internet access over analog (POTS) telephone lines. It supports both Packet Transfer Mode (PTM) and Asynchronous Transfer Mode (ATM). You can have multiple ADSL (ADSL, ADSL2, ADSL2+) connections or multiple VDSL (VDSL, VDSL2) connections.

you can use Quality of Service (QoS) to efficiently manage traffic on your network by giving priority to certain types of traffic and/or to particular computers.

Please refer to the following description of the product name format.

- “H” denotes an integrated 4-port hub (switch).
- “N” denotes 802.11n draft 2.0. The “N” models support 802.11n wireless connection mode.

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

Models ending in “1”, for example P-870HN-51, denote a device that works over the analog telephone system, POTS (Plain Old Telephone Service).

See Chapter 25 on page 253 for a full list of features.

1.2 Ways to Manage the ZyXEL Device

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

- Web Configurator. This is recommended for everyday management of the ZyXEL Device using a (supported) web browser.
- TR-069. This is an auto-configuration server used to remotely configure your device.

1.3 Good Habits for Managing the ZyXEL Device

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

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

1.4 Applications for the ZyXEL Device

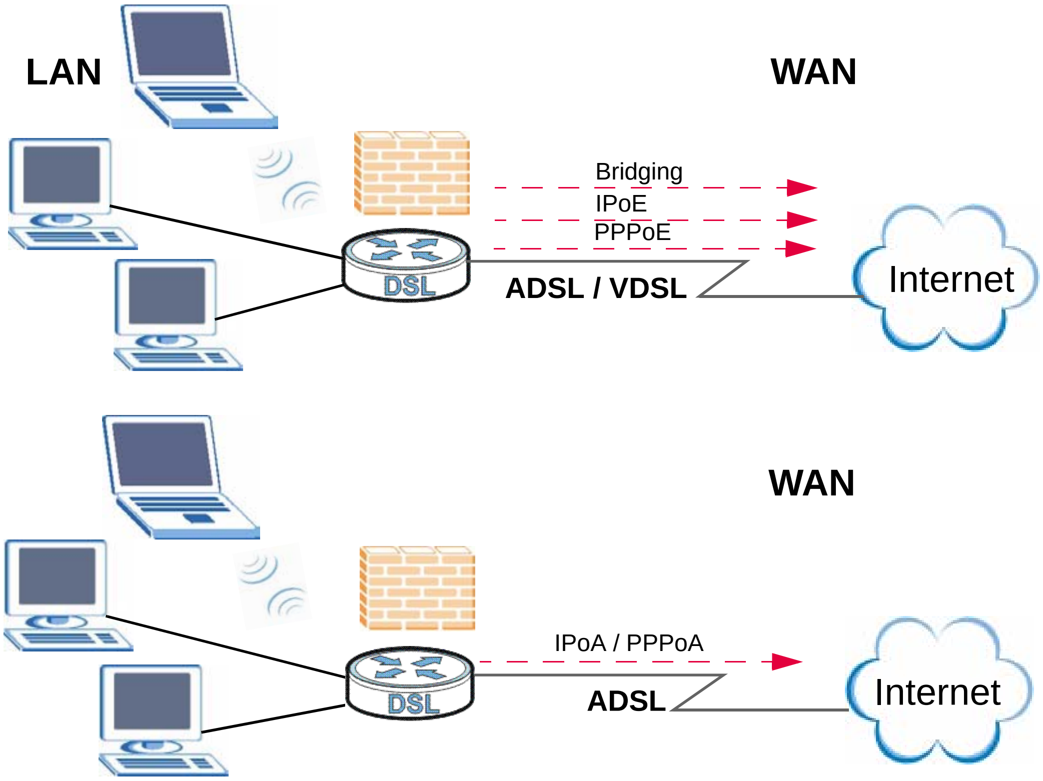
Here are some example uses for which the ZyXEL Device is well suited.

1.4.1 Internet Access

Your ZyXEL Device provides shared Internet access by connecting the DSL port to the **DSL** or **MODEM** jack on a splitter or your telephone jack. Computers can connect to the ZyXEL Device’s LAN ports (or wirelessly). You can have multiple

WAN services over one ADSL or VDSL line. The ZyXEL Device cannot work in ADSL and VDSL mode at the same time.

Figure 1 ZyXEL Device's Internet Access Application

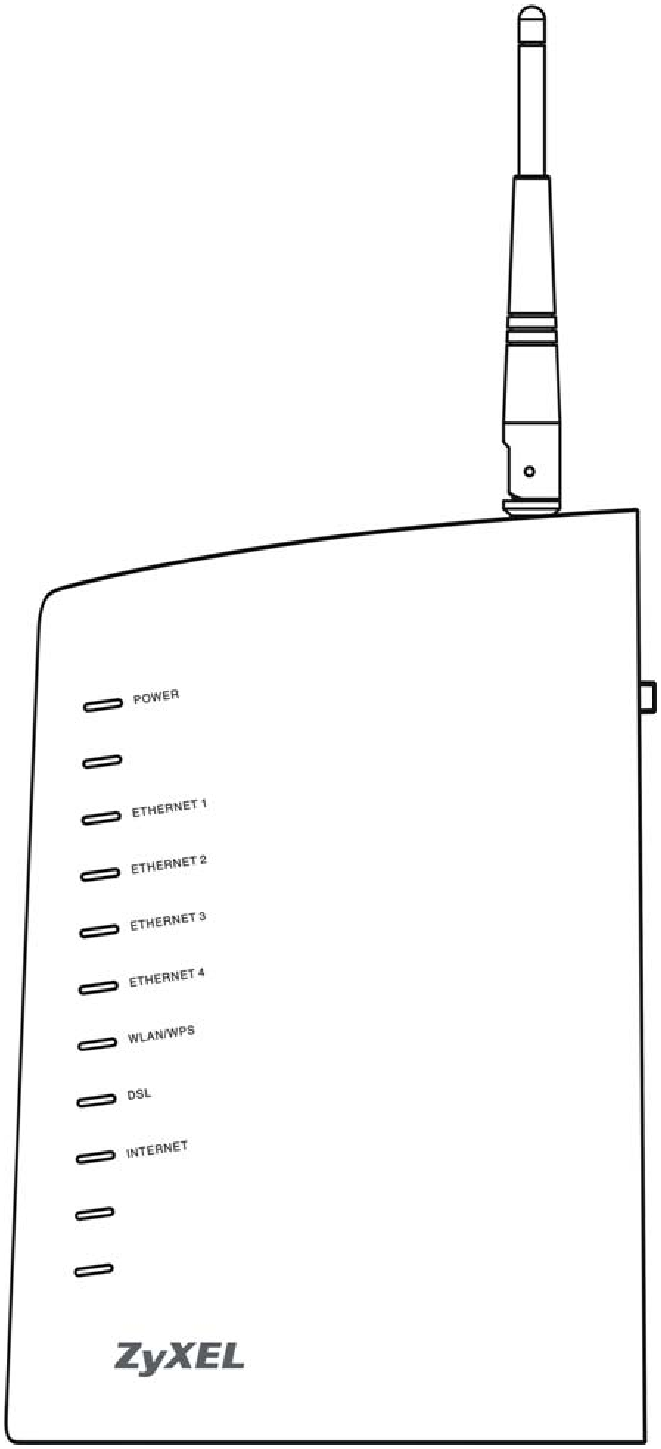


You can also configure IP filtering on the ZyXEL Device for secure Internet access. When the IP filter is on, all incoming traffic from the Internet to your network is blocked by default unless it is initiated from your network. This means that probes from the outside to your network are not allowed,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

1.5 LEDs (Lights)

The following graphic displays the labels of the LEDs.

Figure 2 The Front Panel of the Device:



None of the LEDs are on if the ZyXEL Device is not receiving power.

Table 1 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The ZyXEL Device is receiving power and ready for use.
		Blinking	The ZyXEL Device is self-testing.
	Red	On	The ZyXEL Device detected an error while self-testing, or there is a device malfunction.
		Off	The ZyXEL Device is not receiving power.
ETHERNET 1-4	Green	On	The ZyXEL Device has an Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The ZyXEL Device is sending/receiving data to /from the LAN.
		Off	The ZyXEL Device does not have an Ethernet connection with the LAN.
WLAN/ WPS	Green	On	The wireless network is activated.
		Blinking	The ZyXEL Device is communicating with other wireless clients.
	Orange	Blinking	The ZyXEL Device is setting up a WPS connection.
		Off	The wireless network is not activated.
DSL	Green	On	The ADSL line is up.
		Blinking	The ZyXEL Device is initializing the ADSL line.
	Orange	On	The VDSL line is up.
		Blinking	The ZyXEL Device is initializing the VDSL line.
		Off	The DSL line is down.
INTERNET	Green	On	The ZyXEL Device has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used) and the DSL connection is up.
	Red	On	The ZyXEL Device attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
		Off	The ZyXEL Device does not have an IP connection.

Refer to the Quick Start Guide for information on hardware connections.

1.6 The RESET Button

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

1.6.1 Using the Reset Button

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

2 To set the device back to the factory default settings, press the **RESET** button for ten seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the device restarts.

1.7 The WPS WLAN Button

You can use the **WPS WLAN** button at the rear panel of the device to turn the wireless LAN off or on. You can also use it to activate WPS in order to quickly set up a wireless network with strong security.

1.7.1 Turn the Wireless LAN Off or On

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

2 Press the **WPS WLAN** button for one second and release it. The **WLAN / WPS** LED should change from on to off or vice versa.

1.7.2 Activate WPS

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

2 Press the **WPS WLAN** button for more than five seconds and release it. Press the WPS button on another WPS -enabled device within range of the ZyXEL Device. The **WLAN / WPS** LED should flash while the ZyXEL Device sets up a WPS connection with the wireless device.

Note: You must activate WPS in the ZyXEL Device and in another wireless device within two minutes of each other. See Section 7.10.4 on page 125 for more information.

2

Tutorials

This chapter shows you how to set up a wireless network (see page 27) and how to set up multiple VDSL connection groups (see page 37).

2.1 How to Set up a Wireless Network

This tutorial gives you examples of how to set up an access point and wireless client for wireless communication using the following parameters. The wireless clients can access the Internet through an AP wirelessly.

2.1.1 Example Parameters

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

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

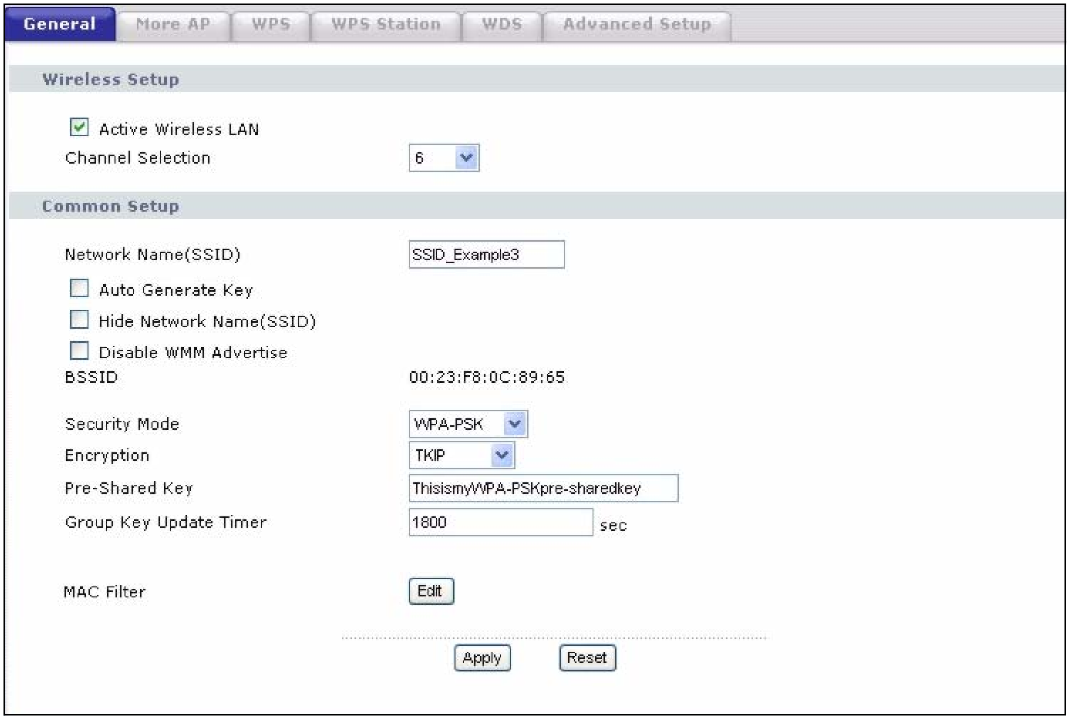
We use the ZyXEL Device web screens and M-302 utility screens as an example. The screens may vary slightly for different models.

2.1.2 Configuring the AP

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

1 Open the **Network > Wireless LAN** screen in the AP’s web configurator.

Figure 3 AP: Wireless LAN



Wireless Setup

☑ Active Wireless LAN

Channel Selection: 6

Common Setup

Network Name(SSID): SSID_Example3

□ Auto Generate Key

□ Hide Network Name(SSID)

□ Disable WMM Advertise

BSSID: 00:23:F8:0C:89:65

Security Mode: WPA-PSK

Encryption: TKIP

Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey

Group Key Update Timer: 1800 sec

MAC Filter

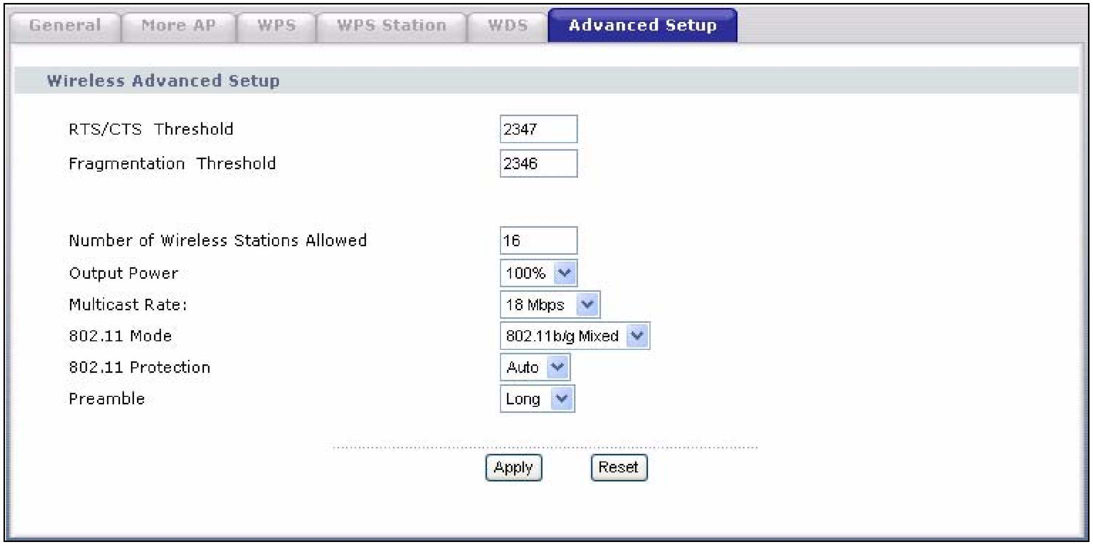
2 Make sure the **Active Wireless LAN** check box is selected.

3 Enter “SSID_Example3” as the SSID and select a channel which is not used by another AP.

4 Set security mode to **WPA-PSK** and enter “ThisismyWPA-PSKpre-sharedkey” in the **Pre-Shared Key** field. Click **Apply**.

5 Click the **Advanced Setup** tab and select **802.11b/g Mixed** in the **802.11 Mode** field. Click **Apply**.

Figure 4 AP: Wireless LAN > Advanced Setup

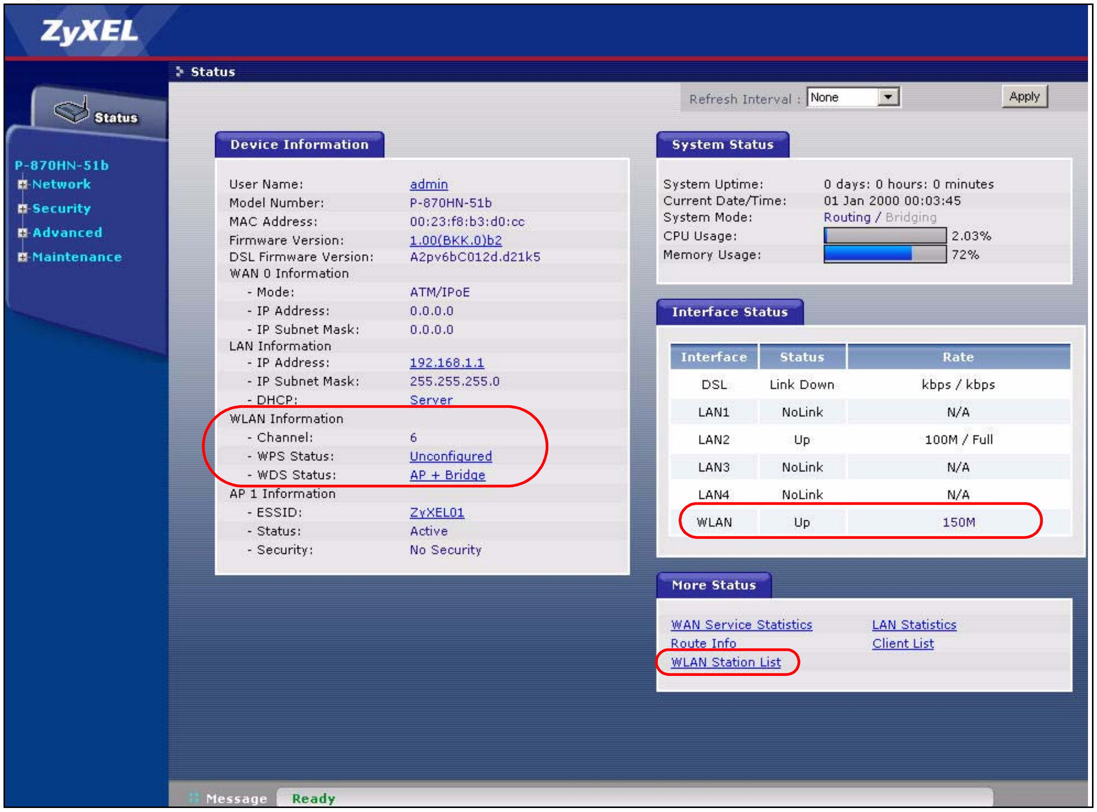


Wireless Advanced Setup

RTS/CTS Threshold	2347
Fragmentation Threshold	2346
Number of Wireless Stations Allowed	16
Output Power	100%
Multicast Rate:	18 Mbps
802.11 Mode	802.11b/g Mixed
802.11 Protection	Auto
Preamble	Long

6 Open the **Status** screen.Verify your wireless and wireless security settings under **Device Information** and check if the WLAN connection is up under **Interface Status**.

Figure 5 AP: Status



Device Information

User Name:	admin
Model Number:	P-870HN-51b
MAC Address:	00:23:f8:b3:d0:cc
Firmware Version:	1.00(BKK.0)b2
DSL Firmware Version:	A2pv6bC012d.d21k5
WAN 0 Information	
- Mode:	ATM/IPoE
- IP Address:	0.0.0.0
- IP Subnet Mask:	0.0.0.0
LAN Information	
- IP Address:	192.168.1.1
- IP Subnet Mask:	255.255.255.0
- DHCP:	Server
WLAN Information	
- Channel:	6
- WPS Status:	Unconfigured
- WDS Status:	AP + Bridge
AP 1 Information	
- ESSID:	ZyXEL01
- Status:	Active
- Security:	No Security

System Status

System Uptime:	0 days: 0 hours: 0 minutes
Current Date/Time:	01 Jan 2000 00:03:45
System Mode:	Routing / Bridging
CPU Usage:	2.03%
Memory Usage:	72%

Interface Status

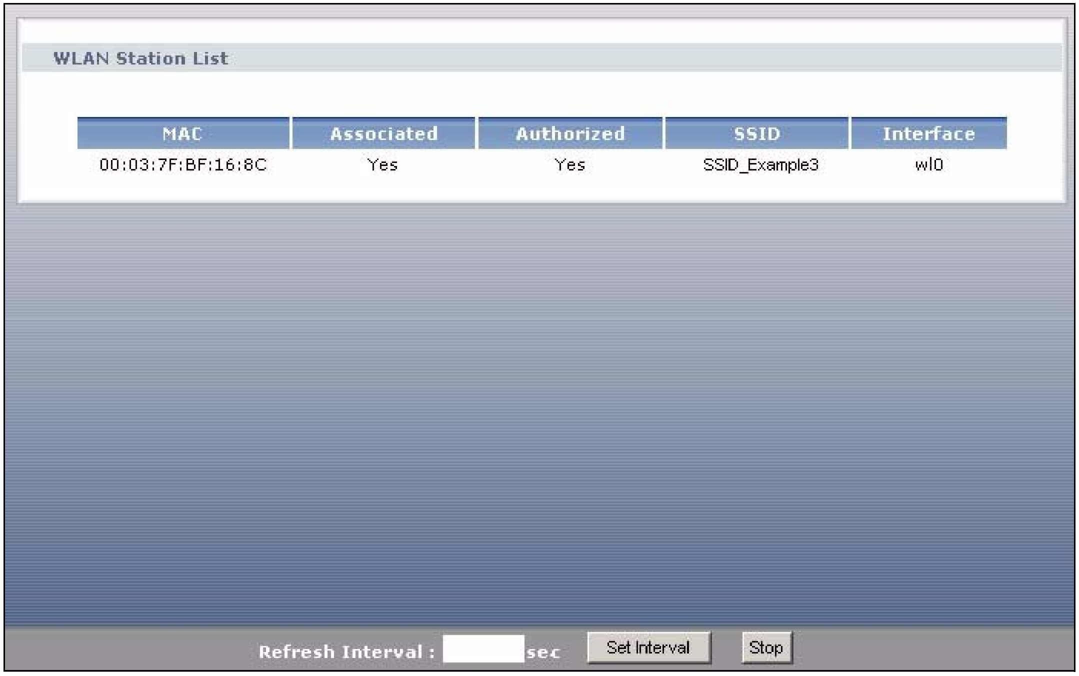
Interface	Status	Rate
DSL	Link Down	kbps / kbps
LAN1	NoLink	N/A
LAN2	Up	100M / Full
LAN3	NoLink	N/A
LAN4	NoLink	N/A
WLAN	Up	150M

More Status

WAN Service Statistics
LAN Statistics
Route Info
Client List
WLAN Station List

7 Click the **WLAN Station List** hyperlink in the AP's **Status** screen. You can see if any wireless client has connected to the AP.

Figure 6 AP: Status: WLAN Station List



WLAN Station List

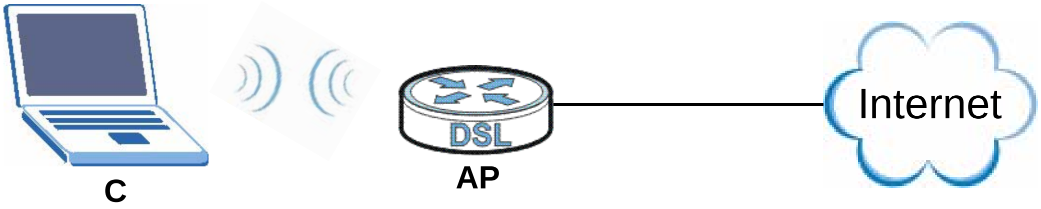
MAC	Associated	Authorized	SSID	Interface
00:03:7F:BF:16:8C	Yes	Yes	SSID_Example3	wl0

2.1.3 Configuring the Wireless Client

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

2.1.3.1 Connecting to a Wireless LAN

The following sections show you how to join a wireless network using the ZyXEL utility, as in the following diagram. The wireless client is labeled **C** and the access point is labeled **AP**.



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

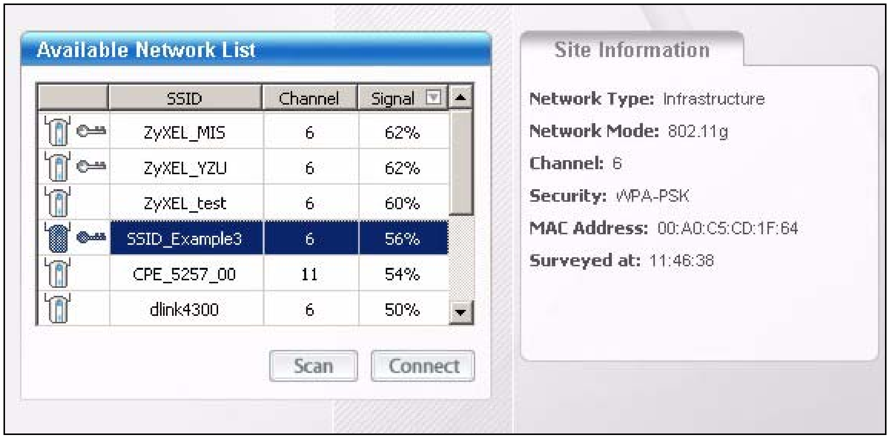
- Configure nothing and leave the wireless client to automatically scan for and connect to any available network that has no wireless security configured.
- Manually connect to a network.
- Configure a profile to have the wireless client automatically connect to a specific network or peer computer.

This example illustrates how to manually connect your wireless client to an access point (AP) which is configured for WPA-PSK security and connected to the Internet. Before you connect to the access point, you must know its Service Set IDentity (SSID) and WPA-PSK pre-shared key. In this example, the SSID is "SSID_Example3" and the pre-shared key is "ThisismyWPA-PSKpre-sharedkey".

After you install the ZyXEL utility and then insert the wireless client, follow the steps below to connect to a network using the **Site Survey** screen.

1 Open the ZyXEL utility and click the **Site Survey** tab to open the screen shown next.

Figure 7 ZyXEL Utility: Site Survey



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

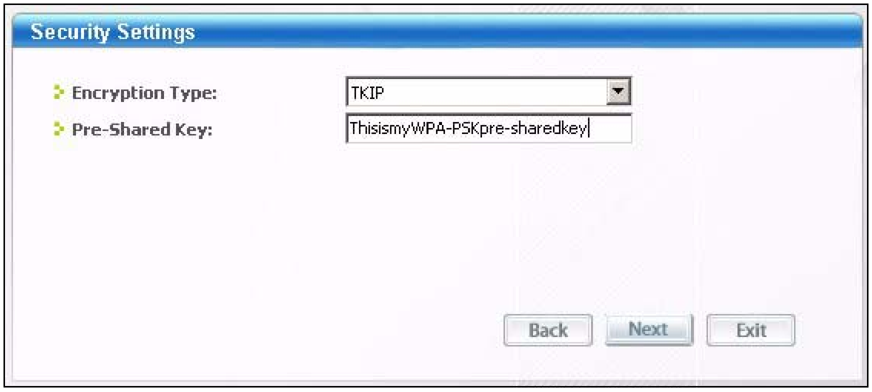
Network Type: Infrastructure
Network Mode: 802.11g
Channel: 6
Security: WPA-PSK
MAC Address: 00:A0:C5:CD:1F:64
Surveyed at: 11:46:38

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

3 When you try to connect to an AP with security configured, a window will pop up prompting you to specify the security settings. Enter the pre-shared key and leave the encryption type at the default setting.

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

Figure 8 ZyXEL Utility: Security Settings



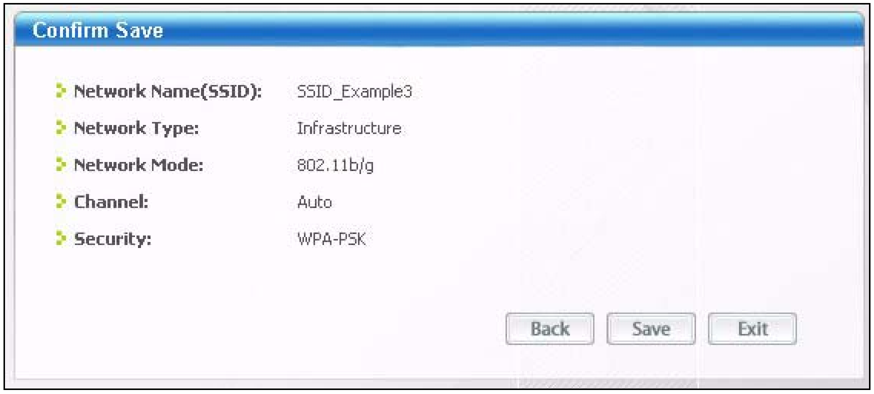
Security Settings

Encryption Type: TKIP

Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey

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

Figure 9 ZyXEL Utility: Confirm Save



Confirm Save

Network Name(SSID): SSID_Example3

Network Type: Infrastructure

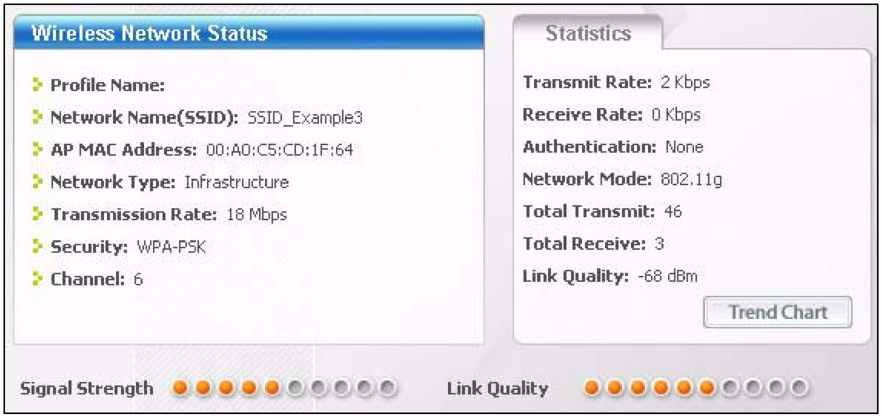
Network Mode: 802.11b/g

Channel: Auto

Security: WPA-PSK

5 The ZyXEL utility returns to the **Link Info** screen while it connects to the wireless network using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection. Check the network information in the **Link Info** screen to verify that you have successfully connected to the selected network. If the wireless client is not connected to a network, the fields in this screen remain blank.

Figure 10 ZyXEL Utility: Link Info



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

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

6 Open your Internet browser and enter http://www.zyxel.com or the URL of any other web site in the address bar. If you are able to access the web site, your wireless connection is successfully configured.

If you cannot access the web site, try changing the encryption type in the **Security Settings** screen, check the Troubleshooting section of this User's Guide or contact your network administrator.

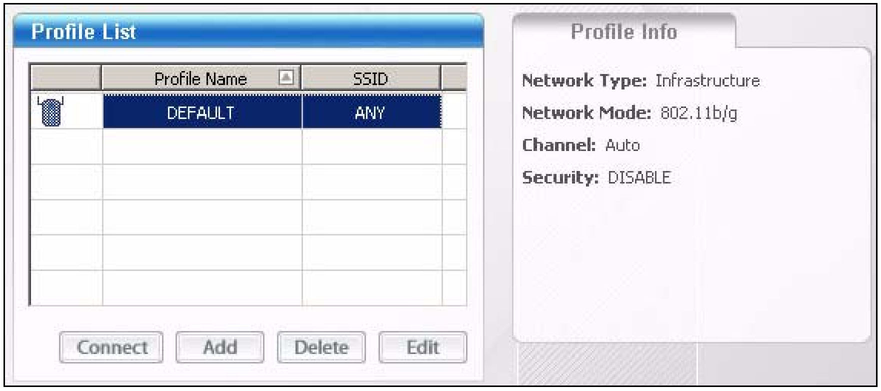
2.1.3.2 Creating and Using a Profile

A profile lets you automatically connect to the same wireless network every time you use the wireless client. You can also configure different profiles for different networks, for example if you connect a notebook computer to wireless networks at home and at work.

This example illustrates how to set up a profile and connect the wireless client to an access point configured for WPA-PSK security. In this example, the SSID is “SSID_Example3”, the profile name is “PN_Example3” and the pre-shared key is “ThisismyWPA-PSKpre-sharedkey”. You have chosen the profile name “PN_Example3”.

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

Figure 11 ZyXEL Utility: Profile

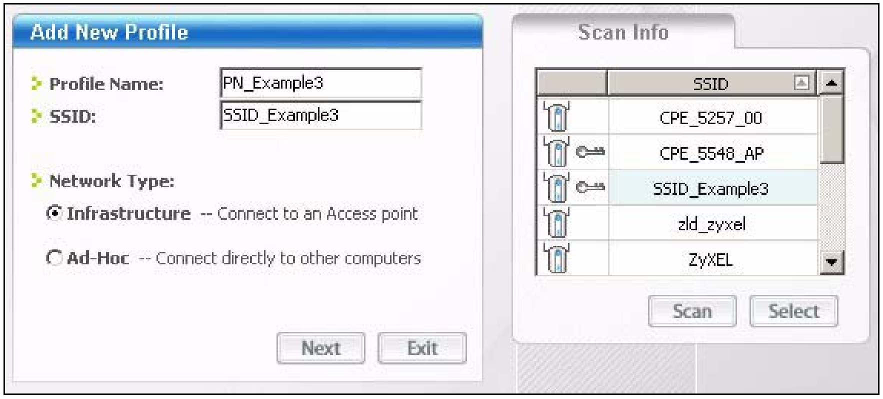


	Profile Name	SSID
	DEFAULT	ANY

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

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

Figure 12 ZyXEL Utility: Add New Profile



Profile Name: PN_Example3
SSID: SSID_Example3

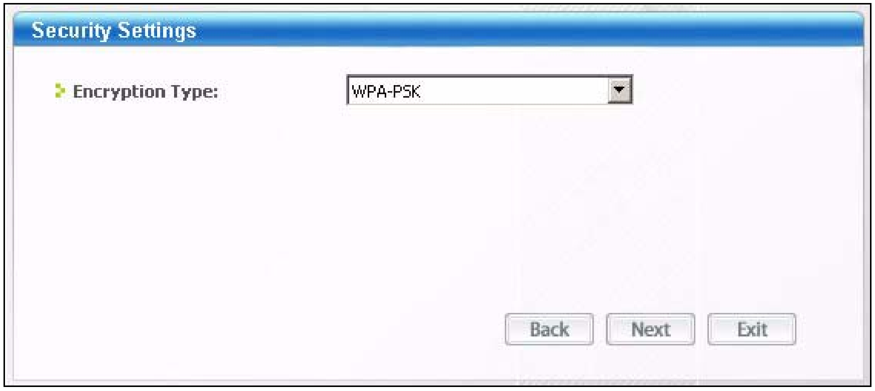
Network Type:
● Infrastructure -- Connect to an Access point
○ Ad-Hoc -- Connect directly to other computers

	SSID
	CPE_5257_00
	CPE_5548_AP
	SSID_Example3
	zld_zyxel
	ZyXEL

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

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

Figure 13 ZyXEL Utility: Profile Security

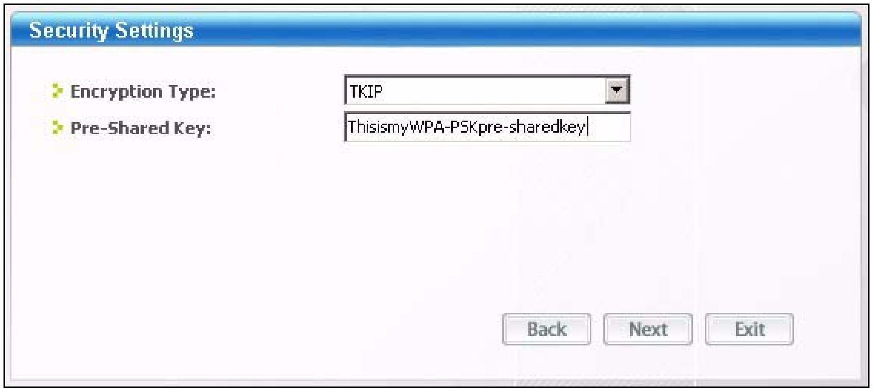


Security Settings

Encryption Type: WPA-PSK

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

Figure 14 ZyXEL Utility: Profile Encryption



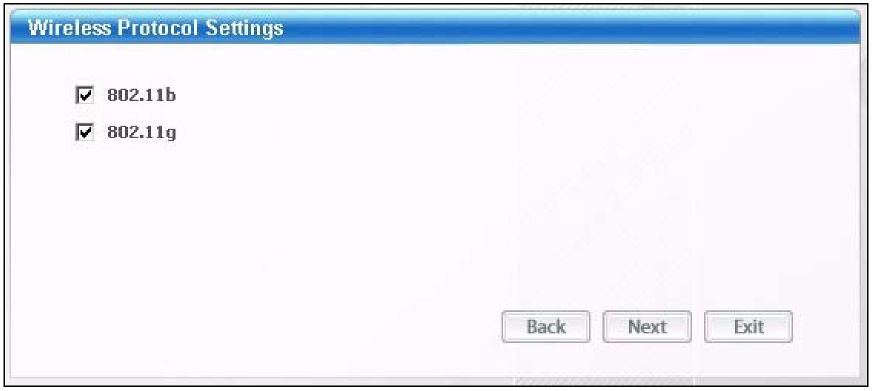
Security Settings

Encryption Type: TKIP

Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey

6 In the next screen, leave both boxes checked.

Figure 15 Profile: Wireless Protocol Settings.



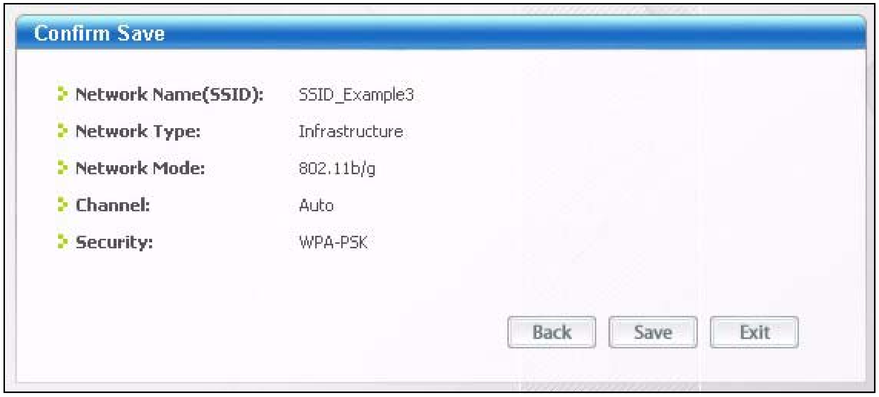
Wireless Protocol Settings

☑ 802.11b

☑ 802.11g

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

Figure 16 Profile: Confirm Save



Confirm Save

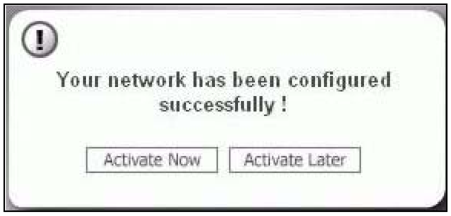
- Network Name(SSID): SSID_Example3
- Network Type: Infrastructure
- Network Mode: 802.11b/g
- Channel: Auto
- Security: WPA-PSK

8 Click **Activate Now** to use the new profile immediately. Otherwise, click the **Activate Later** button.

If you clicked **Activate Later**, you can select the profile from the list in the **Profile** screen and click **Connect** to activate it.

Note: Only one profile can be activated and used at any given time.

Figure 17 Profile: Activate



Your network has been configured successfully !

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

10 Open your Internet browser, enter http://www.zyxel.com or the URL of any other web site in the address bar and press ENTER. If you are able to access the web site, your new profile is successfully configured.

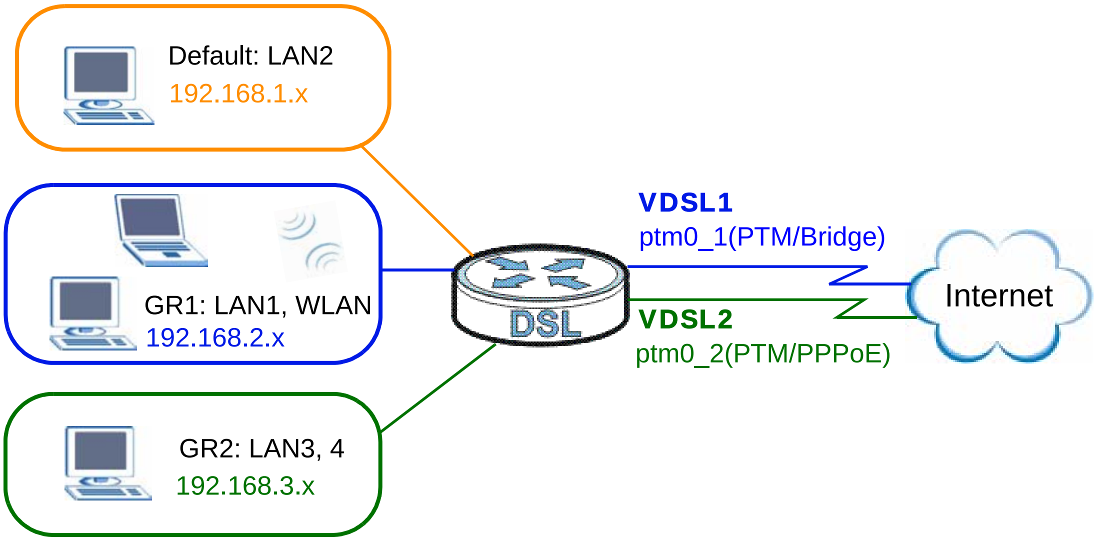
11 If you cannot access the Internet go back to the **Profile** screen, select the profile you are using and click **Edit**. Check the details you entered previously. Also, refer to the Troubleshooting section of this User's Guide or contact your network administrator if necessary.

2.2 How to Set up Multiple VDSL Connection Groups

This tutorial shows you how to set up two VDSL WAN connections for two LAN groups. GR1 will use VDSL connection 1. GR2 will use VDSL connection 2. There is also a third default group that has no WAN connection associated to it.

Table 2 VDSL Connection Groups

GROUP	LAN	WAN
Default	LAN2	N/A
GR1	LAN1, WLAN	VDSL1: ptm0_1(PTM/Bridge)
GR2	LAN3, LAN4	VDSL2: ptm0_2(PTM/PPPoE)

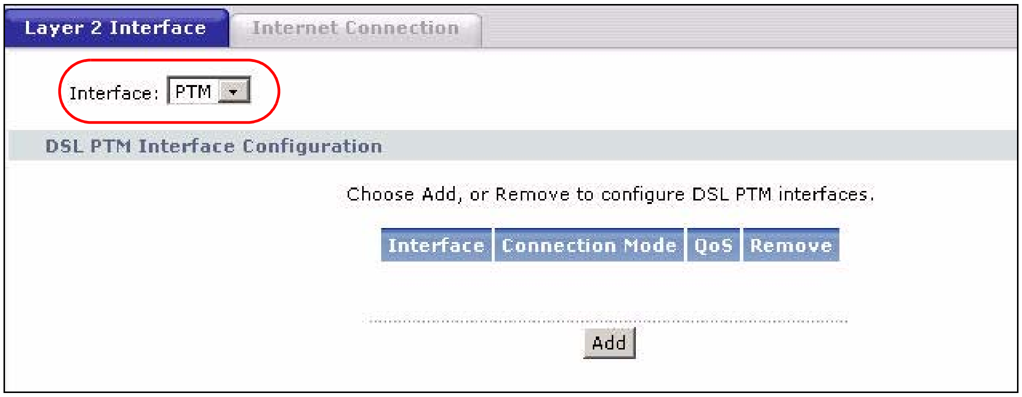


2.2.1 Adding WAN Internet Connections

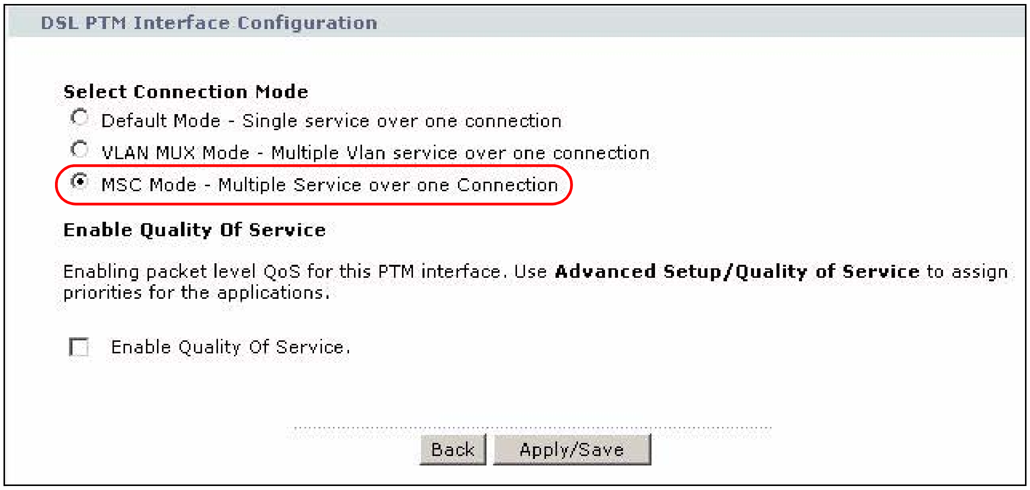
In this example, we will add 2 new WAN connections: PTM/Bridge and PTM/PPPoE.

2.2.1.1 Adding a PTM/Bridge WAN Service

1 Click **Network > WAN > Layer 2 Interface**. Select **PTM** as your interface, then click **Add**.



2 Select the **MSC Mode** as the PTM Connection Mode. Then click **Apply/Save**.


DSL PTM Interface Configuration

Select Connection Mode

○ Default Mode - Single service over one connection

○ VLAN MUX Mode - Multiple Vlan service over one connection

● MSC Mode - Multiple Service over one Connection

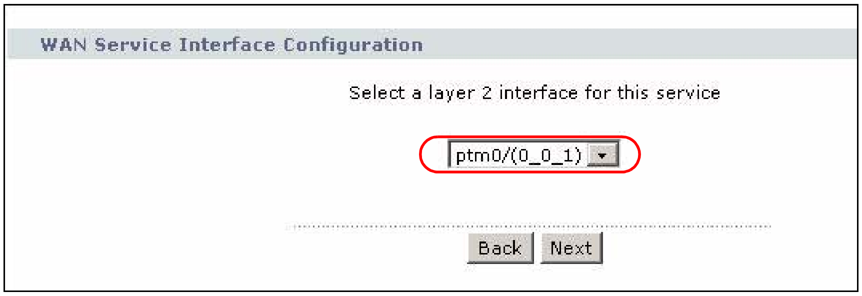
Enable Quality Of Service

Enabling packet level QoS for this PTM interface. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

□ Enable Quality Of Service.

3 The PTM interface is added to the Layer 2 Interface screen. Click **Network > WAN > Internet Connection** and click **Add**.

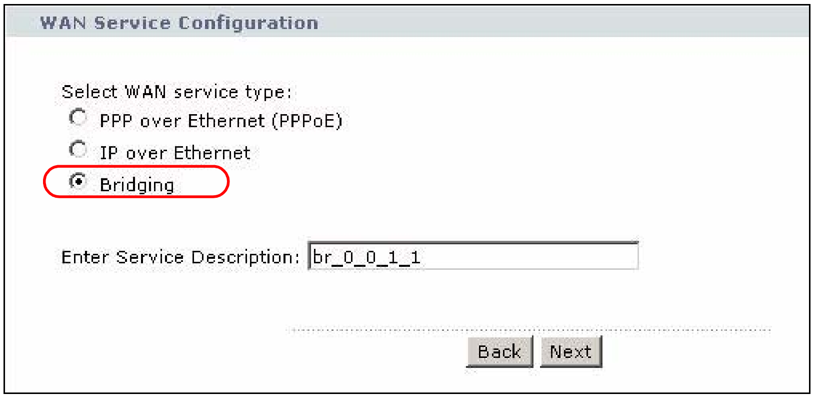
4 Select **PTM0/(0_0_1)** as the layer 2 interface for this service and click **Next**.


WAN Service Interface Configuration

Select a layer 2 interface for this service

ptm0/(0_0_1)

5 Select **Bridging** as the WAN service type. Then click **Next** to finish the setup.



WAN Service Configuration

Select WAN service type:

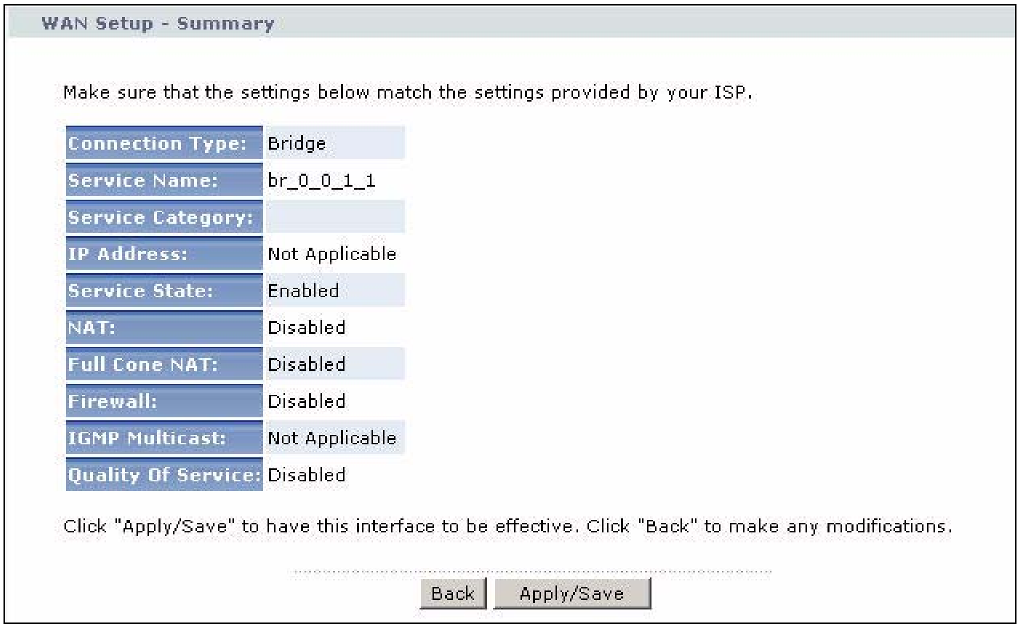
○ PPP over Ethernet (PPPoE)

○ IP over Ethernet

● Bridging

Enter Service Description: br_0_0_1_1

6 The WAN setup summary is displayed. If the settings are correct, click **Apply/ Save**.



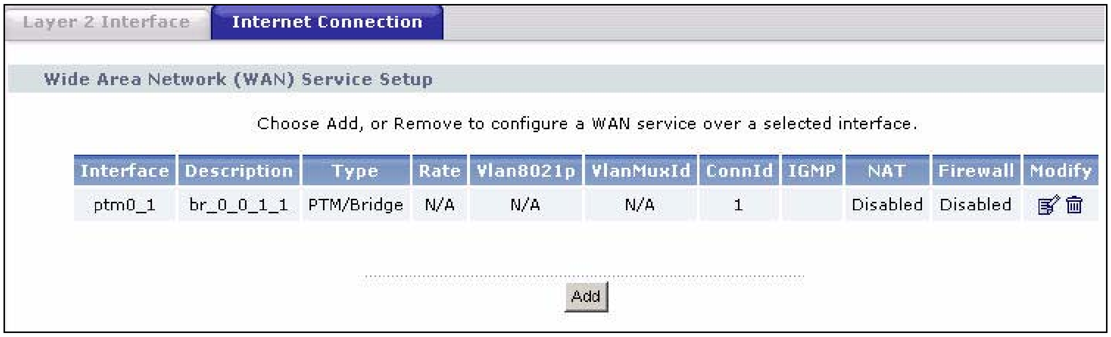
WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	Bridge
Service Name:	br_0_0_1_1
Service Category:	
IP Address:	Not Applicable
Service State:	Enabled
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Not Applicable
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

7 The PTM/Bridge WAN connection is configured successfully. The Internet Connection screen should look like the following.



Wide Area Network (WAN) Service Setup

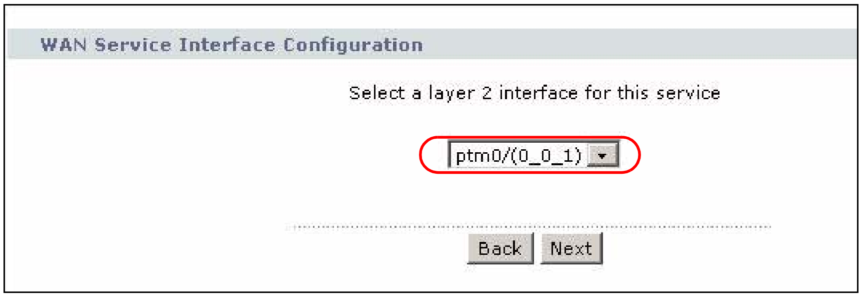
Choose Add, or Remove to configure a WAN service over a selected interface.

Interface	Description	Type	Rate	Vlan8021p	VlanMuxId	ConnId	IGMP	NAT	Firewall	Modify
ptm0_1	br_0_0_1_1	PTM/Bridge	N/A	N/A	N/A	1		Disabled	Disabled	✎ 🗑

2.2.1.2 Adding a PTM/PPPoE WAN Service

1 Click **Network > WAN > Internet Connection** and click **Add**.

2 Select **PTM0/(0_0_1)** as the layer 2 interface for this service and click **Next**.

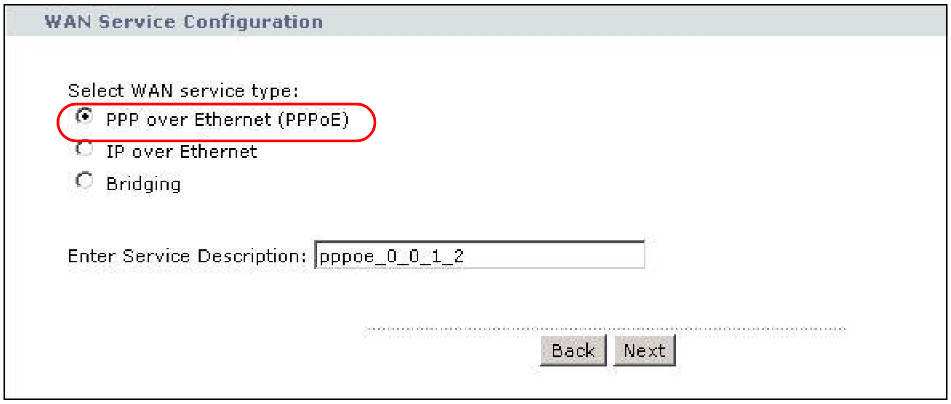


WAN Service Interface Configuration

Select a layer 2 interface for this service

ptm0/(0_0_1)

3 Select **PPP over Ethernet** as the WAN service type. Then click **Next**.



WAN Service Configuration

Select WAN service type:

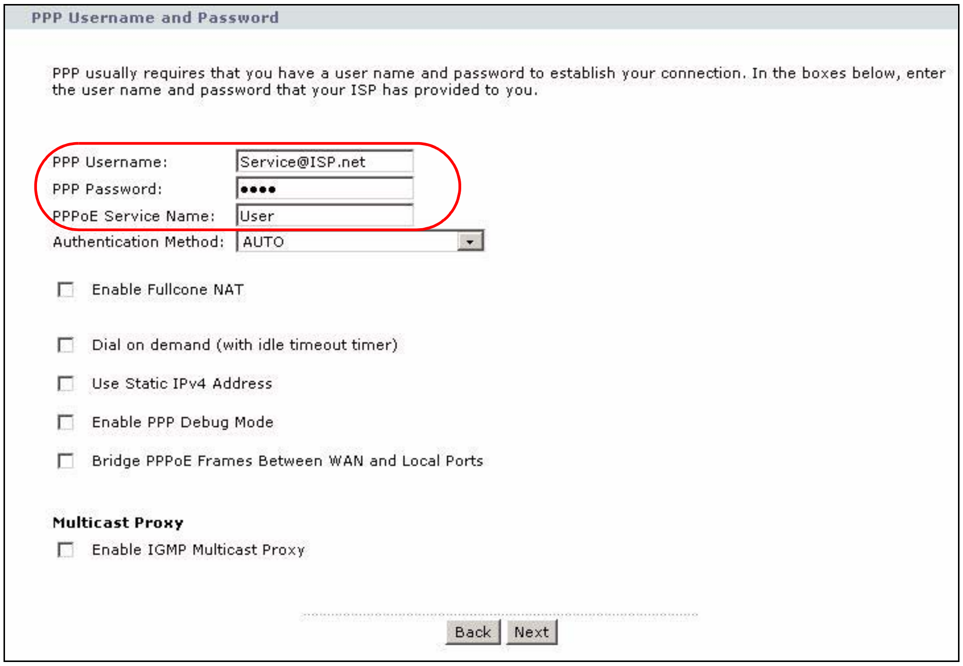
● PPP over Ethernet (PPPoE)

○ IP over Ethernet

○ Bridging

Enter Service Description: pppoe_0_0_1_2

4 Configure the PPP User and Password screen. The PPP Username is **Service@ISP.net**, the PPP Password is **1234**, and the PPPoE Service Name is **User**. Click **Next** when you finish the settings.



PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username: Service@ISP.net

PPP Password: ●●●●

PPPoE Service Name: User

Authentication Method: AUTO

□ Enable Fullcone NAT

□ Dial on demand (with idle timeout timer)

□ Use Static IPv4 Address

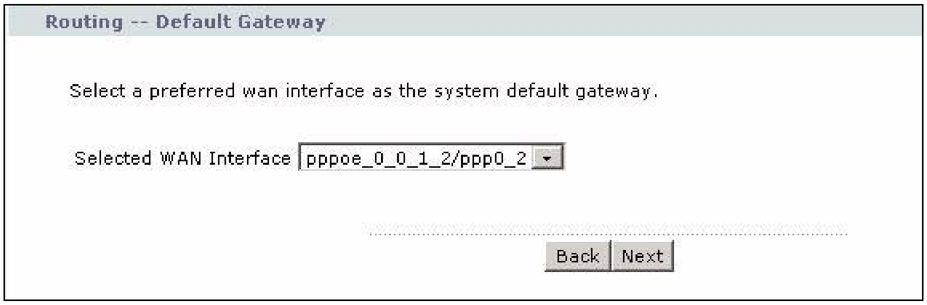
□ Enable PPP Debug Mode

□ Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

□ Enable IGMP Multicast Proxy

5 Select **pppoe_0_0_1_2 / ppp0_2** as the WAN Interface. Then click **Next**.

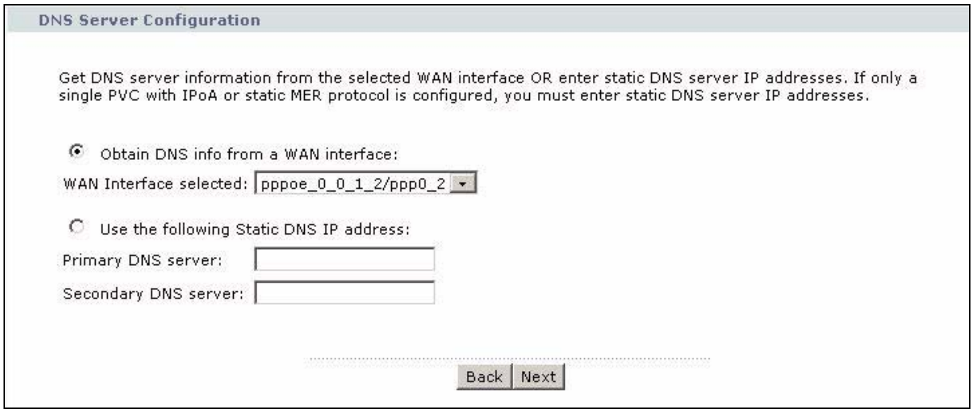


Routing -- Default Gateway

Select a preferred wan interface as the system default gateway.

Selected WAN Interface pppoe_0_0_1_2/ppp0_2

6 Obtain DNS from the PPPoE WAN interface that you selected. Then click **Next** to finish the setup.



DNS Server Configuration

Get DNS server information from the selected WAN interface OR enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.

● Obtain DNS info from a WAN interface:

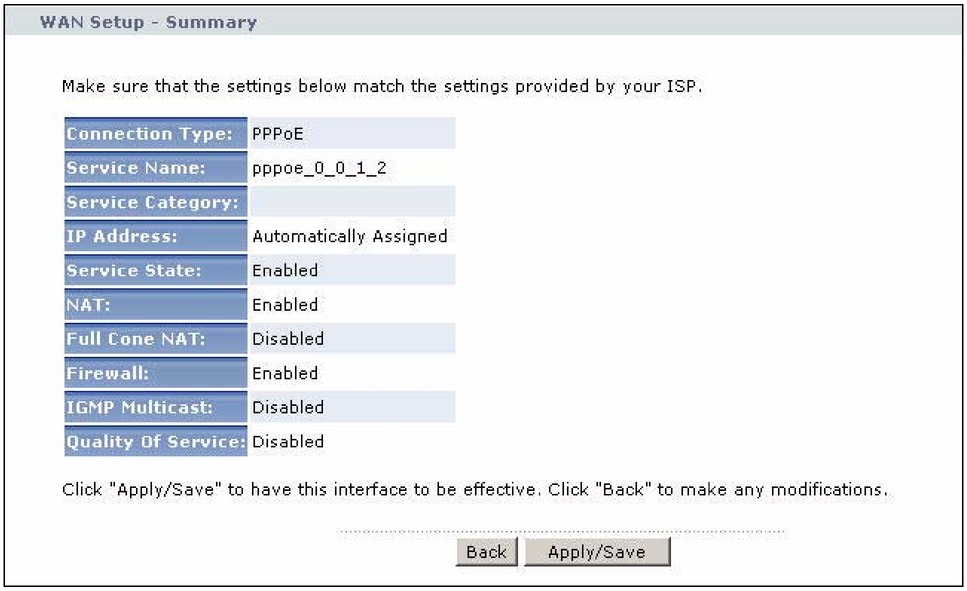
WAN Interface selected: pppoe_0_0_1_2/ppp0_2

○ Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

7 The WAN setup summary is displayed. If the settings are correct, click **Apply/ Save**.



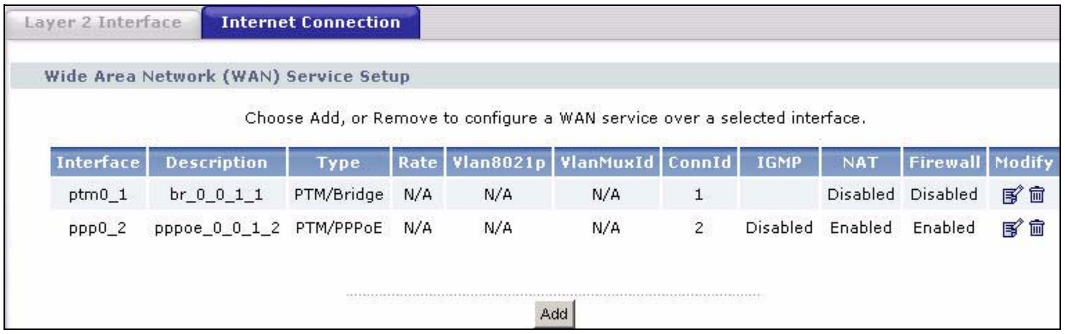
WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	PPPoE
Service Name:	pppoe_0_0_1_2
Service Category:	
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

8 The PTM/PPPoE WAN connection is configured successfully. The Internet Connection screen should look like the following.



Wide Area Network (WAN) Service Setup

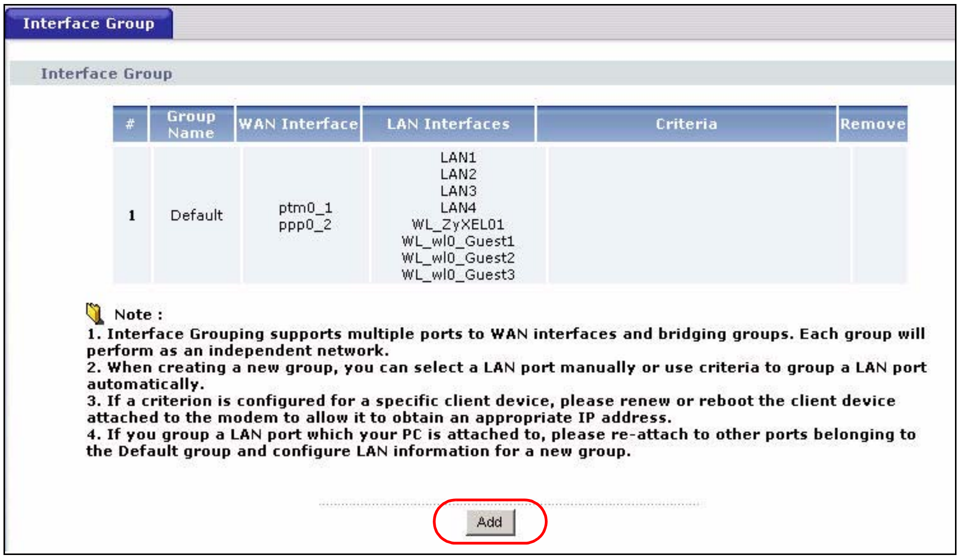
Choose Add, or Remove to configure a WAN service over a selected interface.

Interface	Description	Type	Rate	Vlan8021p	VlanMuxId	ConnId	IGMP	NAT	Firewall	Modify
ptm0_1	br_0_0_1_1	PTM/Bridge	N/A	N/A	N/A	1		Disabled	Disabled	✎ 🗑
ppp0_2	pppoe_0_0_1_2	PTM/PPPoE	N/A	N/A	N/A	2	Disabled	Enabled	Enabled	✎ 🗑

2.2.2 Setting Interface Groups

This part shows examples of creating multiple networks groups with the WAN services that you have configured in the previous section.

1 Click **Advanced Setup > Interface Group** to open the following screen. Click **Add** to create a new interface group **GR1**.



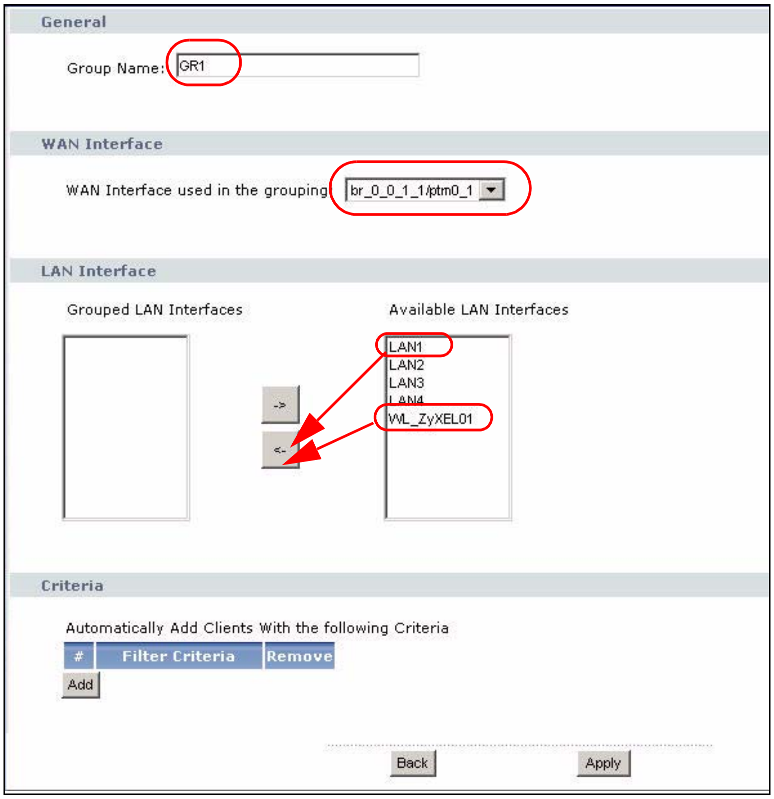
Interface Group

Interface Group

#	Group Name	WAN Interface	LAN Interfaces	Criteria	Remove
1	Default	ptm0_1 ppp0_2	LAN1 LAN2 LAN3 LAN4 WL_ZyXEL01 WL_wl0_Guest1 WL_wl0_Guest2 WL_wl0_Guest3		

Note :
1. Interface Grouping supports multiple ports to WAN interfaces and bridging groups. Each group will perform as an independent network.
2. When creating a new group, you can select a LAN port manually or use criteria to group a LAN port automatically.
3. If a criterion is configured for a specific client device, please renew or reboot the client device attached to the modem to allow it to obtain an appropriate IP address.
4. If you group a LAN port which your PC is attached to, please re-attach to other ports belonging to the Default group and configure LAN information for a new group.

2 Enter **GR1** as the Group Name. In this group, we will associate PTM/Bridge as the WAN interface with LAN1 and WL_ZyXEL01 (WLAN) as the LAN interfaces. Select **br_0_0_1_1/ptm0_1**(VDSL1) from the **WAN Interface** drop-down list. Select **LAN1** and **WL_ZyXEL01** (WLAN) from the **Available LAN Interfaces** list and click <- to add it to the **Grouped LAN Interfaces**. Click **Apply** to finish the settings.



General

Group Name: GR1

WAN Interface

WAN Interface used in the grouping: br_0_0_1_1/ptm0_1

LAN Interface

Grouped LAN Interfaces

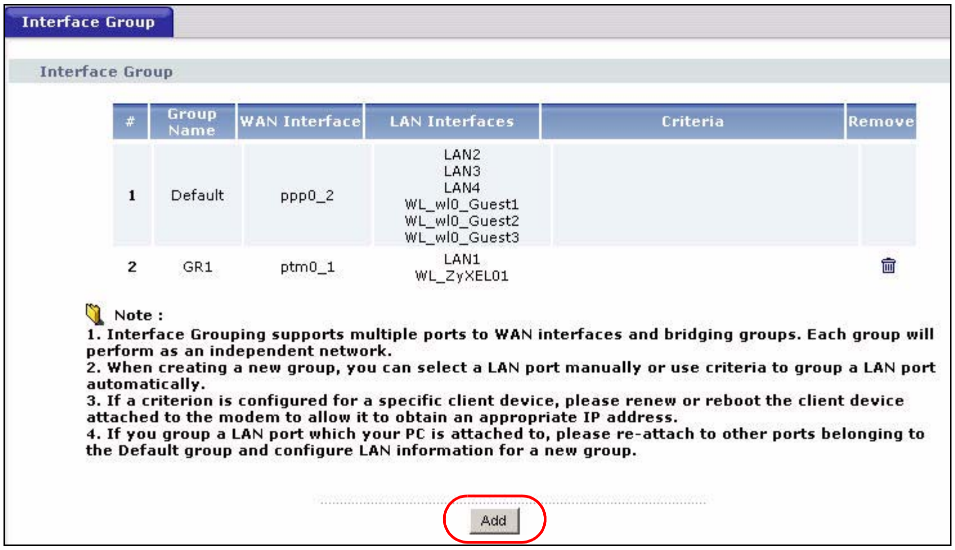
Available LAN Interfaces: LAN1, LAN2, LAN3, LAN4, WL_ZyXEL01

Criteria

Automatically Add Clients With the following Criteria

#	Filter Criteria	Remove

3 GR1 has been added successfully to the interface group list. Click **Add** to create another interface group: **GR2**.



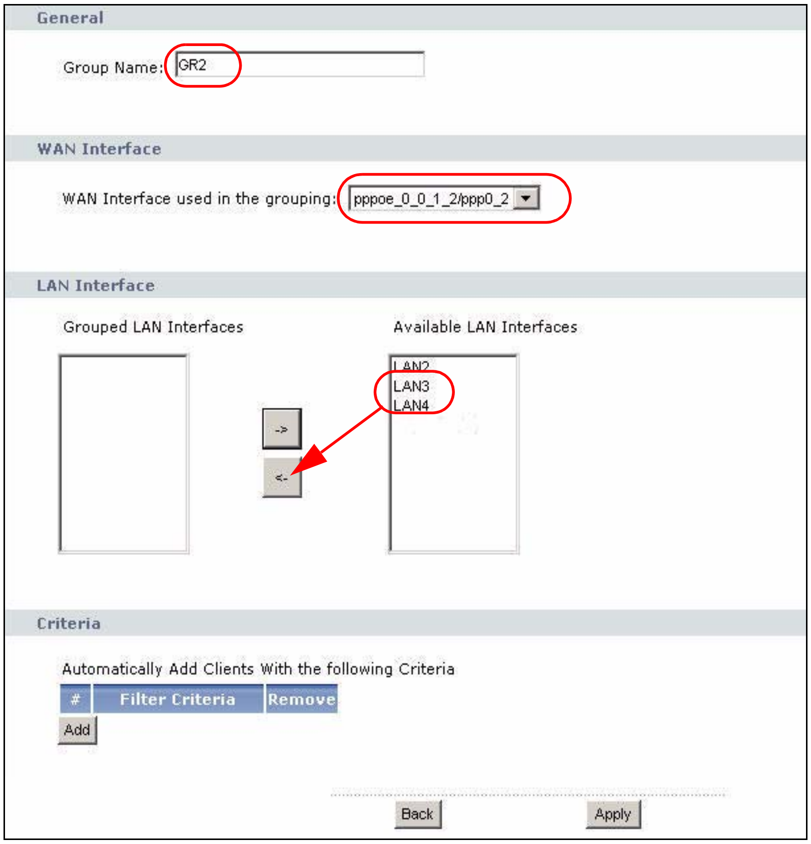
Interface Group

#	Group Name	WAN Interface	LAN Interfaces	Criteria	Remove
1	Default	ppp0_2	LAN2 LAN3 LAN4 WL_wl0_Guest1 WL_wl0_Guest2 WL_wl0_Guest3		
2	GR1	ptm0_1	LAN1 WL_ZyXEL01		🗑

Note :

1. Interface Grouping supports multiple ports to WAN interfaces and bridging groups. Each group will perform as an independent network.
2. When creating a new group, you can select a LAN port manually or use criteria to group a LAN port automatically.
3. If a criterion is configured for a specific client device, please renew or reboot the client device attached to the modem to allow it to obtain an appropriate IP address.
4. If you group a LAN port which your PC is attached to, please re-attach to other ports belonging to the Default group and configure LAN information for a new group.

4 Enter **GR2** as the Group Name. In this group, we will associate PTM/PPPoE as the WAN interface with LAN3 and LAN4 as the LAN interfaces. Select **pppoe_0_0_1_2/ppp0_2** (VDSL2) from the **WAN Interface** drop-down list. Select **LAN3** and **LAN4** from the **Available LAN Interfaces** list and click <- to add them to the **Grouped LAN Interfaces**. Click **Apply** to finish the settings.



General

Group Name: GR2

WAN Interface

WAN Interface used in the grouping: pppoe_0_0_1_2/ppp0_2

LAN Interface

Grouped LAN Interfaces

Available LAN Interfaces

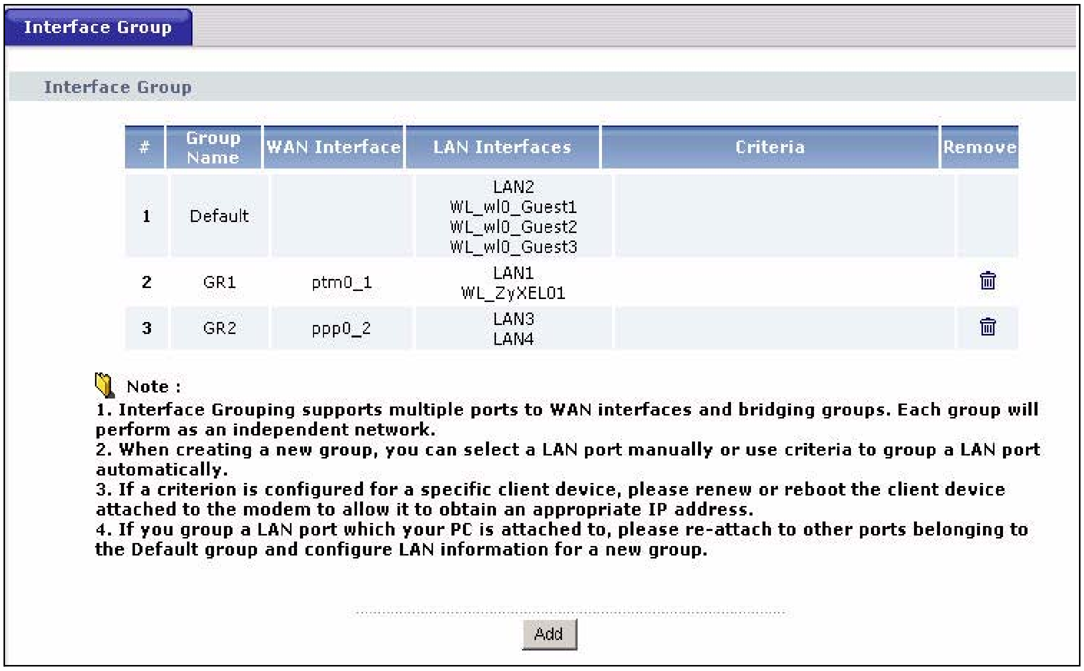
LAN2
LAN3
LAN4

Criteria

Automatically Add Clients With the following Criteria

#	Filter Criteria	Remove

5 GR2 has been added successfully to the interface group list. The screen should look like the following.



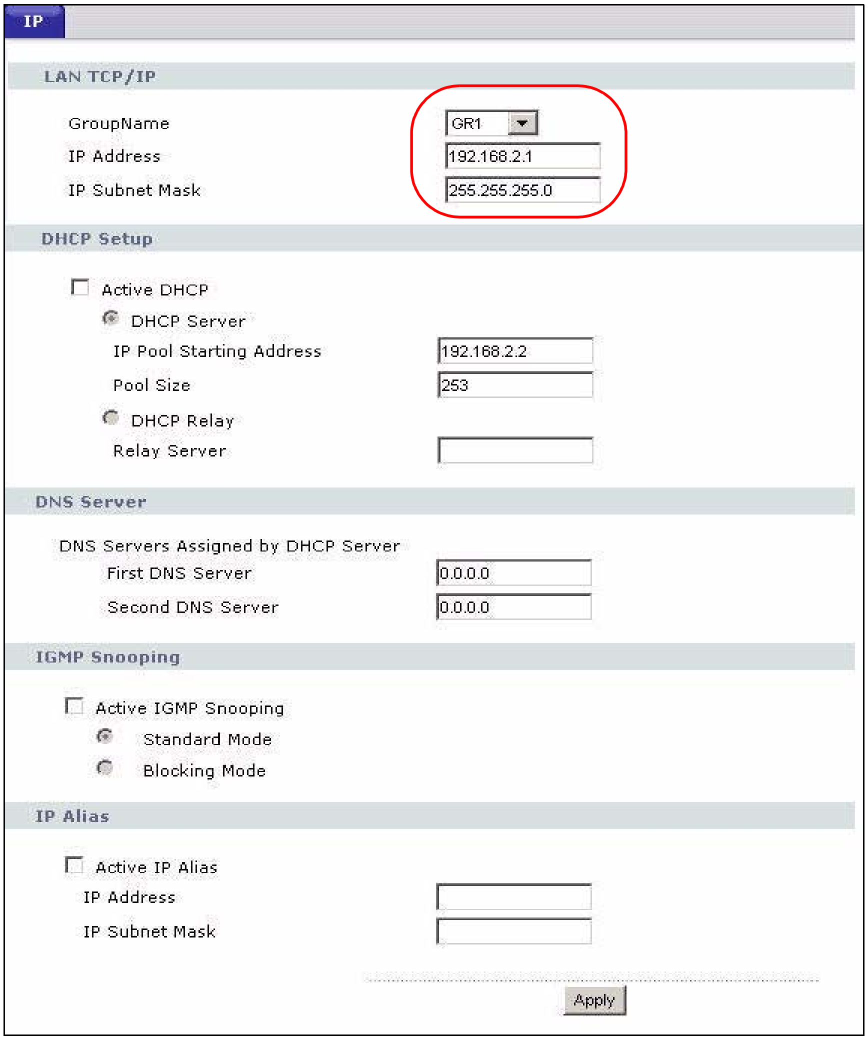
Interface Group

#	Group Name	WAN Interface	LAN Interfaces	Criteria	Remove
1	Default		LAN2 WL_wl0_Guest1 WL_wl0_Guest2 WL_wl0_Guest3		
2	GR1	ptm0_1	LAN1 WL_ZyXEL01		🗑
3	GR2	ppp0_2	LAN3 LAN4		🗑

Note :
1. Interface Grouping supports multiple ports to WAN interfaces and bridging groups. Each group will perform as an independent network.
2. When creating a new group, you can select a LAN port manually or use criteria to group a LAN port automatically.
3. If a criterion is configured for a specific client device, please renew or reboot the client device attached to the modem to allow it to obtain an appropriate IP address.
4. If you group a LAN port which your PC is attached to, please re-attach to other ports belonging to the Default group and configure LAN information for a new group.

2.2.3 Configuring Interface Group IP

1 Click **Network** > **LAN** > **IP**. Select **GR1** from the GroupName drop-down list. The IP Address (192.168.2.1) and IP Subnet Mask (255.255.255.0) is obtained automatically.



LAN TCP/IP

GroupName	GR1
IP Address	192.168.2.1
IP Subnet Mask	255.255.255.0

DHCP Setup

□ Active DHCP

● DHCP Server

IP Pool Starting Address	192.168.2.2
Pool Size	253

○ DHCP Relay

Relay Server	

DNS Server

DNS Servers Assigned by DHCP Server

First DNS Server	0.0.0.0
Second DNS Server	0.0.0.0

IGMP Snooping

□ Active IGMP Snooping

● Standard Mode

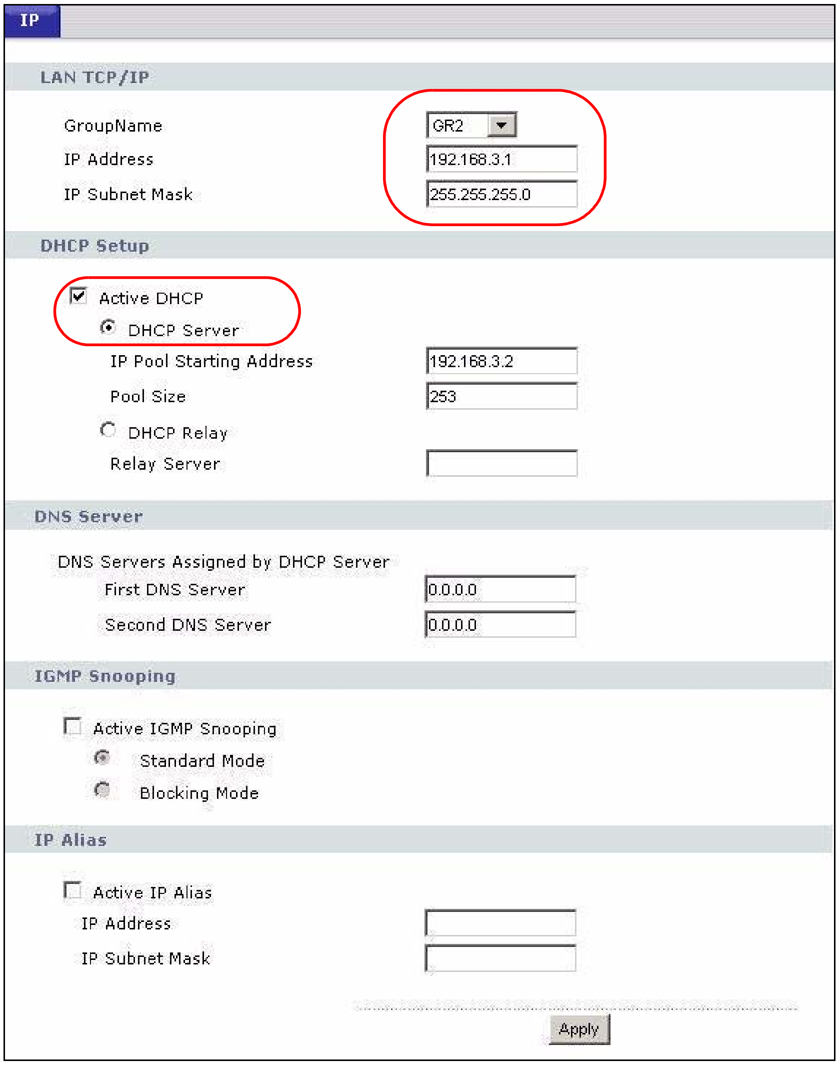
○ Blocking Mode

IP Alias

□ Active IP Alias

IP Address	
IP Subnet Mask	

2 Select **GR2** from the GroupName drop-down list. The IP Address (192.168.3.1) and IP Subnet Mask (255.255.255.0) is obtained automatically. Select **Active DHCP** and **DHCP Server** to have the ZyXEL Device act as the DHCP server for the network. Click **Apply** when you finish the settings.



IP

LAN TCP/IP

GroupName: GR2
IP Address: 192.168.3.1
IP Subnet Mask: 255.255.255.0

DHCP Setup

☑ Active DHCP
● DHCP Server
IP Pool Starting Address: 192.168.3.2
Pool Size: 253
○ DHCP Relay
Relay Server:

DNS Server

DNS Servers Assigned by DHCP Server
First DNS Server: 0.0.0.0
Second DNS Server: 0.0.0.0

IGMP Snooping

☐ Active IGMP Snooping
● Standard Mode
○ Blocking Mode

IP Alias

☐ Active IP Alias
IP Address:
IP Subnet Mask:

2.2.4 Testing the VDSL Connection Groups

To test if the connection groups are successfully configured, you can do the following: connect your computer to LAN1 of the ZyXEL Device. After a few seconds, your computer gets a new IP from the WAN side. If you can access Internet by using this VDSL connection, GR1 is successfully configured.

To test GR2, connect your computer to LAN3 or LAN4 of the ZyXEL Device. After a few seconds, the IP address of your computer should be renewed to 192.168.3.x automatically. If you can access Internet by using this VDSL connection, GR2 is successfully configured.

3

Introducing the Web Configurator

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

3.1 Web Configurator Overview

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

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

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

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

3.1.1 Accessing the Web Configurator

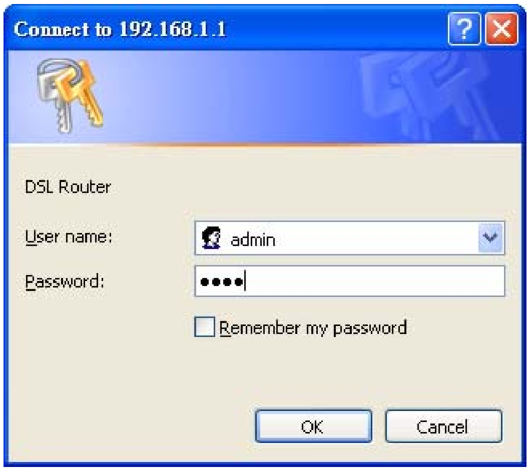
1 Make sure your ZyXEL Device hardware is properly connected (refer to the Quick Start Guide).

2 Launch your web browser.

3 Type "http://192.168.1.1" as the URL.

4 A password screen displays. Enter the default admin user name **admin** and default admin password **1234**. Otherwise, enter the default user name **user** and user password **user**. You cannot configure some settings with the user account. The password displays in non-readable characters. If you have changed the password, enter your password and click **Login**. Click **Cancel** to revert to the default password in the password field.

Figure 18 Password Screen



User name: admin

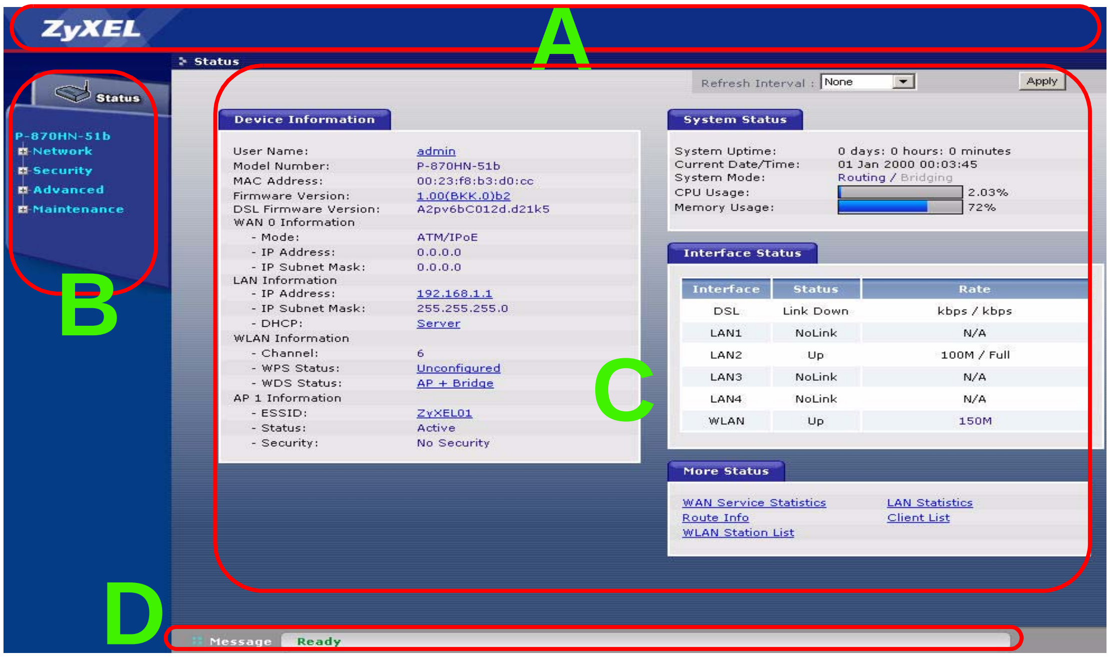
Password: ••••

□ Remember my password

3.2 Web Configurator Main Screen

This guide uses the P-870HN-51b screenshots as an example. The screens may vary slightly for different ZyXEL Device models.

Figure 19 Main Screen



Refresh Interval : None

Device Information

User Name:	admin
Model Number:	P-870HN-51b
MAC Address:	00:23:f8:b3:d0:cc
Firmware Version:	1.00(BKK.0)b2
DSL Firmware Version:	A2pv6bC012d.d21k5
WAN 0 Information	
- Mode:	ATM/IPoE
- IP Address:	0.0.0.0
- IP Subnet Mask:	0.0.0.0
LAN Information	
- IP Address:	192.168.1.1
- IP Subnet Mask:	255.255.255.0
- DHCP:	Server
WLAN Information	
- Channel:	6
- WPS Status:	Unconfigured
- WDS Status:	AP + Bridge
AP 1 Information	
- ESSID:	ZyXEL01
- Status:	Active
- Security:	No Security

System Status

System Uptime:	0 days: 0 hours: 0 minutes
Current Date/Time:	01 Jan 2000 00:03:45
System Mode:	Routing / Bridging
CPU Usage:	2.03%
Memory Usage:	72%

Interface Status

Interface	Status	Rate
DSL	Link Down	kbps / kbps
LAN1	NoLink	N/A
LAN2	Up	100M / Full
LAN3	NoLink	N/A
LAN4	NoLink	N/A
WLAN	Up	150M

More Status

WAN Service Statistics
LAN Statistics
Route Info
Client List
WLAN Station List

Message Ready

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

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

3.2.1 Navigation Panel

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

Table 3 Navigation Panel Summary

LINK	TAB	FUNCTION
Status		This screen shows the ZyXEL Device's general device and network status information. Use this screen to access the statistics and client list.
Network		
WAN	Layer 2 Interface	Use this screen to add or remove a DSL PTM (Packet Transfer Mode) interface.
	Internet Connection	Use this screen to configure ISP parameters, WAN IP address assignment, and other advanced properties.
LAN	IP	Use this screen to configure LAN TCP/IP, DHCP and IP alias settings.
Wireless LAN	General	Use this screen to configure the wireless LAN settings, WLAN authentication/security settings and MAC filtering rules.
	More AP	Use this screen to configure multiple BSSs on the ZyXEL Device.
	WPS	Use this screen to enable WPS (Wi-Fi Protected Setup) and view the WPS status.
	WPS Station	Use this screen to use WPS to set up your wireless network.
	WDS	Use this screen to set up Wireless Distribution System links to other access points.
	Advanced Setup	Use this screen to configure the advanced wireless LAN settings.
NAT	Port Forwarding	The **NAT** screens are available only when you enable NAT in a WAN connection. Use this screen to make your local servers visible to the outside world.
	Trigger Port	Use this screen to change your ZyXEL Device's port triggering settings.
	DMZ Host	Use this screen to configure a default server which receives packets from ports that are not specified in the **Port Forwarding** screen.
	ALG	Use this screen to allow SIP sessions to pass through the ZyXEL Device.

Table 3 Navigation Panel Summary

LINK	TAB	FUNCTION
Security		
MAC Filter		Use this screen to configure filtering rule(s) that blocks or allows traffic according to its destination and/or source MAC address in bridge mode.
Firewall	Incoming	This screen shows a summary of the IP filtering rules, and allows you to add or remove an incoming IP filtering rule that allows incoming traffic from the WAN.
Certificate	Local Certificates	Use this screen to view a summary list of certificates and manage certificates and certification requests.
	Trusted CA	Use this screen to view and manage the list of the trusted CAs.
Advanced		
Static Route	IP Static Route	Use this screen to configure IP static routes to tell your device about networks beyond the directly connected remote nodes.
Policy Forwarding		Use this screen to configure policy routing on the ZyXEL Device.
RIP		Use this screen to configure RIP (Routing Information Protocol) settings.
QoS	General	Use this screen to enable QoS.
	Queue Setup	Use this screen to configure QoS queues.
	Class Setup	Use this screen to define a classifier.
	Monitor	Use this screen to view QoS packets statistics.
Dynamic DNS		This screen allows you to use a static hostname alias for a dynamic IP address.
Remote MGMT	TR069	Use this screen to configure the ZyXEL Device to be managed by an ACS (Auto Configuration Server).
	TR064	Use this screen to enable management via TR-064 on the LAN.
	Service Control	Use this screen to configure which services/protocols can access which ZyXEL Device interface.
	IP Address	Use this screen to configure from which IP address(es) users can manage the ZyXEL Device.
UPnP	General	Use this screen to turn UPnP on or off.
Parental Control	Time Restriction	Use this screen to configure the days and times when the restrictions are enforced.
	URL Filter	Use this screen to prevent users of your network from viewing inappropriate web content.
Interface Group		Use this screen to map a port to a PVC or bridge group.
Maintenance		
System	General	Use this screen to configure your device’s name, domain name, management inactivity timeout and password.
	Time Setting	Use this screen to change your ZyXEL Device’s time and date.
Logs	View Log	Use this screen to view the logs for the level that you selected.
	Log Settings	Use this screen to change your ZyXEL Device’s log settings.

Table 3 Navigation Panel Summary

LINK	TAB	FUNCTION
Tools	Firmware	Use this screen to upload firmware to your device.
	Configuration	Use this screen to backup and restore your device’s configuration (settings) or reset the factory default settings.
	Restart	This screen allows you to reboot the ZyXEL Device without turning the power off.
Diagnostic	General	Use this screen to test the connections to other devices.
	802.1ag	Use this screen to configure CFM (Connectivity Fault Management) MD (maintenance domain) and MA (maintenance association), perform connectivity tests and view test reports.

3.2.2 Main Window

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

Right after you log in, the **Status** screen is displayed. See Chapter 4 on page 55 for more information about the **Status** screen.

3.2.3 Status Bar

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

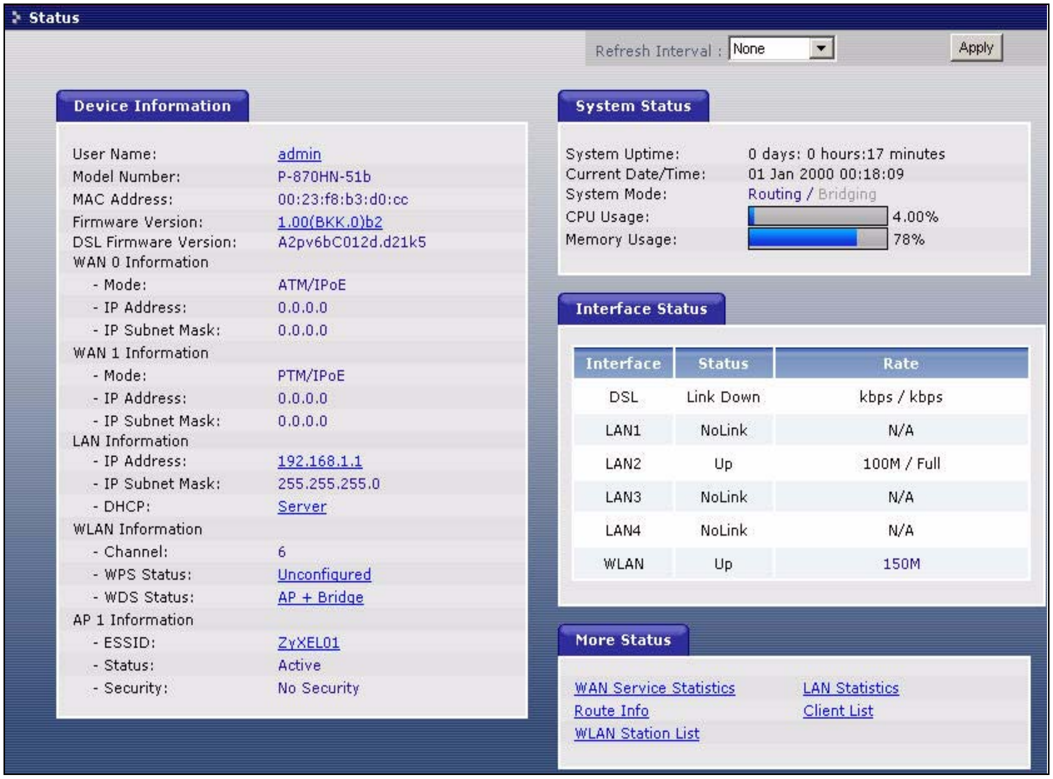
Status Screens

Use the **Status** screens to look at the current status of the device, system resources and interfaces (LAN and WAN). The **Status** screen also provides detailed information from DHCP and statistics from traffic.

4.1 Status Screen

Click **Status** to open this screen.

Figure 20 Status Screen



Device Information

User Name:	admin
Model Number:	P-870HN-51b
MAC Address:	00:23:f8:b3:d0:cc
Firmware Version:	1.00(BKK.0)b2
DSL Firmware Version:	A2pv6bC012d.d21k5
WAN 0 Information	
- Mode:	ATM/IPoE
- IP Address:	0.0.0.0
- IP Subnet Mask:	0.0.0.0
WAN 1 Information	
- Mode:	PTM/IPoE
- IP Address:	0.0.0.0
- IP Subnet Mask:	0.0.0.0
LAN Information	
- IP Address:	192.168.1.1
- IP Subnet Mask:	255.255.255.0
- DHCP:	Server
WLAN Information	
- Channel:	6
- WPS Status:	Unconfigured
- WDS Status:	AP + Bridge
AP 1 Information	
- ESSID:	ZyXEL01
- Status:	Active
- Security:	No Security

System Status

System Uptime:	0 days: 0 hours:17 minutes
Current Date/Time:	01 Jan 2000 00:18:09
System Mode:	Routing / Bridging
CPU Usage:	4.00%
Memory Usage:	78%

Interface Status

Interface	Status	Rate
DSL	Link Down	kbps / kbps
LAN1	NoLink	N/A
LAN2	Up	100M / Full
LAN3	NoLink	N/A
LAN4	NoLink	N/A
WLAN	Up	150M

More Status

Each field is described in the following table.

Table 4 Status Screen

LABEL	DESCRIPTION
Refresh Interval	Enter how often you want the ZyXEL Device to update this screen.
Apply	Click this to update this screen immediately.
Device Information	
User Name	This field displays the ZyXEL Device system name. It is used for identification. Click this to go to the screen where you can change it.
Model Number	This is the model name of your device.
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your ZyXEL Device.
Firmware Version	This field displays the current version of the firmware inside the device. It also shows the date the firmware version was created. Click this to go to the screen where you can change it.
DSL Firmware Version	This field displays the current version of the device's DSL modem code.
WAN Information	
Mode	This is the method of encapsulation used by your ISP.
IP Address	This field displays the current IP address of the ZyXEL Device in the WAN.
IP Subnet Mask	This field displays the current subnet mask in the WAN.
LAN Information	
IP Address	This field displays the current IP address of the ZyXEL Device in the LAN. Click this to go to the screen where you can change it.
IP Subnet Mask	This field displays the current subnet mask in the LAN.
DHCP	This field displays what DHCP services the ZyXEL Device is providing to the LAN. Choices are: **Server** - The ZyXEL Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. **Relay** - The ZyXEL Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. **None** - The ZyXEL Device is not providing any DHCP services to the LAN. Click this to go to the screen where you can change it.
WLAN Information	
Channel	This is the channel number used by the ZyXEL Device now.

Table 4 Status Screen

LABEL	DESCRIPTION
WPS Status	This field displays the status of WPS (Wi-Fi Protected Setup). Click this to go to the screen where you can change it.
WDS Status	This field displays • **AP** when WDS is disabled. • **Bridge** when the ZyXEL Device functions as a wireless network bridge only to use WDS (Wireless Distribution System) to establish wireless links with other APs. • **AP+Bridge** when WDS is enabled and the ZyXEL Device acts as a bridge and access point simultaneously. Click this to go to the screen where you can change it
AP Information	
ESSID	This is the descriptive name used to identify the ZyXEL Device in this wireless network. Click this to go to the screen where you can change it.
Status	This shows the current status of the wireless network.
Security	This shows the level of wireless security the ZyXEL Device is using in this wireless network.
System Status	
System Uptime	This field displays how long the ZyXEL Device has been running since it last started up. The ZyXEL Device starts up when you plug it in, when you restart it (**Maintenance > Tools > Restart**), or when you reset it (see Section 1.6 on page 25).
Current Date/Time	This field displays the current date and time in the ZyXEL Device. You can change this in **Maintenance > System > Time Setting**.
System Mode	This displays whether the ZyXEL Device is functioning as a router or a bridge.
CPU Usage	This field displays what percentage of the ZyXEL Device's processing ability is currently used. When this percentage is close to 100%, the ZyXEL Device is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using QoS; see Chapter 14 on page 177).
Memory Usage	This field displays what percentage of the ZyXEL Device's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100%, the ZyXEL Device is probably becoming unstable, and you should restart the device. See Section 22.4 on page 238, or turn off the device (unplug the power) for a few seconds.
Interface Status	
Interface	This column displays each interface the ZyXEL Device has.

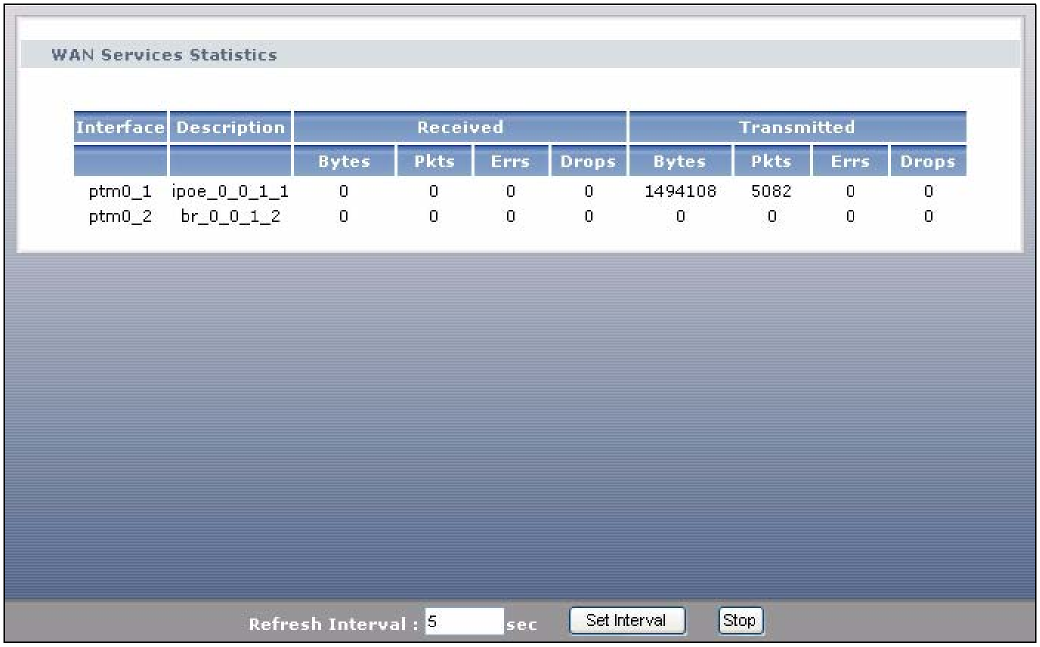
Table 4 Status Screen

LABEL	DESCRIPTION
Status	This field indicates whether or not the ZyXEL Device is using the interface. For the DSL interface, this field displays **LinkDown** (line is down) or **Up** (line is up or connected). For the LAN interface, this field displays **Up** when the ZyXEL Device is using the interface and **NoLink** when the line is disconnected. For the WLAN interface, it displays **Up** when WLAN is enabled or **Disabled** when WLAN is not active.
Rate	For the DSL interface, it displays the downstream and upstream transmission rate. For the LAN interface, this displays the port speed and duplex setting. For the WLAN interface, it displays the maximum transmission rate.
More Status	
WAN Service Statistics	Click this link to view packet specific statistics of the WAN connection(s). See Section 4.1.1 on page 59.
Route Info	Click this link to view the internal routing table on the ZyXEL Device. See Section 4.1.2 on page 60.
WLAN Station List	Click this link to display the MAC address(es) of the wireless stations that are currently associating with the ZyXEL Device. See Section 4.1.3 on page 62.
LAN Statistics	Click this link to view packet specific statistics on the LAN and WLAN interfaces. See Section 4.1.4 on page 63.
Client List	Click this link to view current DHCP client information. See Section 4.1.5 on page 64.

4.1.1 WAN Service Statistics

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

Figure 21 Status > WAN Service Statistics



WAN Services Statistics

Interface	Description	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
ptm0_1	ipoe_0_0_1_1	0	0	0	0	1494108	5082	0	0
ptm0_2	br_0_0_1_2	0	0	0	0	0	0	0	0

Refresh Interval : 5 sec

The following table describes the labels in this screen.

Table 5 Status > WAN Service Statistics

LABEL	DESCRIPTION
Interface	This shows the name of the WAN interface used by this connection. The default name **ipoa***, **pppoa*, atm*** or **ptm*** indicates the DSL port. **pppx** (where x starts from 0 and is the index number of PPP connection on the ZyXEL Device) indicates a PPP connection via any one of the WAN interface. The number after the dot (**.**) represents the VLAN ID number assigned to traffic sent through this connection. The number after the underscore (_) represents the index number of connections through the same interface. **(null)** means the entry is not valid.
Description	This shows the descriptive name of this connection. **0** and **35** or **0** and **1** are the default VPI and VCI numbers. The last number represents the index number of connections over the same PVC or the VLAN ID number assigned to traffic sent through this connection. **(null)** means the entry is not valid.
Received	
Bytes	This indicates the number of bytes received on this interface.

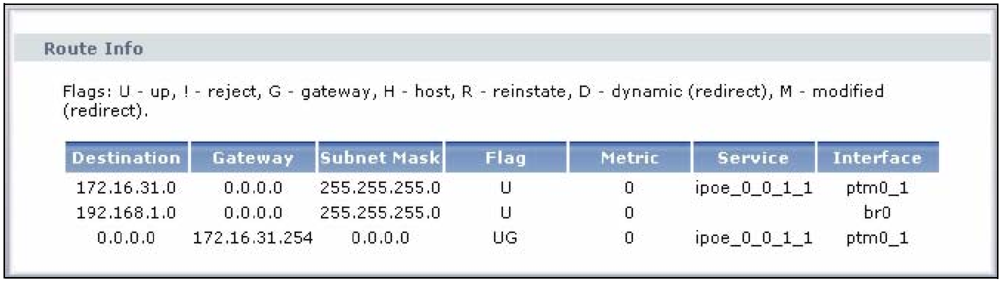
Table 5 Status > WAN Service Statistics (continued)

LABEL	DESCRIPTION
Pkts	This indicates the number of transmitted packets on this interface.
Errs	This indicates the number of frames with errors received on this interface.
Drops	This indicates the number of received packets dropped on this interface.
Transmitted	
Bytes	This indicates the number of bytes transmitted on this interface.
Pkts	This indicates the number of transmitted packets on this interface.
Errs	This indicates the number of frames with errors transmitted on this interface.
Drops	This indicates the number of outgoing packets dropped on this interface.
Refresh Interval	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the **Refresh Interval** field.
Stop	Click **Stop** to stop refreshing statistics.

4.1.2 Route Info

Routing is based on the destination address only and the ZyXEL Device takes the shortest path to forward a packet. Click **Status > Route Info** to access this screen. Use this screen to view the internal routing table on the ZyXEL Device.

Figure 22 Status > Route Info



Route Info

Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate, D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
172.16.31.0	0.0.0.0	255.255.255.0	U	0	ipoe_0_0_1_1	ptm0_1
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
0.0.0.0	172.16.31.254	0.0.0.0	UG	0	ipoe_0_0_1_1	ptm0_1

The following table describes the labels in this screen.

Table 6 Status > Route Info

LABEL	DESCRIPTION
Destination	This indicates the destination IP address of this route.
Gateway	This indicates the IP address of the gateway that helps forward this route’s traffic.
Subnet Mask	This indicates the destination subnet mask of this route.

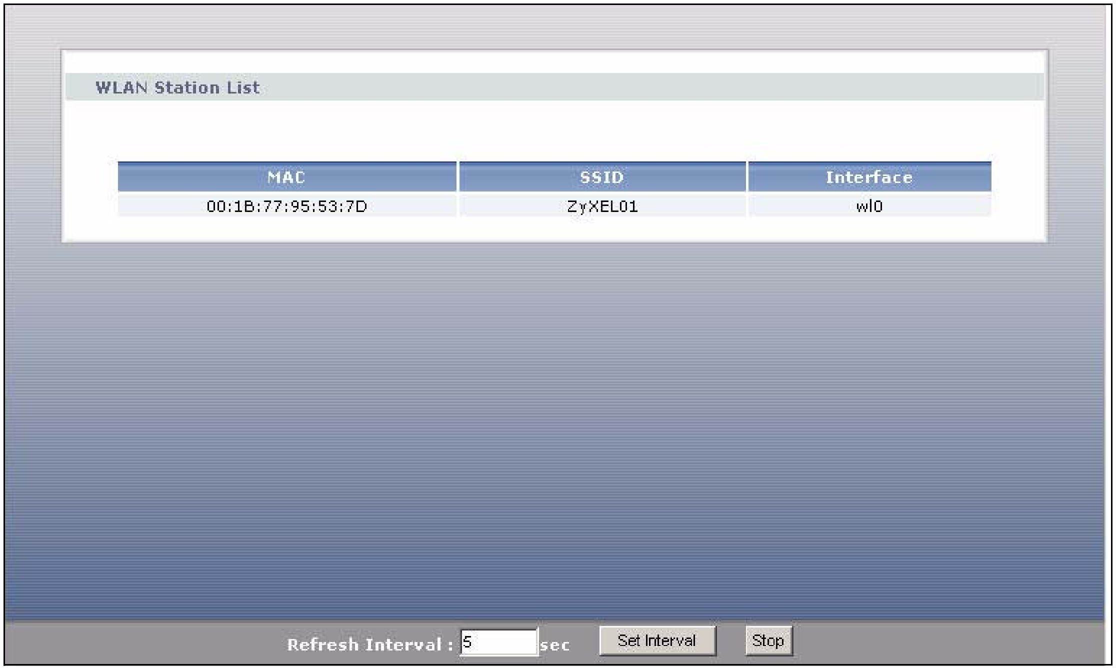
Table 6 Status > Route Info (continued)

LABEL	DESCRIPTION
Flag	This indicates the route status. **U**p: The route is up. **!**(Reject): The route is blocked and will force a route lookup to fail. **G**ateway: The route uses a gateway to forward traffic. **H**ost: The target of the route is a host. **R**einstate: The route is reinstated for dynamic routing. **D**ynamic (redirect): The route is dynamically installed by a routing daemon or redirect **M**odified (redirect): The route is modified from a routing daemon or redirect.
Metric	The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". The smaller the number, the lower the "cost".
Service	This indicates the name of the service used to forward the route.
Interface	This indicates the name of the interface through which the route is forwarded. • **br*** indicates the LAN interface. • **ptm*** indicates the VDSL WAN interface using IPoE or in bridge mode. • **atm*** indicates the ADSL WAN interface using IPoE or in bridge mode. • **pppoa*** indicates the ADSL WAN interface using PPPoA. • **ipoa*** indicates the ADSL WAN interface using IPoA.

4.1.3 WLAN Station List

Click **Status > WLAN Station List** to access this screen. Use this screen to view the wireless stations that are currently associated to the ZyXEL Device.

Figure 23 Status > WLAN Station List



WLAN Station List

MAC	SSID	Interface
00:1B:77:95:53:7D	ZyXEL01	wl0

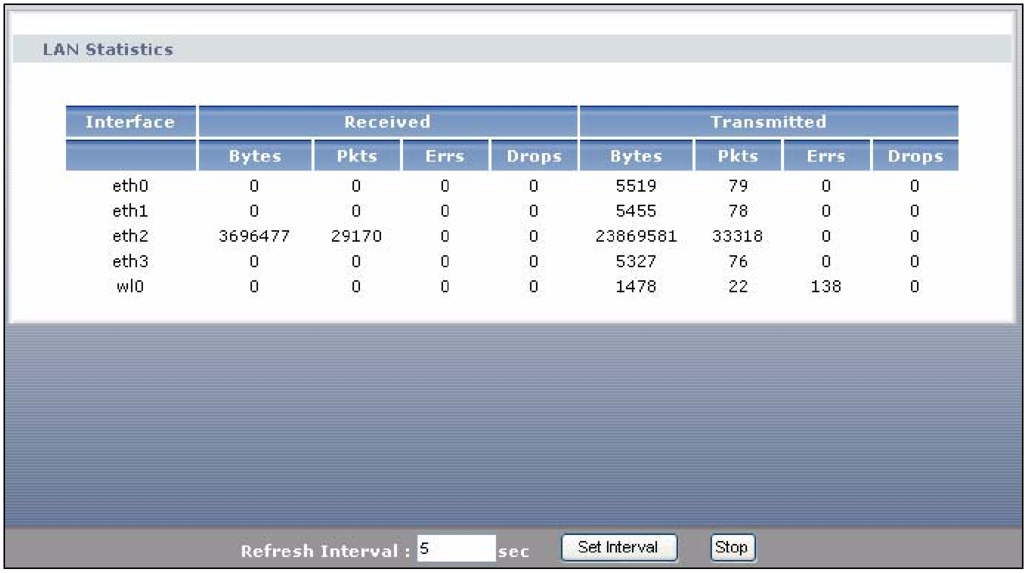
The following table describes the labels in this screen.

Table 7 Status > WLAN Station List

LABEL	DESCRIPTION
MAC	This field shows the MAC (Media Access Control) address of an associated wireless station.
SSID	This field shows the SSID to which the wireless station is connected.
Interface	This field shows the wireless interface to which the wireless station is connected.
Refresh Interval	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the **Refresh Interval** field.
Stop	Click **Stop** to stop refreshing statistics.

4.1.4 LAN Statistics

Click **Status > LAN Statistics** to access this screen. Use this screen to view the LAN statistics.



LAN Statistics

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth0	0	0	0	0	5519	79	0	0
eth1	0	0	0	0	5455	78	0	0
eth2	3696477	29170	0	0	23869581	33318	0	0
eth3	0	0	0	0	5327	76	0	0
wl0	0	0	0	0	1478	22	138	0

Refresh Interval : 5 sec

Figure 24 Status > LAN Statistics

The following table describes the labels in this screen.

Table 8 Status > LAN Statistics

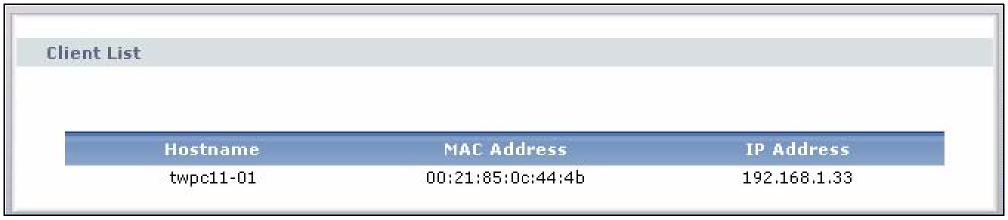
LABEL	DESCRIPTION
Interface	This shows the LAN or WLAN interface. **eth0~3** represent the physical Ethernet ports 1~ 4.
Received	
Bytes	This indicates the number of bytes received on this interface.
Pkts	This indicates the number of transmitted packets on this interface.
Errs	This indicates the number of frames with errors received on this interface.
Drops	This indicates the number of received packets dropped on this interface.
Transmitted	
Bytes	This indicates the number of bytes transmitted on this interface.
Pkts	This indicates the number of transmitted packets on this interface.
Errs	This indicates the number of frames with errors transmitted on this interface.
Drops	This indicates the number of outgoing packets dropped on this interface.
Refresh Interval	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the **Refresh Interval** field.
Stop	Click **Stop** to stop refreshing statistics.

4.1.5 Client List

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyXEL Device as a DHCP server or disable it. When configured as a server, the ZyXEL Device provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

Click **Status > Client List** to open the following screen. The read-only DHCP table shows current DHCP client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the ZyXEL Device's DHCP server.

Figure 25 Status > Client List



Client List

Hostname	MAC Address	IP Address
twpc11-01	00:21:85:0c:44:4b	192.168.1.33

The following table describes the labels in this screen.

Table 9 Status > Client List

LABEL	DESCRIPTION
Host Name	This indicates the computer host name.
MAC Address	Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. This indicates the MAC address of the client computer.
IP Address	This indicates the IP address assigned to this client computer.

PART II
Network

5

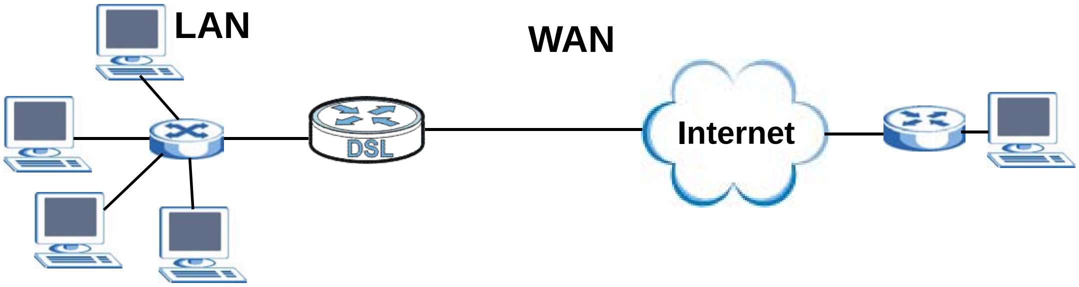
WAN Setup

5.1 Overview

This chapter discusses the ZyXEL Device's **WAN** screens. Use these screens to configure your ZyXEL Device for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks (such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

Figure 26 LAN and WAN



- See Section 5.6 on page 85 for advanced technical information on WAN.

5.1.1 What You Can Do in this Chapter

- The **Layer 2 Interface** screen lets you view, remove or add a layer-2 WAN interface (Section 5.4 on page 69).
- The **Internet Connection** screen lets you view and configure the WAN settings on the ZyXEL Device for Internet access (Section 5.5 on page 73).

5.2 What You Need to Know

Encapsulation Method

Encapsulation is used to include data from an upper layer protocol into a lower layer protocol. To set up a WAN connection to the Internet, you need to use the same encapsulation method used by your ISP (Internet Service Provider). If your ISP offers a dial-up Internet connection using PPPoE (PPP over Ethernet) or PPPoA, they should also provide a username and password (and service name) for user authentication.

WAN IP Address

The WAN IP address is an IP address for the ZyXEL Device, which makes it accessible from an outside network. It is used by the ZyXEL Device to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the ZyXEL Device tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es) (and a gateway IP address if you use the Ethernet or ENET ENCAP encapsulation method).

ATM

Asynchronous Transfer Mode (ATM) is a LAN and WAN networking technology that provides high-speed data transfer. ATM uses fixed-size packets of information called cells. With ATM, a high QoS (Quality of Service) can be guaranteed. ATM uses a connection-oriented model and establishes a virtual circuit (VC) between two endpoints before the actual data exchange begins.

PTM

Packet Transfer Mode (PTM) is packet-oriented and supported by the VDSL2 standard. In PTM, packets are encapsulated directly in the High-level Data Link Control (HDLC) frames. It is designed to provide a low-overhead, transparent way of transporting packets over DSL links, as an alternative to ATM.

5.3 Before You Begin

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

5.4 The Layer 2 Interface Screen

The ZyXEL Device must have a layer-2 interface to allow users to use the DSL port to access the Internet. The screen varies depending on the interface type you select.

Note: The ATM and PTM layer-2 interfaces cannot work at the same time.

Figure 27 Layer 2 Interface: PTM

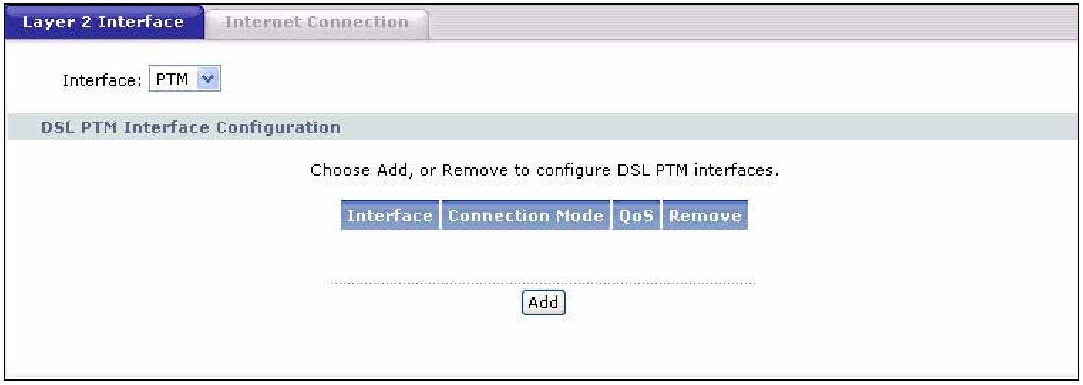
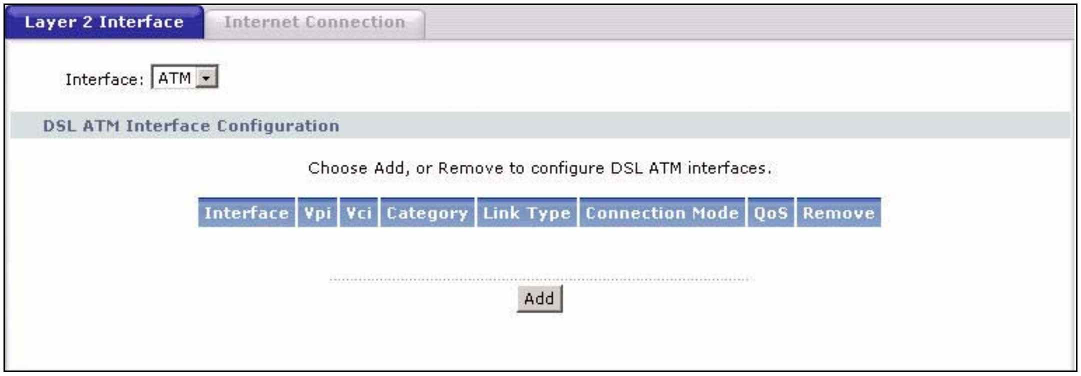


Figure 28 Layer 2 Interface: ATM



The following table describes the fields in this screen.

Table 10 Layer 2 Interface

LABEL	DESCRIPTION
Interface	Select an interface for which you want to configure here. **PTM**: The ZyXEL Device uses the VDSL technology for data transmission over the DSL port. **ATM**: The ZyXEL Device uses the ADSL technology for data transmission over the DSL port.
Interface	This is the name of the interface.
Vpi	This is the Virtual Path Identifier (VPI).
Vci	This is the Virtual Channel Identifier (VCI).
Category	This is the ATM traffic class.
Link Type	This is the DSL link type of the ATM layer-2 interface.

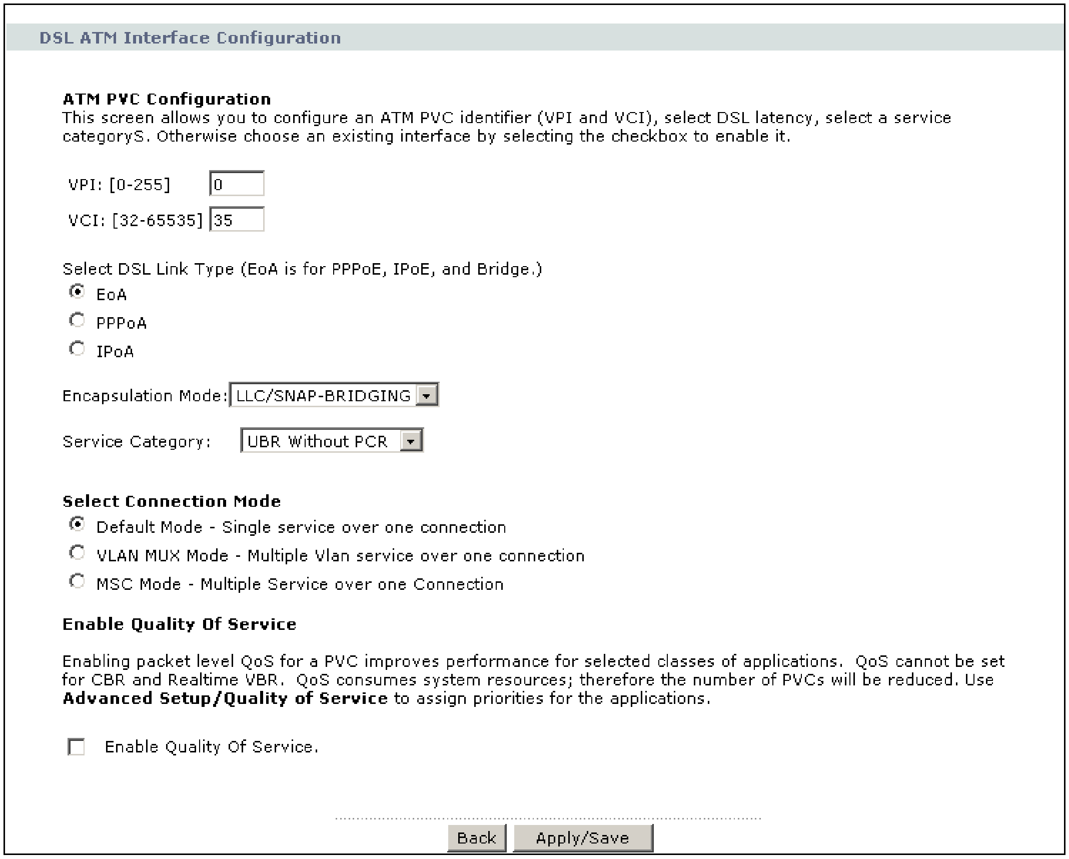
Table 10 Layer 2 Interface (continued)

LABEL	DESCRIPTION
Connection Mode	This shows the connection mode of the layer-2 interface.
QoS	This shows whether QoS (Quality of Service) is enabled on the ZyXEL Device.
Remove	Click the **Remove** button to delete this interface from the ZyXEL Device. A window displays asking you to confirm that you want to delete the interface. You cannot remove the layer-2 interface when a WAN service is associated with it.
Add	Click this button to create a new layer-2 interface.

5.4.1 Layer 2 Interface Configuration

Click the **Add** button in the **Layer 2 Interface** screen to open the following screen. Use this screen to create a new layer-2 interface. At the time of writing, you can configure only one PTM interface on the ZyXEL Device. You can have multiple ATM layer-2 interfaces using different VPI and/or VCI values. The screen varies depending on the interface type you select.

Figure 29 DSL ATM Interface Configuration



DSL ATM Interface Configuration

ATM PVC Configuration
This screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service categoryS. Otherwise choose an existing interface by selecting the checkbox to enable it.

VPI: [0-255] 0
VCI: [32-65535] 35

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)
● EoA
○ PPPoA
○ IPoA

Encapsulation Mode: LLC/SNAP-BRIDGING

Service Category: UBR Without PCR

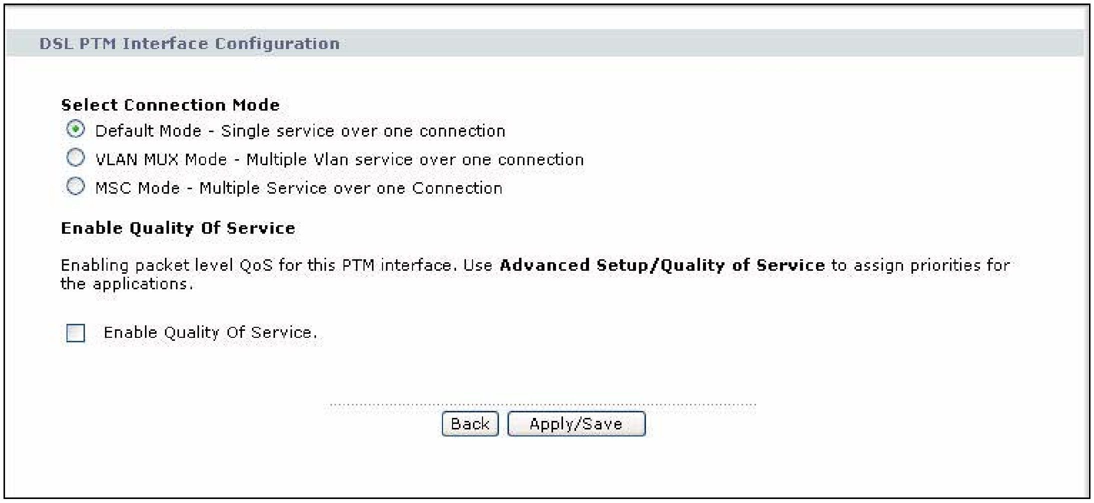
Select Connection Mode
● Default Mode - Single service over one connection
○ VLAN MUX Mode - Multiple Vlan service over one connection
○ MSC Mode - Multiple Service over one Connection

Enable Quality Of Service

Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

□ Enable Quality Of Service.

Figure 30 DSL PTM Interface Configuration



DSL PTM Interface Configuration

Select Connection Mode
● Default Mode - Single service over one connection
○ VLAN MUX Mode - Multiple Vlan service over one connection
○ MSC Mode - Multiple Service over one Connection

Enable Quality Of Service

Enabling packet level QoS for this PTM interface. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

□ Enable Quality Of Service.

The following table describes the fields in this screen.

Table 11 DSL PTM Interface Configuration

LABEL	DESCRIPTION
ATM PVC Configuration	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. This section is available only when you configure an ATM layer-2 interface.
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.
Select DSL Link Type	Select **EoA** (Ethernet over ATM) to have an Ethernet header in the packet, so that you can have multiple services/connections over one PVC. You can set each connection to have its own MAC address or all connections share one MAC address but use different VLAN IDs for different services. **EoA** supports ENET ENCAP (IPoE), PPPoE and RFC1483/2684 bridging encapsulation methods. Select **PPPoA** (PPP over ATM) to allow just one PPPoA connection over a PVC. Select **IPoA** (IP over ATM) to allow just one RFC 1483 routing connection over a PVC.
Encapsulation Mode	Select the method of multiplexing used by your ISP from the drop-down list. Choices are: • **VC/MUX:** In VC multiplexing, each protocol is carried on a single ATM virtual circuit (VC). To transport multiple protocols, the ZyXEL Device needs separate VCs. There is a binding between a VC and the type of the network protocol carried on the VC. This reduces payload overhead since there is no need to carry protocol information in each Protocol Data Unit (PDU) payload. • **LLC/SNAP-BRIDGING**: In LCC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header. This is available only when you select **EoA** in the **Select DSL Link Type** field. • **LLC/ENCAPSULATION**: More than one protocol can be carried over the same VC. This is available only when you select **PPPoA** in the **Select DSL Link Type** field. • **LLC/SNAP-ROUTING**: In LCC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header. This is available only when you select **EoA** in the **Select DSL Link Type** field.
Service Category	Select **UBR Without PCR** or **UBR With PCR** for applications that are non-time sensitive, such as e-mail. Select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **Realtime VBR** (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation. Select **Non Realtime VBR** (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation.

Table 11 DSL PTM Interface Configuration (continued)

LABEL	DESCRIPTION
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here. This field is not available when you select **UBR Without PCR**.
Sustainable Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec. This field is available only when you select **Non Realtime VBR** or **Realtime VBR**.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535. This field is available only when you select **Non Realtime VBR** or **Realtime VBR**.
Select Connection Mode	Select **Default Mode** to allow only one WAN service over a single virtual circuit. Select **VLAN MUX Mode** to allow multiplexing of multiple protocols over a single virtual circuit. You need to assign a VLAN ID and priority level to traffic through each WAN connection. All WAN connections share one MAC address. Select **MSC Mode** to allow multiple WAN services over a single virtual circuit. Each WAN connection has its own MAC address. This field is not available if you select **PPPoA** or **IPoA** as the DSL link type. The ZyXEL Device uses **Default Mode** automatically for **PPPoA** or **IPoA**.
Enable Quality Of Service	Select this option to activate QoS (Quality of Service) on this interface to group and prioritize traffic. Traffic is grouped according to the VLAN group. This field is not available when you select **CBR** or **Realtime VBR**.
Back	Click this button to return to the previous screen without saving any changes.
Apply/Save	Click this button to save your changes and go back to the previous screen.

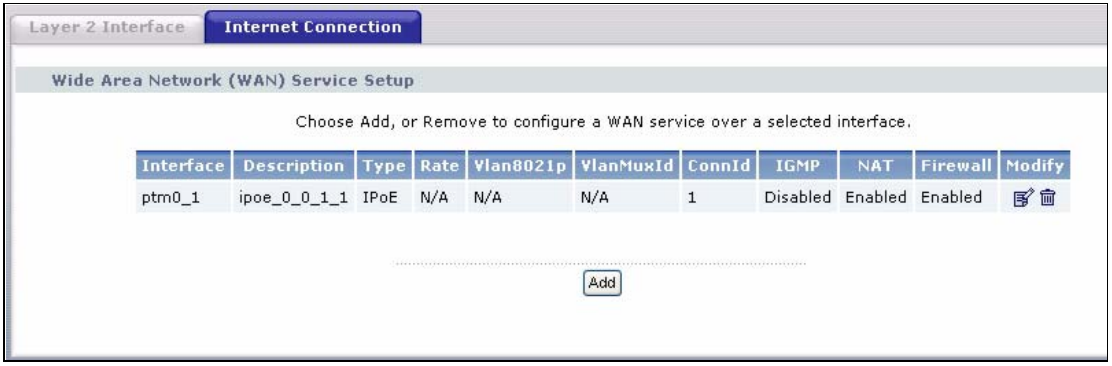
5.5 The Internet Connection Screen

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

To use NAT, firewall or IGMP proxy in the ZyXEL Device, you need to configure a WAN connection with PPPoE or IPoE.

Note: When a layer-2 interface is in **VLAN MUX Mode** or **MSC Mode**, you can configure up to eight WAN services for each interface.

Figure 31 Internet Connection



Choose Add, or Remove to configure a WAN service over a selected interface.

Interface	Description	Type	Rate	Vlan8021p	VlanMuxId	ConnId	IGMP	NAT	Firewall	Modify
ptm0_1	ipoe_0_0_1_1	IPoE	N/A	N/A	N/A	1	Disabled	Enabled	Enabled	

The following table describes the labels in this screen.

Table 12 Internet Connection

LABEL	DESCRIPTION
Interface	This shows the name of the interface used by this connection. A default name **ipoa***, **pppoa***, **atm*** or **ptm*** indicates DSL port. The **pppx** name (where x starts from 0 and is the index number of PPP connection on the ZyXEL Device) indicates a PPP connection via any one of the WAN interface. The number after the dot (**.**) represents the VLAN ID number assigned to traffic sent through this connection. The number after the underscore (_) represents the index number of connections through the same interface. **(null)** means the entry is not valid.
Description	This is the service name of this connection. **0** and **35** or **0** and **1** are the default VPI and VCI numbers. The last number represents the index number of connections over the same PVC or the VLAN ID number assigned to traffic sent through this connection. **(null)** means the entry is not valid.
Type	This shows the method of encapsulation used by this connection.
Rate	This shows the maximum data rate (in Kbps) allowed for traffic sent through this connection. This displays **N/A** when there is no limit on transmission rate.
Vlan8021p	This indicates the 802.1P priority level assigned to traffic sent through this connection. This displays **N/A** when there is no priority level assigned.
VlanMuxId	This indicates the VLAN ID number assigned to traffic sent through this connection. This displays **N/A** when there is no VLAN ID number assigned.
ConnId	This shows the index number of each connection. This displays **N/A** when the interface used by the connection is in **Default Mode**.

Table 12 Internet Connection

LABEL	DESCRIPTION
IGMP	This shows whether IGMP (Internet Group Multicast Protocol) is activated or not for this connection. IGMP is not available when the connection uses the bridging service.
NAT	This shows whether NAT is activated or not for this interface. NAT is not available when the connection uses the bridging service.
Firewall	This shows whether the firewall is activated or not for this connection. The firewall is not available when the connection uses the bridging service.
Modify	Click the **Edit** icon to configure the WAN connection. Click the **Remove** icon to delete the WAN connection.
Add	Click **Add** to create a new connection.

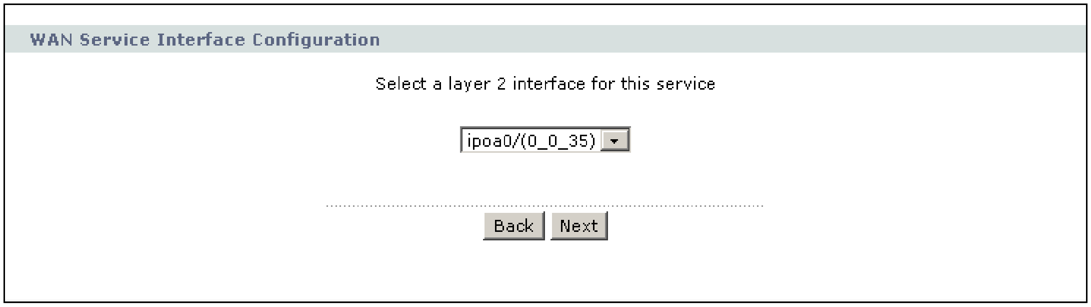
5.5.1 WAN Connection Configuration

Click the **Edit** or **Add** button in the **WAN Service** screen to configure a WAN connection.

5.5.1.1 WAN Interface

This screen displays when you add a new WAN connection.

Figure 32 WAN Configuration: WAN Interface



WAN Service Interface Configuration

Select a layer 2 interface for this service

ipoa0/(0_0_35)

The following table describes the labels in this screen.

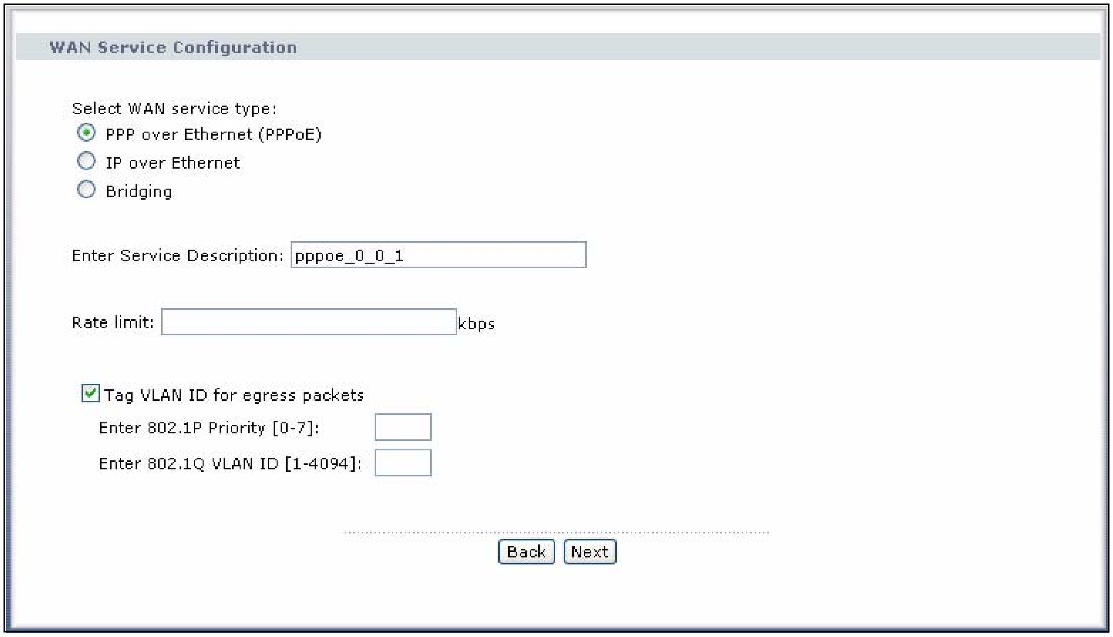
Table 13 WAN Configuration: WAN Interface

LABEL	DESCRIPTION
Select a layer 2 interface for this service	Select **ptm0** to use the DSL port as the WAN port and use the VDSL technology for data transmission. Select **atm0** to use the DSL port as the WAN port and use the ADSL technology for data transmission.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

5.5.1.2 Service Type

If you set the DSL link type to **PPPoA** or **IPoA** for the ATM interface and configure a WAN connection using the ATM interface, you only need to configure the **Enter Service Description** field in this screen.

Figure 33 WAN Configuration: Service Type



WAN Service Configuration

Select WAN service type:

● PPP over Ethernet (PPPoE)
○ IP over Ethernet
○ Bridging

Enter Service Description: pppoe_0_0_1

Rate limit: kbps

☑ Tag VLAN ID for egress packets

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [1-4094]:

Figure 34 The following table describes the labels in this screen.

Table 14 WAN Configuration: Service Type

LABEL	DESCRIPTION
Select WAN service type	Select the method of encapsulation used by your ISP. Choices are **PPP over Ethernet (PPPoE)**, **IP over Ethernet** and **Bridging**.
Enter Service Description	Specify a name for this connection or use the automatically generated one.
Rate Limit	Enter the maximum transmission rate in Kbps for traffic sent through the WAN connection. Otherwise, leave this field blank to disable the rate limit. This field is not available for an ATM connection if QoS is disabled in the DSL ATM Interface Configuration.
Tag VLAN ID for egress packets	Select this option to add the VLAN tag (specified below) to the outgoing traffic through this connection. This field is available when the layer-2 interface is in **VLANMUX** mode.
Enter 802.1P Priority	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Type the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level. This field is available when the layer-2 interface is in **VLANMUX** mode.

Table 14 WAN Configuration: Service Type

LABEL	DESCRIPTION
Enter 802.1Q VLAN ID	Type the VLAN ID number (from 1 to 4094) for traffic through this connection. This field is available when the PTM interface is in **VLANMUX** mode.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

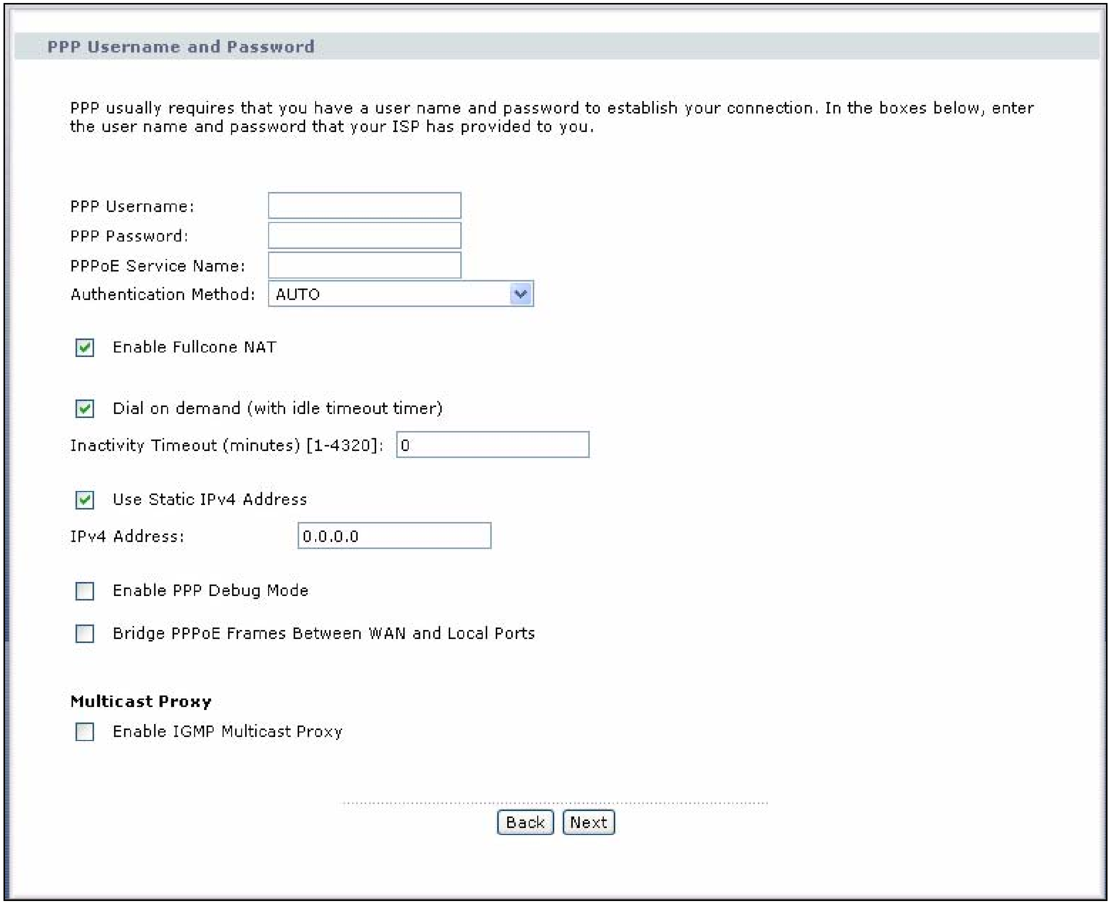
5.5.1.3 WAN IP Address and DNS Server

The screen differs by the encapsulation you selected in the previous screen. See Section 5.6 on page 85 for more information.

PPPoE or PPPoA

This screen displays when you select **PPP over Ethernet (PPPoE)** in the **WAN Service Configuration** screen or set the DSL link type to **PPPoA** for the ATM interface and configure a WAN connection using the ATM interface.

Figure 35 WAN Configuration: PPPoE



PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method: AUTO

☑ Enable Fullcone NAT

☑ Dial on demand (with idle timeout timer)

Inactivity Timeout (minutes) [1-4320]: 0

☑ Use Static IPv4 Address

IPv4 Address: 0.0.0.0

□ Enable PPP Debug Mode

□ Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

□ Enable IGMP Multicast Proxy

The following table describes the labels in this screen.

Table 15 WAN Configuration: PPPoE or PPPoA

LABEL	DESCRIPTION
PPP User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
PPP Password	Enter the password associated with the user name above.
PPPoE Service Name	Type the name of your PPPoE service here. This field is not available for a PPPoA connection.
Authentication Method	The ZyXEL Device supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms. Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **AUTO** - Your ZyXEL Device accepts either CHAP or PAP when requested by this remote node. **PAP** - Your ZyXEL Device accepts PAP only. **CHAP** - Your ZyXEL Device accepts CHAP only. **MSCHAP** - Your ZyXEL Device accepts MSCHAP only. MS-CHAP is the Microsoft version of the CHAP.
Enable Fullcone NAT	Select this option to enable full cone NAT on the ZyXEL Device.
Dial on Demand	Select this check box when you do not want the connection up all the time and specify an idle time-out in the **Inactivity Timeout** field.
Inactivity Timeout	Specify an idle time-out when you select **Dial on Demand**. The default setting is 0, which means the Internet session will not timeout.
Use Static IPv4 Address	A static IPv4 address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you do not have a dynamic IP address.
IPv4 Address	Enter the static IP address provided by your ISP.
Enable PPP Debug Mode	Select this option to display PPP debugging messages on the console.

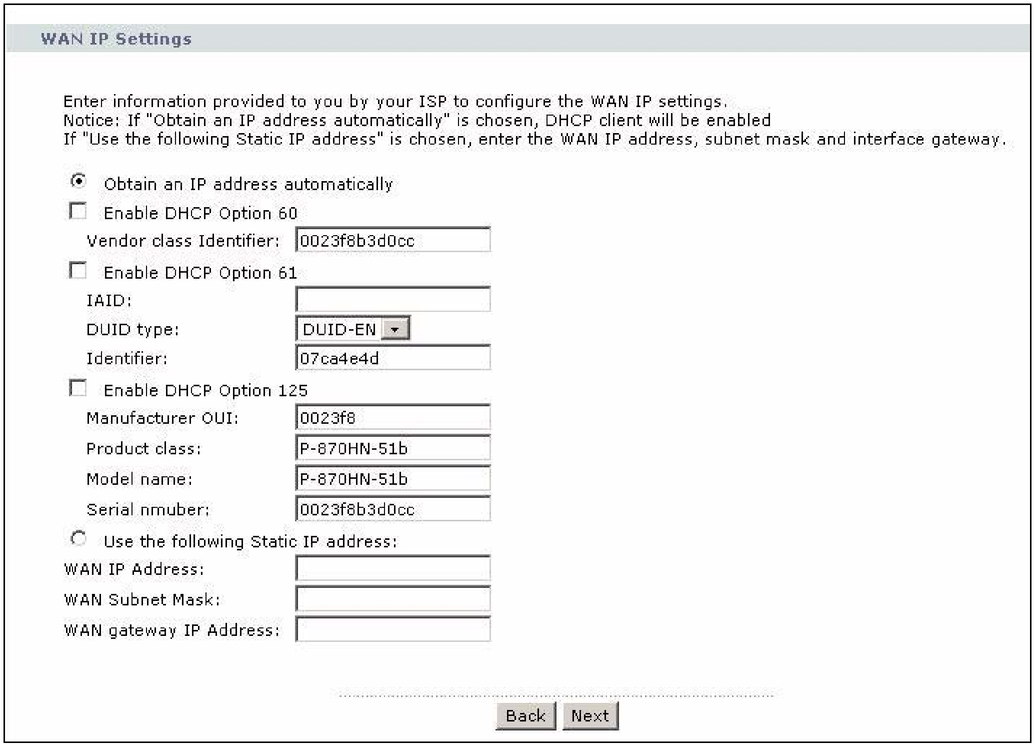
Table 15 WAN Configuration: PPPoE or PPPoA

LABEL	DESCRIPTION
Bridge PPPoE Frames Between WAN and Local Ports	Select this option to forward PPPoE packets from the WAN port to the LAN ports and from the LAN ports to the WAN port. In addition to the ZyXEL Device's built-in PPPoE client, you can select this 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. This is an alternative to NAT for application where NAT is not appropriate. Clear this if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP. This field is not available for a PPPoA connection.
Enable IGMP Multicast Proxy	Select this check box to have the ZyXEL Device act as an IGMP proxy on this connection. This allows the ZyXEL Device to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

IPoE

This screen displays when you select **IP over Ethernet** in the **WAN Service Configuration** screen.

Figure 36 WAN Configuration: IPoE



WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: If "Obtain an IP address automatically" is chosen, DHCP client will be enabled
If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.

● Obtain an IP address automatically

□ Enable DHCP Option 60

Vendor class Identifier: 0023f8b3d0cc

□ Enable DHCP Option 61

IAID:
DUID type: DUID-EN
Identifier: 07ca4e4d

□ Enable DHCP Option 125

Manufacturer OUI: 0023f8
Product class: P-870HN-51b
Model name: P-870HN-51b
Serial nmuber: 0023f8b3d0cc

○ Use the following Static IP address:

WAN IP Address:
WAN Subnet Mask:
WAN gateway IP Address:

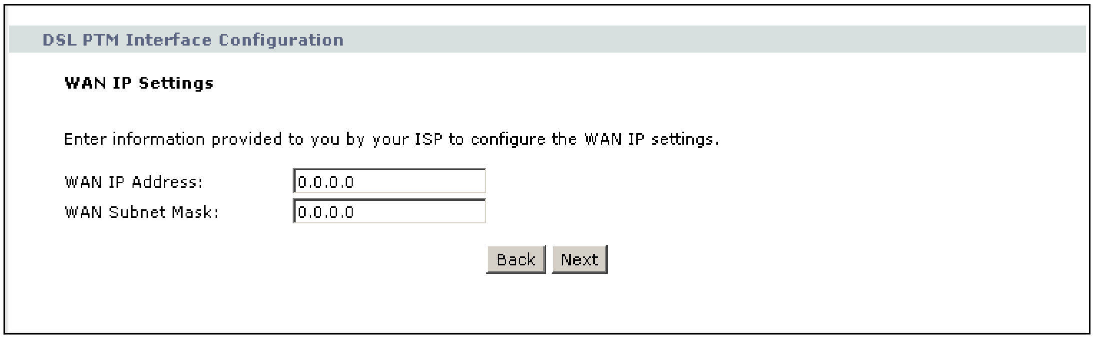
The following table describes the labels in this screen.

Table 16 WAN Configuration: IPoE

LABEL	DESCRIPTION
Obtain an IP address automatically	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you have a dynamic IP address.
Enable DHCP Option 60	Select this to identify the vendor and functionality of the ZyXEL Device in DHCP requests that the ZyXEL Device sends to a DHCP server when getting a WAN IP address.
Vendor Class Identifier	Enter the Vendor Class Identifier (Option 60), such as the type of the hardware or firmware.
Enable DHCP Option 61	Select this to identify the ZyXEL Device in DHCP requests that the ZyXEL Device sends to a DHCP server when getting a WAN IP address.
IAID	Enter the Identity Association Identifier (IAID) of the ZyXEL Device. For example, the WAN connection index number.
DUID Type	Select **Other** to enter any string that identifies the ZyXEL Device in the **DUID** field. Select **DUID-LL** (DUID Based on Link-layer Address) to enter the ZyXEL Device's hardware address, that is the MAC address in the **DUID** field. Select **DUID-EN** (DUID Assigned by Vendor Based on Enterprise Number) to enter the vendor's registered private enterprise number.
Identifier	Enter a unique identifier assigned by the vendor. This field is available when you select **DUID-EN** in the **DUID Type** field.
Enable DHCP Option 125	Select this to add vendor specific information to DHCP requests that the ZyXEL Device sends to a DHCP server when getting a WAN IP address.
Manufacturer OUI	Specify the vendor's OUI (Organization Unique Identifier). It is usually the first three bytes of the MAC address.
Product Class	Enter the product class of the ZyXEL Device.
Model Name	Enter the model name of the ZyXEL Device.
Serial Number	Enter the serial number of the ZyXEL Device.
Use the following Static IP address	Select this if you have a static IP address.
WAN IP Address	Enter the static IP address provided by your ISP.
WAN Subnet Mask	Enter the subnet mask provided by your ISP.
WAN gateway IP Address	Enter the gateway IP address provided by your ISP.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

IPoA

Figure 37 This screen displays only when you set the DSL link type to **IPoA** for the ATM interface and configure a WAN connection using the ATM interface.



DSL PTM Interface Configuration

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.

WAN IP Address: 0.0.0.0

WAN Subnet Mask: 0.0.0.0

The following table describes the labels in this screen.

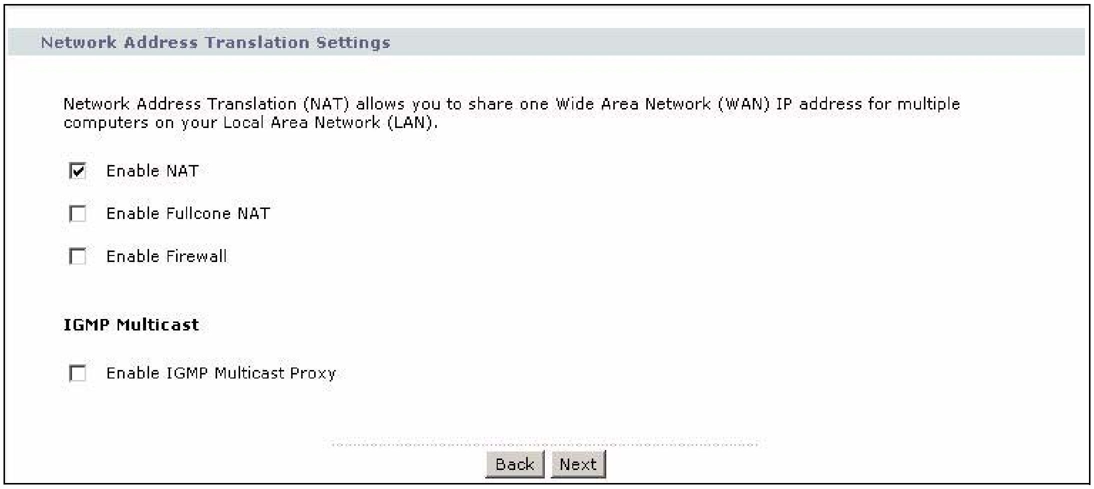
Table 17 WAN Configuration: IPoA

LABEL	DESCRIPTION
WAN IP Address	Enter the static IP address provided by your ISP.
WAN Subnet Mask	Enter the subnet mask provided by your ISP.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

5.5.1.4 NAT, IGMP Multicast and Firewall Activation

The screen is available only when you select **IP over Ethernet** in the **WAN Service Configuration** screen or set the DSL link type to **IPoA** for the ATM interface and configure a WAN connection using the ATM interface.

Figure 38 WAN Configuration: NAT, IGMP Multicast and Firewall Activation: IPoE/ IPoA



Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

☑ Enable NAT

□ Enable Fullcone NAT

□ Enable Firewall

IGMP Multicast

□ Enable IGMP Multicast Proxy

The following table describes the labels in this screen.

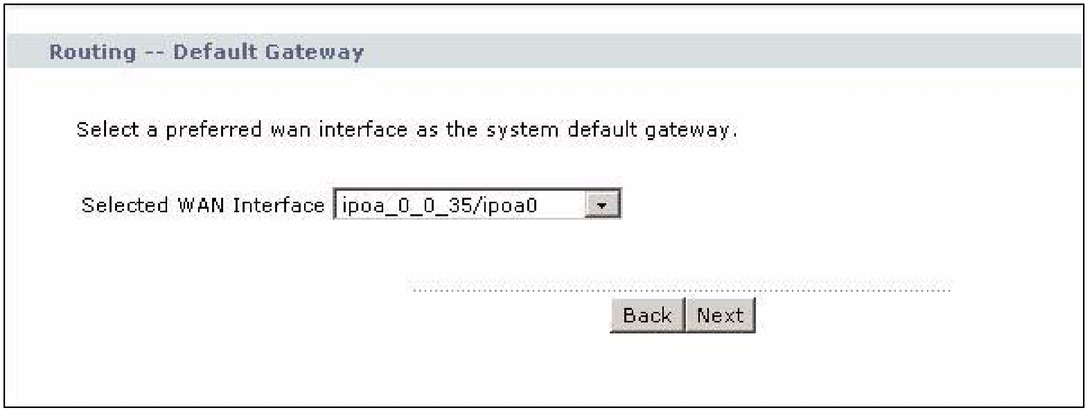
Table 18 WAN Configuration: NAT, IGMP Multicast and Firewall Activation: IPoE

LABEL	DESCRIPTION
Enable NAT	Select this check box to activate NAT on this connection.
Enable Fullcone NAT	Select this check box to activate full cone NAT on this connection. This field is available only when you select **Enable NAT**.
Enable Firewall	Select this check box to activate Firewall on this connection.
Enable IGMP Multicast Proxy	Select this check box to have the ZyXEL Device act as an IGMP proxy on this connection. This allows the ZyXEL Device to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

5.5.1.5 Default Gateway

The screen is not available when you select **Bridging** in the **WAN Service Configuration** screen.

Figure 39 WAN Configuration: Default Gateway: PPPoE, PPPoA, IPoE or IPoA



Routing -- Default Gateway

Select a preferred wan interface as the system default gateway.

Selected WAN Interface: ipoa_0_0_35/ipoa0

The following table describes the labels in this screen.

Table 19 WAN Configuration: Default Gateway: PPPoE or IPoE

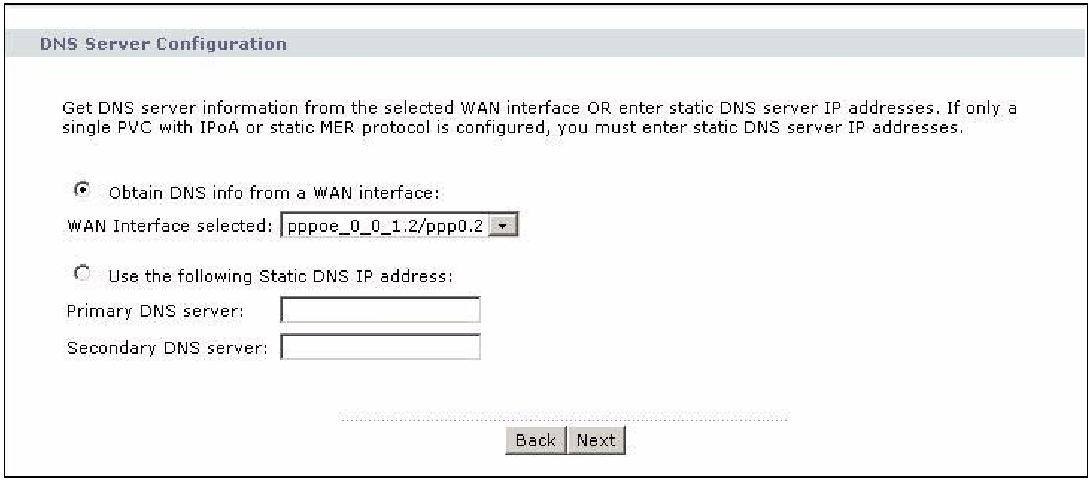
LABEL	DESCRIPTION
Selected WAN Interface	Select a WAN interface through which you want to forward the traffic.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

5.5.1.6 DNS Server

The screen is not available when you select **Bridging** in the **WAN Service Configuration** screen.

Note: If you configure only one IPoA or IPoE connection using the ATM interface on the ZyXEL Device, you must enter the static DNS server address.

Figure 40 WAN Configuration: DNS Server: PPPoE, PPPoA, IPoE or IPoA



DNS Server Configuration

Get DNS server information from the selected WAN interface OR enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.

● Obtain DNS info from a WAN interface:

WAN Interface selected: pppoe_0_0_1.2/ppp0.2

○ Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

The following table describes the labels in this screen.

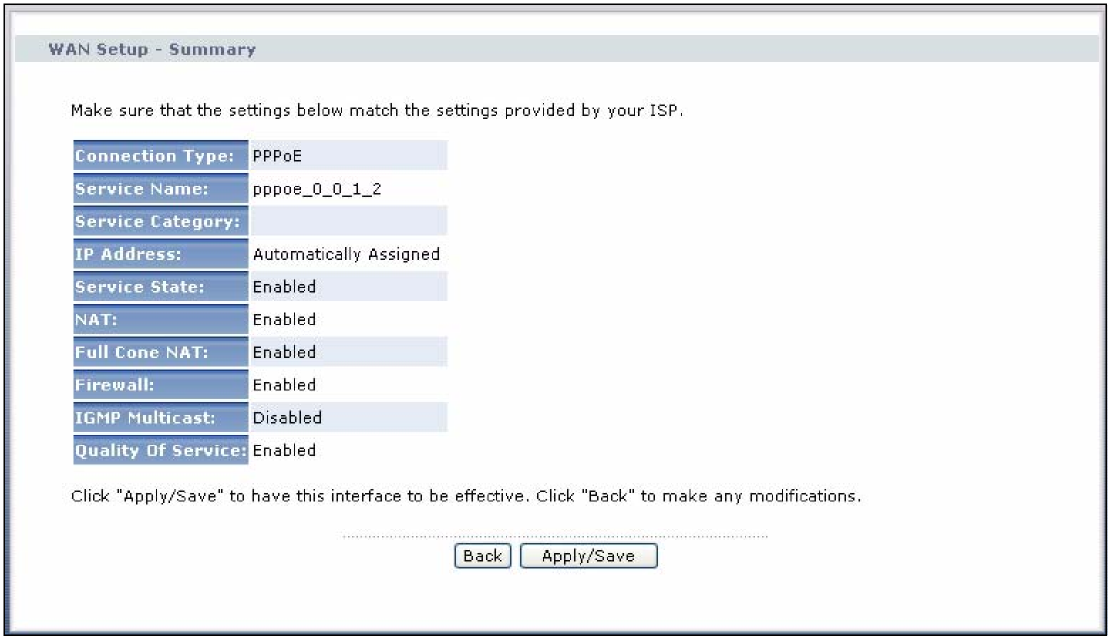
Table 20 WAN Configuration: DNS Server: PPPoE or IPoE

LABEL	DESCRIPTION
Obtain DNS info from a WAN interface	Select this to have the ZyXEL Device get the DNS server addresses from the ISP automatically.
WAN interface selected	This displays the WAN interface you selected in the previous screen.
Use the following Static DNS IP address	Select this to have the ZyXEL Device use the DNS server addresses you configure manually.
Primary DNS server	Enter the first DNS server address assigned by the ISP.
Secondary DNS server	Enter the second DNS server address assigned by the ISP.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

5.5.1.7 Configuration Summary

This read-only screen shows the current WAN connection settings.

Figure 41 WAN Configuration: Configuration Summary



WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	PPPoE
Service Name:	pppoe_0_0_1_2
Service Category:	
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Full Cone NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

The following table describes the labels in this screen.

Table 21 WAN Configuration: Configuration Summary

LABEL	DESCRIPTION
Connection Type	This is the encapsulation method used by this connection.
Service Name	This is the name of the service.
Service Category	This is the ATM traffic class. This field is blank for a PTM or Ethernet WAN connection.
IP Address	This shows whether the WAN IP address is assigned by the ISP, manually configured or not configurable.
Service State	This shows whether this service is active or not.
NAT	This shows whether NAT is active or not for this connection.
Full Cone NAT	This shows whether full cone NAT is active or not for this connection.
Firewall	This shows whether Firewall is active or not for this connection.
IGMP Multicast	This shows whether IGMP multicasting is active or not for this connection.
Quality Of Service	This shows whether QoS is active or not for this connection.
Back	Click this button to return to the previous screen.
Apply/Save	Click this button to save your changes.

5.6 Technical Reference

The following section contains additional technical information about the ZyXEL Device features described in this chapter.

Encapsulation

Be sure to use the encapsulation method required by your ISP. The ZyXEL Device can work in bridge mode or routing mode. When the ZyXEL Device is in routing mode, it supports the following methods.

IP over Ethernet

IP over Ethernet (IPoE) is an alternative to PPPoE. IP packets are being delivered across an Ethernet network, without using PPP encapsulation. They 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 Ethernet cells.

ENET ENCAP

The MAC Encapsulated Routing Link Protocol (ENET ENCAP) is only implemented with the IP network protocol. IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. For instance, it encapsulates routed Ethernet frames into bridged ATM cells.

PPP over Ethernet

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

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

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

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

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

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.

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 RFC 1483 for more detailed information.

Multiplexing

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

VC-based Multiplexing

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

LLC-based Multiplexing

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

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.

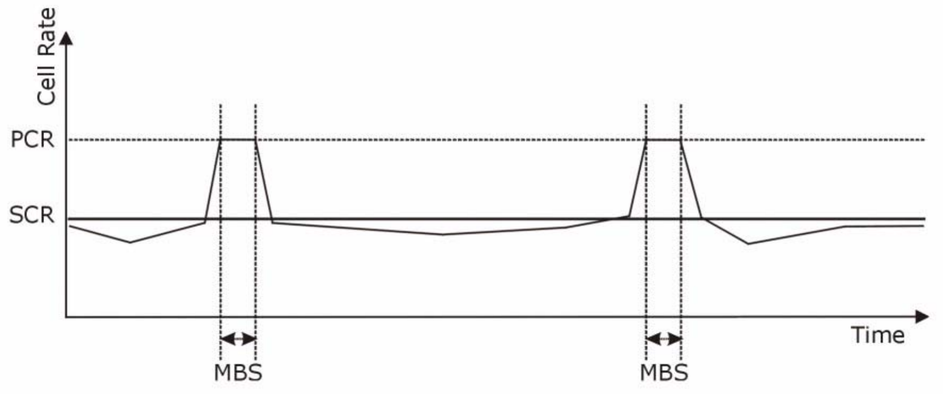
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

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 42 Example of Traffic Shaping



ATM Traffic Classes

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

Constant Bit Rate (CBR)

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

Variable Bit Rate (VBR)

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

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

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

Unspecified Bit Rate (UBR)

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

IP Address Assignment

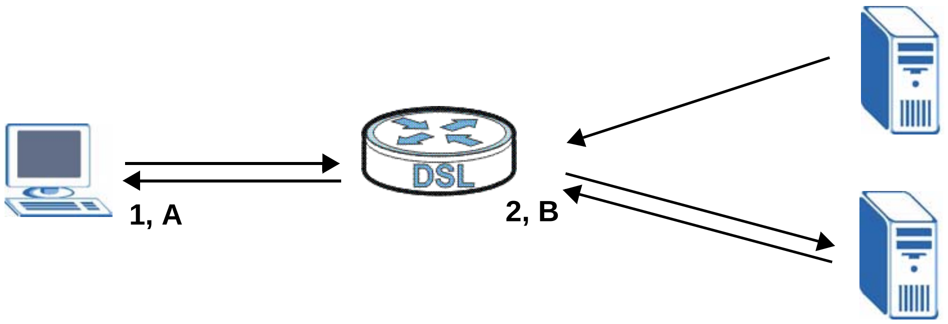
A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP address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

Full Cone NAT

In full cone NAT, the NAT router maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. The NAT router also maps packets coming to that external IP address and port to the internal IP address and port.

In the following example, the ZyXEL Device maps the source address of all packets sent from the internal IP address **1** and port **A** to IP address **2** and port **B** on the external network. The ZyXEL Device also performs NAT on all incoming packets sent to IP address **2** and port **B** and forwards them to IP address **1**, port **A**.

Figure 43 Full Cone NAT Example



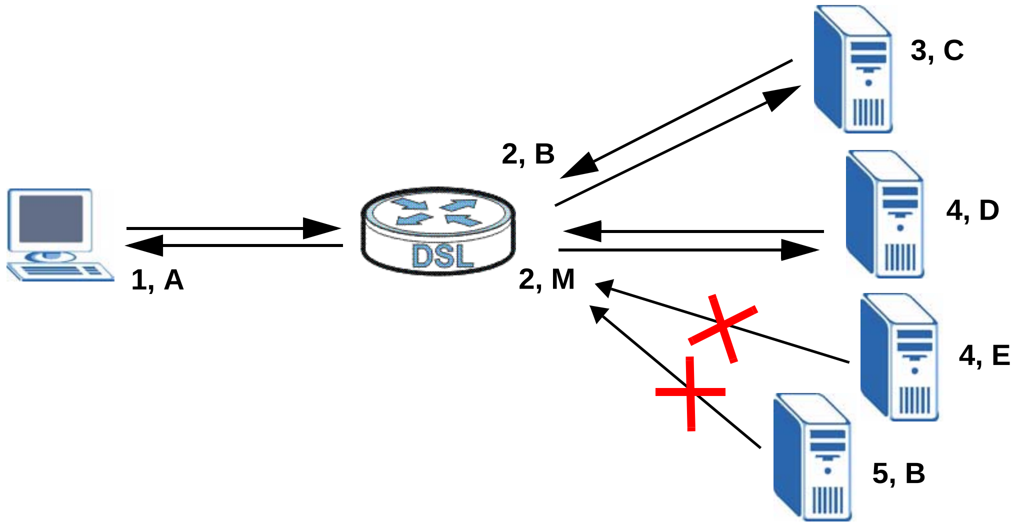
Symmetric NAT

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

In the following example, the ZyXEL Device maps the source address IP address **1** and port **A** to IP address **2** and port **B** on the external network for packets sent to IP address **3** and port **C**. The ZyXEL Device uses a different mapping (IP address **2** and port **M**) for packets sent to IP address **4** and port **D**.

A host on the external network (IP address **3** and port **C** for example) can only send packets to the internal host via the external IP address and port that the NAT router used in sending a packet to the external host's IP address and port. So in the example, only **3, C** is allowed to send packets to **2, B** and only **4, D** is allowed to send packets to **2, M**.

Figure 44 Symmetric NAT



Introduction to VLANs

A Virtual Local Area Network (VLAN) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In Multi-Tenant Unit (MTU) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

Introduction to IEEE 802.1Q Tagged VLAN

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier), residing within the type/ length field of the Ethernet frame) and two bytes of TCI (Tag Control Information), starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID	User Priority	CFI	VLAN ID
2 Bytes	3 Bits	1 Bit	12 Bits

Multicast

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

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

At start up, the ZyXEL Device queries all directly connected networks to gather group membership. After that, the ZyXEL Device periodically updates this information.

DNS Server Address Assignment

Use Domain Name System (DNS) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is

204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The ZyXEL Device can get the DNS server addresses in the following ways.

1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.

2 If your ISP dynamically assigns the DNS server IP addresses (along with the ZyXEL Device's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

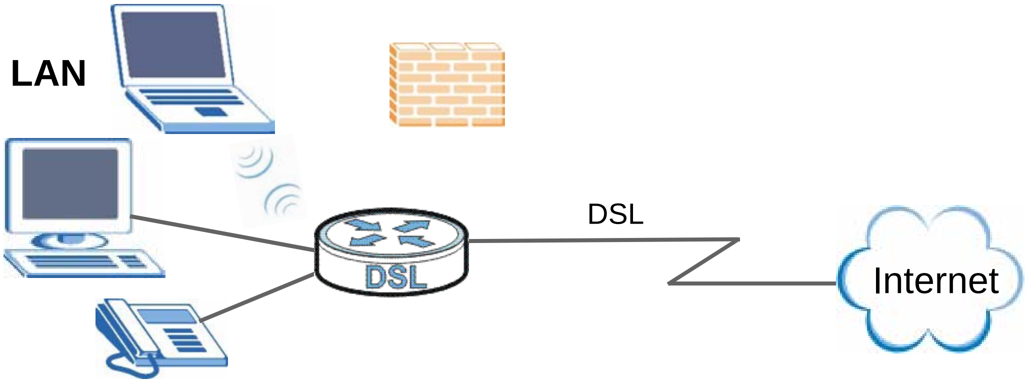
6

LAN Setup

6.1 Overview

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is usually located in one immediate area such as a building or floor of a building.

The LAN screens can help you configure a LAN DHCP server and manage IP addresses.



- See Section 6.4 on page 97 for more information on LANs.
- See Appendix D on page 313 for more information on IP addresses and subnetting.

6.1.1 What You Can Do in this Chapter

The **LAN IP** screen lets you set the LAN IP address and subnet mask of your ZyXEL device and configure other LAN TCP/IP settings (Section 6.3 on page 95).

6.2 What You Need To Know

IP Address

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

Subnet Mask

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

DHCP

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

DHCP Relay

You can also configure the ZyXEL Device to relay client DHCP requests to a DHCP server and the server’s responses back to the clients.

RIP

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers.

Multicast and IGMP

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

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

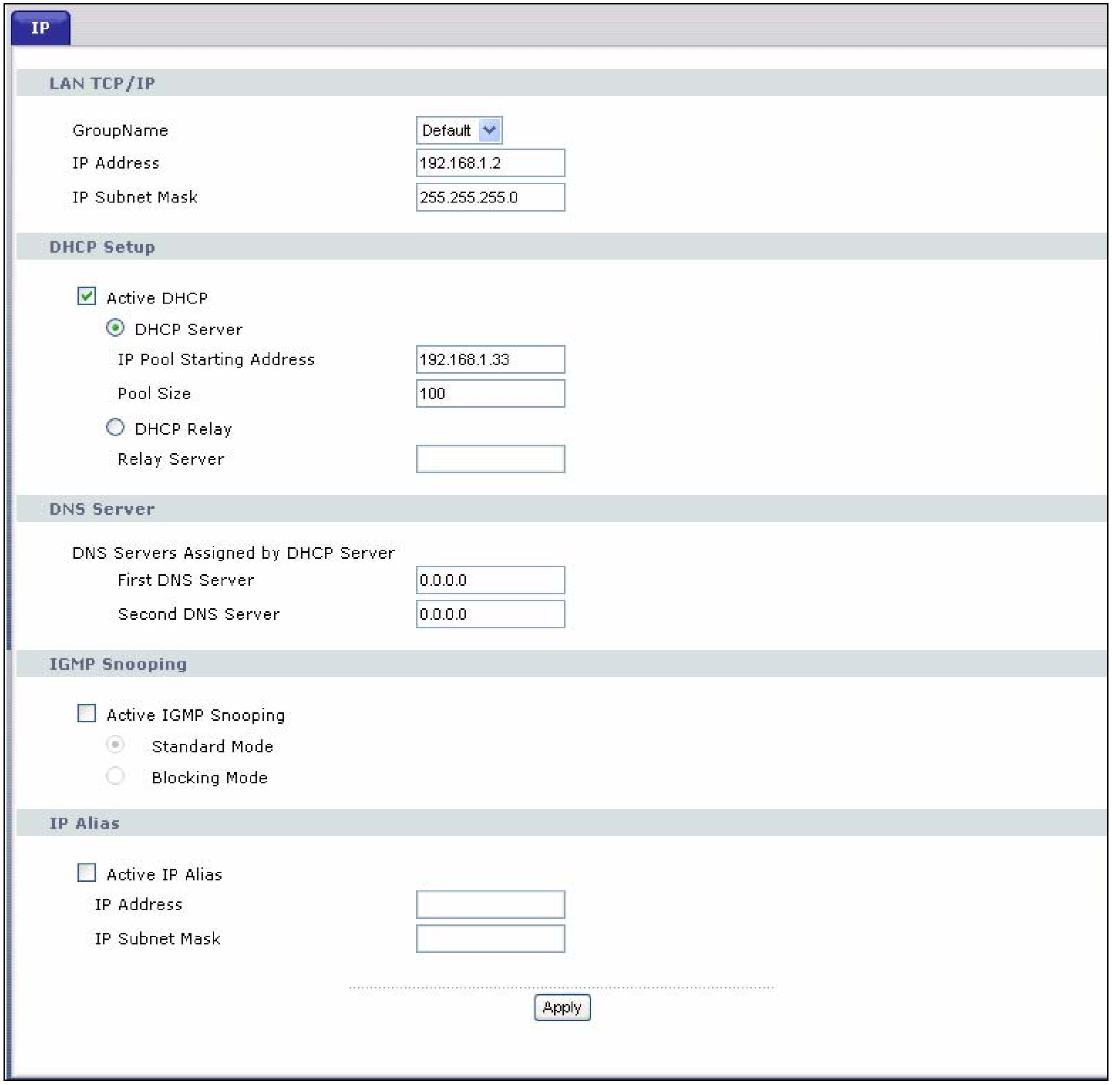
DNS

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

6.3 The LAN IP Screen

Click **Network > LAN** to open the **IP** screen. See Section 6.4 on page 97 for background information. Use this screen to set the Local Area Network IP address and subnet mask of your ZyXEL Device.

Figure 45 LAN > IP



LAN TCP/IP

GroupName: Default
IP Address: 192.168.1.2
IP Subnet Mask: 255.255.255.0

DHCP Setup

☑ Active DHCP
● DHCP Server
IP Pool Starting Address: 192.168.1.33
Pool Size: 100
○ DHCP Relay
Relay Server:

DNS Server

DNS Servers Assigned by DHCP Server
First DNS Server: 0.0.0.0
Second DNS Server: 0.0.0.0

IGMP Snooping

□ Active IGMP Snooping
● Standard Mode
○ Blocking Mode

IP Alias

□ Active IP Alias
IP Address:
IP Subnet Mask:

The following table describes the fields in this screen.

Table 22 LAN > IP

LABEL	DESCRIPTION
LAN TCP/IP	
Group Name	Select the interface group for which you want to configure the LAN TCP/IP settings. See Chapter 19 on page 219 for how to create a new interface group.
IP Address	Enter the LAN IP address you want to assign to your ZyXEL Device in dotted decimal notation, for example, 192.168.1.1 (factory default).
IP Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default).
DHCP Setup	
Active DHCP	Select this to have the ZyXEL Device act as a DHCP server or DHCP relay agent. Otherwise, deselect this to not have the ZyXEL Device provide any DHCP services. The DHCP server will be disabled.
DHCP Server	Select this option to have the ZyXEL Device assign IP addresses and provide subnet mask, gateway, and DNS server information to the network. The ZyXEL Device is the DHCP server for the network. When the ZyXEL Device acts as a DHCP server, the following items need to be set:
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
DHCP Relay	Select this option to have the ZyXEL Device forward DHCP request to the DHCP server.
Relay Server	If you select **DHCP Relay**, enter the IP address of the DHCP server.
DNS Servers Assigned by DHCP Server If you do not configure DNS servers, the ZyXEL Device uses its LAN IP address and tells the DHCP clients on the LAN that itself is the DNS server. When a LAN client sends a DNS query to the ZyXEL Device, the ZyXEL Device forwards the query to its system DNS server you configured in the WAN screen.	
First DNS Server	Enter the first DNS (Domain Name System) server IP address the ZyXEL Device passes to the DHCP clients.
Second DNS Server	Enter the second DNS (Domain Name System) server IP address the ZyXEL Device passes to the DHCP clients.
IGMP Snooping	
Active IGMP Snooping	Select this option to enable IGMP snooping. This allows the ZyXEL Device to passively learn multicast group.
Standard Mode	Select this to have the ZyXEL Device forward multicast packets to a port that joins the multicast group and broadcast unknown multicast packets from the WAN to all LAN ports.
Blocking Mode	Select this to have the ZyXEL Device block all unknown multicast packets from the WAN.

Table 22 LAN > IP

LABEL	DESCRIPTION
Active IP Alias	Select the check box to configure another LAN network for the ZyXEL Device.
IP Address	Enter the IP address of your ZyXEL Device in dotted decimal notation.
IP Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default).
Apply	Click **Apply** to save your changes back to the ZyXEL Device.

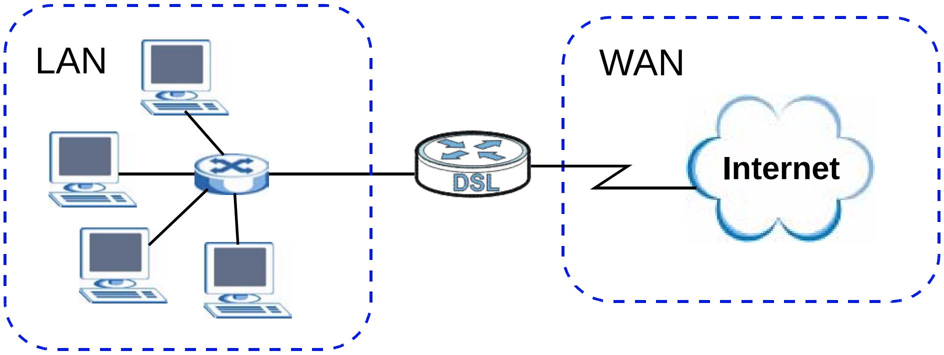
6.4 Technical Reference

The following section contains additional technical information about the ZyXEL Device features described in this chapter.

LANs, WANs and the ZyXEL Device

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

Figure 46 LAN and WAN IP Addresses



DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyXEL Device as a DHCP server or disable it. When configured as a server, the ZyXEL Device provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

IP Pool Setup

The ZyXEL Device is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

LAN TCP/IP

The ZyXEL Device has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

IP Address and Subnet Mask

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

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

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

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

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

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet

Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

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

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

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

Multicast

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

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

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

IP Alias

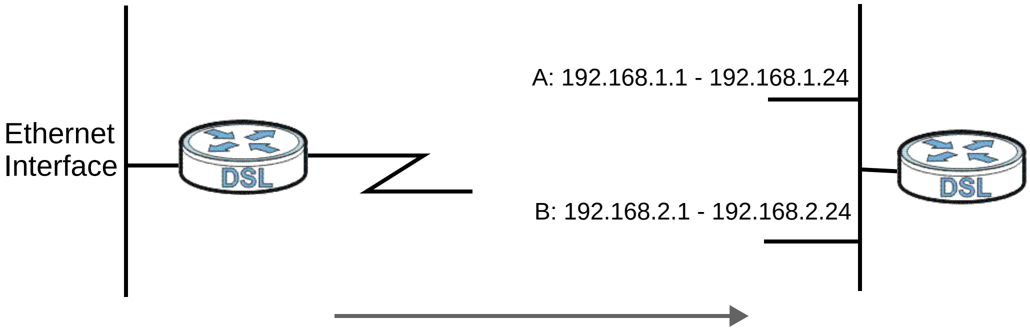
IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The ZyXEL Device supports three logical LAN interfaces via its single physical Ethernet interface with the ZyXEL Device itself as the gateway for each LAN network.

When you use IP alias, you can also configure firewall rules to control access between the LAN's logical networks (subnets).

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

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

Figure 47 Physical Network & Partitioned Logical Networks



7

Wireless LAN

7.1 Overview

This chapter describes how to perform tasks related to setting up and optimizing your wireless network, including the following.

- Turning the wireless connection on or off.
- Configuring a name, wireless channel and security for the network.
- Using WiFi Protected Setup (WPS) to configure your wireless network.
- Using a MAC (Media Access Control) address filter to restrict access to the wireless network.

See Chapter 2 on page 27 for a tutorial showing how to set up your wireless connection in an example scenario.

See Section 7.10 on page 121 for advanced technical information on wireless networks.

7.1.1 What You Can Do in this Chapter

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

- The **General** screen lets you turn the wireless connection on or off, set up wireless security and make other basic configuration changes (Section 7.4 on page 105). You can also configure the MAC filter to allow or block access to the ZyXEL Device based on the MAC addresses of the wireless stations.
- The **More AP** screen lets you set up multiple wireless networks on your ZyXEL Device (Section 7.5 on page 114).
- Use the **WPS** screen and the **WPS Station** screen to use WiFi Protected Setup (WPS). WPS lets you set up a secure network quickly, when connecting to other WPS-enabled devices.

  Use the **WPS** screen (see Section 7.6 on page 115) to enable or disable WPS, generate a security PIN (Personal Identification Number) and see information about the ZyXEL Device's WPS status.

  Use the **WPS Station** (see Section 7.7 on page 116) screen to set up WPS by pressing a button or using a PIN.

- The **WDS** screen lets you set up a Wireless Distribution System, in which the ZyXEL Device acts as a bridge with other ZyXEL access points (Section 7.8 on page 117).
- The **Advanced Setup** screen lets you change the wireless mode, and make other advanced wireless configuration changes (Section 7.9 on page 119).

You don’t necessarily need to use all these screens to set up your wireless connection. For example, you may just want to set up a network name, a wireless radio channel and some security in the **General** screen.

7.2 What You Need to Know

Wireless Basics

“Wireless” is essentially radio communication. In the same way that walkie-talkie radios send and receive information over the airwaves, wireless networking devices exchange information with one another. A wireless networking device is just like a radio that lets your computer exchange information with radios attached to other computers. Like walkie-talkies, most wireless networking devices operate at radio frequency bands that are open to the public and do not require a license to use. However, wireless networking is different from that of most traditional radio communications in that there a number of wireless networking standards available with different methods of data encryption.

Wireless Network Construction

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

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

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

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

Network Names

Each network must have a name, referred to as the SSID - “Service Set IDentifier”. The “service set” is the network, so the “service set identifier” is the network's name. This helps you identify your wireless network when wireless networks' coverage areas overlap and you have a variety of networks to choose from.

Radio Channels

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

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

Wireless Security

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

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

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

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

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

Signal Problems

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

Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters such as electric motors or microwaves. Problems with absorption occur when physical objects (such as thick walls) are between the two radios, muffling the signal.

7.3 Before You Begin

Before you start using these screens, ask yourself the following questions. See Section 7.2 on page 102 if some of the terms used here do not make sense to you.

- What wireless standards do the other wireless devices support (IEEE 802.11g, for example)? What is the most appropriate standard to use?
- What security options do the other wireless devices support (WPA-PSK, for example)? What is the best one to use?
- Do the other wireless devices support WPS (Wi-Fi Protected Setup)? If so, you can set up a well-secured network very easily.

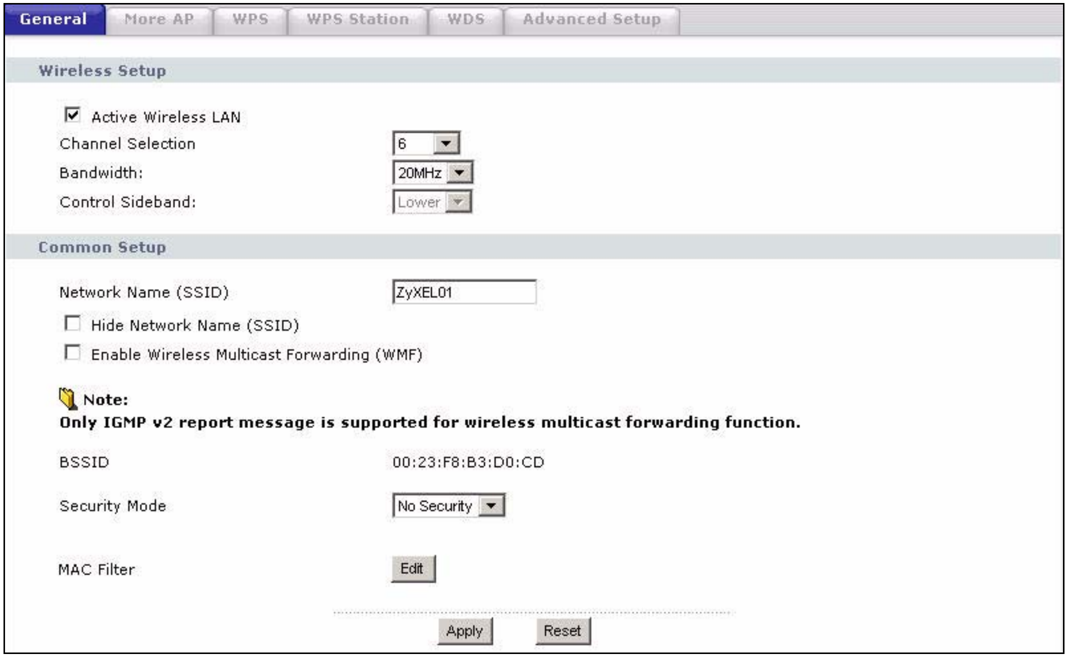
  Even if some of your devices support WPS and some do not, you can use WPS to set up your network and then add the non-WPS devices manually, although this is somewhat more complicated to do.
- What advanced options do you want to configure, if any? If you want to configure advanced options, ensure that you know precisely what you want to do. If you do not want to configure advanced options, leave them alone.

7.4 The General Screen

Note: If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's SSID or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the ZyXEL Device's new settings.

Click **Network > Wireless LAN** to open the **General** screen.

Figure 48 Network > Wireless LAN > General



Wireless Setup

☑ Active Wireless LAN

Channel Selection: 6

Bandwidth: 20MHz

Control Sideband: Lower

Common Setup

Network Name (SSID): ZyXEL01

□ Hide Network Name (SSID)

□ Enable Wireless Multicast Forwarding (WMF)

Note:
Only IGMP v2 report message is supported for wireless multicast forwarding function.

BSSID: 00:23:F8:B3:D0:CD

Security Mode: No Security

MAC Filter: Edit

Apply Reset

The following table describes the labels in this screen.

Table 23 Network > Wireless LAN > General

LABEL	DESCRIPTION
Active Wireless LAN	Click the check box to activate wireless LAN.
Channel Selection	Set the operating frequency/channel depending on your particular region. Either select a channel or use **Auto** to have the ZyXEL Device automatically determine a channel to use. If you are having problems with wireless interference, changing the channel may help. Try to use a channel that is as many channels away from any channels used by neighboring APs as possible. The channel number which the ZyXEL Device is currently using then displays next to this field.

Table 23 Network > Wireless LAN > General

LABEL	DESCRIPTION
Bandwidth	Select whether the ZyXEL Device uses a wireless channel width of **20MHz** or **40MHz**. A standard 20MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300 Mbps. 40MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The wireless clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal. Select **20MHz** if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding. This field is available only when you set the **802.11 Mode** to **802.11n Only** or **802.11b/g/n Mixed** in the **Advanced Setup** screen.
Control Sideband	This is available for some regions when you select a specific channel and set the **Bandwidth** field to **40MHz**. Set whether the control channel (set in the **Channel** field) should be in the **Lower** or **Upper** range of channel bands. This field is available only when you set the **802.11 Mode** to **802.11n Only** or **802.11b/g/n Mixed** in the **Advanced Setup** screen.
Network Name (SSID)	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. Note: If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's SSID or WEP settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the ZyXEL Device's new settings.
Hide Network Name (SSID)	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Enable Wireless Multicast Forwarding (WMF)	Select this check box to allow the ZyXEL Device to transmit wireless multicast traffic.
BSSID	This shows the MAC address of the wireless interface on the ZyXEL Device when wireless LAN is enabled.
Security Mode	See the following sections for more details about this field.
MAC Filter	Click this button to go to the **MAC Filter** screen to configure whether the wireless devices with the MAC addresses listed are allowed or denied to access the ZyXEL Device using this SSID.

Table 23 Network > Wireless LAN > General

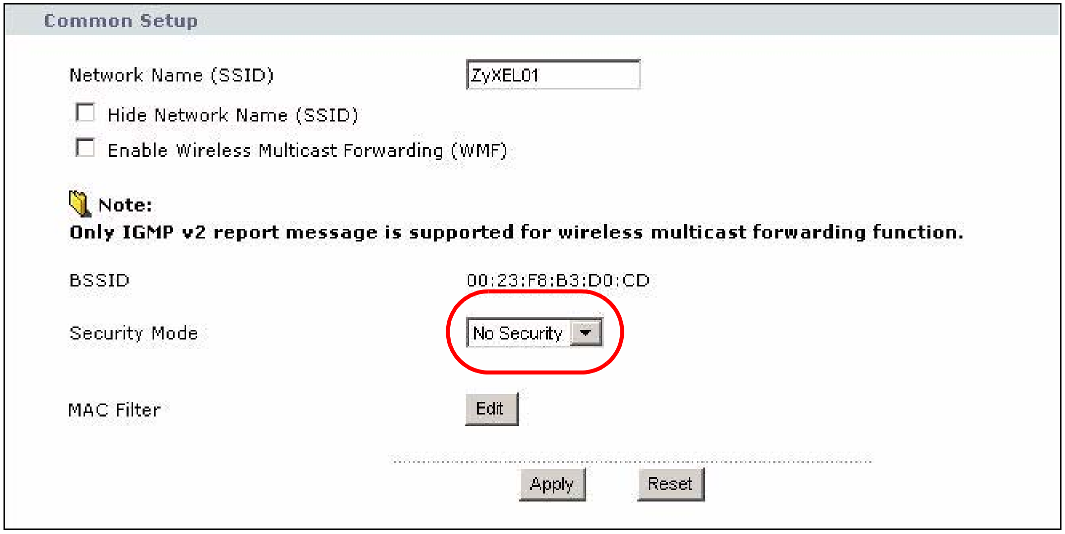
LABEL	DESCRIPTION
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to reload the previous configuration for this screen.

7.4.1 No Security

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

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

Figure 49 Wireless LAN > General: No Security



Common Setup

Network Name (SSID) ZyXEL01

□ Hide Network Name (SSID)

□ Enable Wireless Multicast Forwarding (WMF)

Note:
Only IGMP v2 report message is supported for wireless multicast forwarding function.

BSSID 00:23:F8:B3:D0:CD

Security Mode No Security

MAC Filter Edit

The following table describes the labels in this screen.

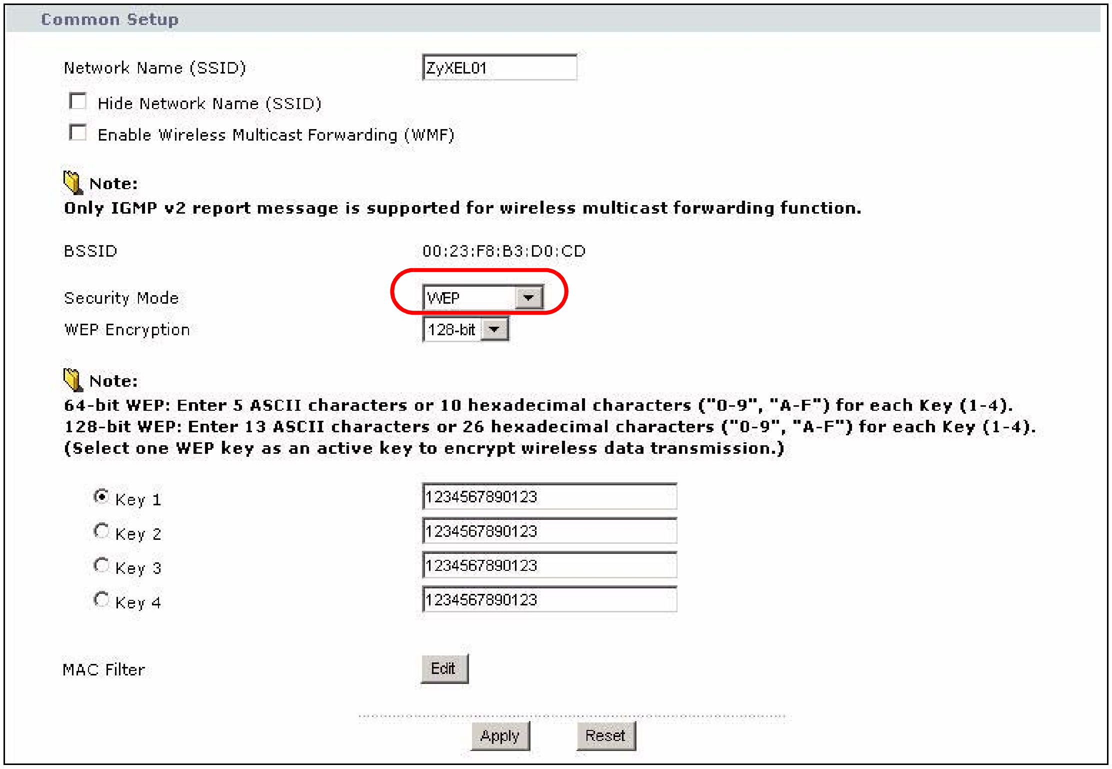
Table 24 Wireless LAN > General: No Security

LABEL	DESCRIPTION
Security Mode	Choose **No Security** from the drop-down list box.

7.4.2 WEP Encryption

In order to configure and enable WEP encryption; click **Network > Wireless LAN** to display the **General** screen. Select **WEP** from the **Security Mode** list.

Figure 50 Wireless LAN > General: Static WEP Encryption



Common Setup

Network Name (SSID): ZyXEL01

□ Hide Network Name (SSID)

□ Enable Wireless Multicast Forwarding (WMF)

Note:
Only IGMP v2 report message is supported for wireless multicast forwarding function.

BSSID: 00:23:F8:B3:D0:CD

Security Mode: WEP

WEP Encryption: 128-bit

Note:
64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key (1-4).
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each Key (1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

● Key 1: 1234567890123
○ Key 2: 1234567890123
○ Key 3: 1234567890123
○ Key 4: 1234567890123

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

Table 25 Network > Wireless LAN > General: Static WEP Encryption

LABEL	DESCRIPTION
Security Mode	Choose **WEP** from the drop-down list box.

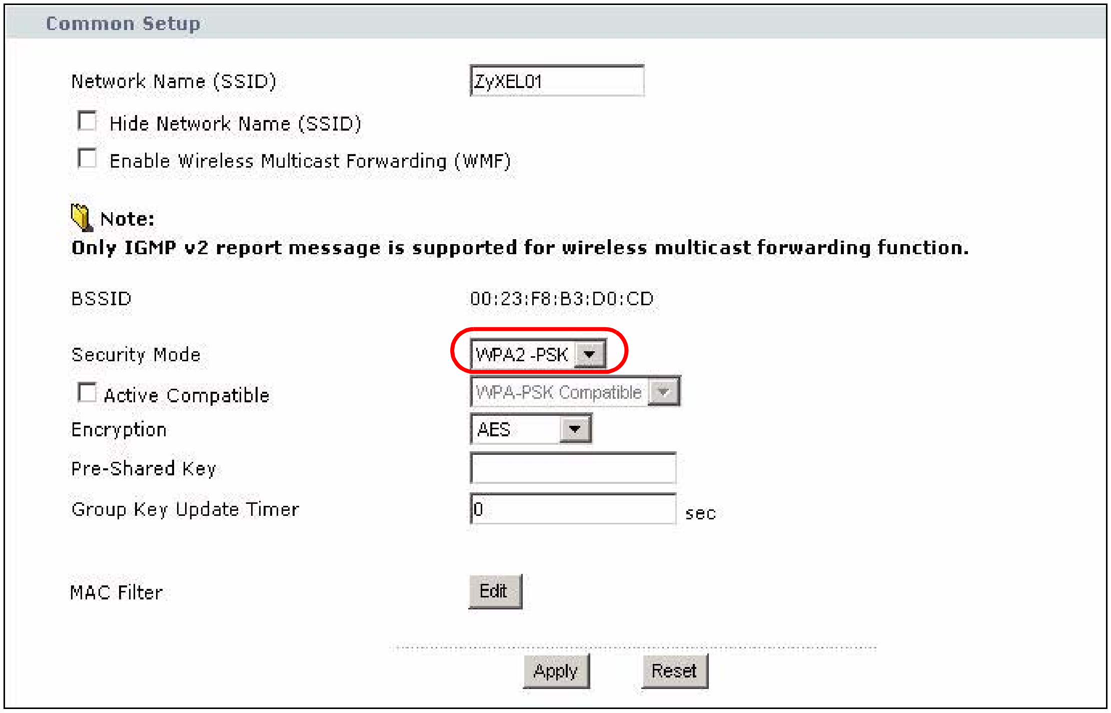
Table 25 Network > Wireless LAN > General: Static WEP Encryption

LABEL	DESCRIPTION
WEP Encryption	WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network. Select **64-bit WEP** or **128-bit WEP** to enable data encryption.
Key 1 to Key 4	The WEP key is used to secure your data from eavesdropping by unauthorized wireless users. Both the ZyXEL Device and the wireless stations must use the same WEP key for data transmission. Only one key can be activated at any one time. Select a default key to use for data encryption. If you chose **64-bit WEP** in the **WEP Encryption** field, then enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. If you chose **128-bit WEP** in the **WEP Encryption** field, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.

7.4.3 WPA(2)-PSK

In order to configure and enable WPA(2)-PSK authentication; click **Network > Wireless LAN** to display the **General** screen. Select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 51 Wireless LAN > General: WPA(2)-PSK



Common Setup

Network Name (SSID) ZyXEL01

□ Hide Network Name (SSID)

□ Enable Wireless Multicast Forwarding (WMF)

Note:
Only IGMP v2 report message is supported for wireless multicast forwarding function.

BSSID 00:23:F8:B3:D0:CD

Security Mode WPA2 -PSK

□ Active Compatible WPA-PSK Compatible

Encryption AES

Pre-Shared Key

Group Key Update Timer 0 sec

MAC Filter Edit

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

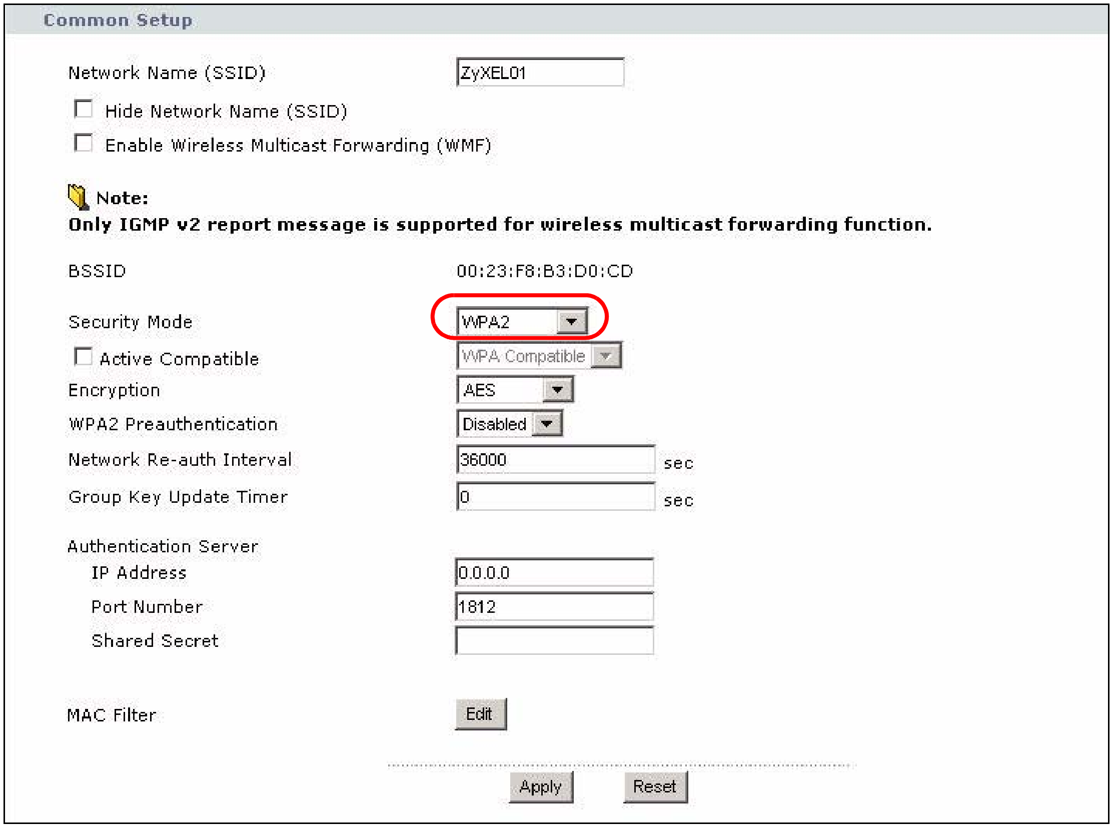
Table 26 Wireless LAN > General: WPA(2)-PSK

LABEL	DESCRIPTION
Security Mode	Choose **WPA-PSK** or **WPA2-PSK** from the drop-down list box.
Active Compatible	This field is only available for WPA2-PSK. Select this if you want the ZyXEL Device to support WPA-PSK and WPA2-PSK simultaneously.
Encryption	Select the encryption type (**TKIP**, **AES** or **TKIP+AES**) for data encryption. Select **TKIP** if your wireless clients can all use TKIP. Select **AES** if your wireless clients can all use AES. Select **TKIP+AES** to allow the wireless clients to use either TKIP or AES.
Pre-Shared Key	The encryption mechanisms used for **WPA(2)** and **WPA(2)-PSK** are the same. The only difference between the two is that **WPA(2)-PSK** uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP (if using **WPA(2)-PSK** key management) or **RADIUS** server (if using WPA(2) key management) sends a new group key out to all clients. The re-keying process is the WPA(2) equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in **WPA(2)-PSK** mode. The ZyXEL Device default is **1800** seconds (30 minutes).

7.4.4 WPA(2) Authentication

Use this screen to configure and enable WPA or WPA2 authentication; click the **Wireless LAN** link under **Network** to display the **General** screen. Select **WPA** or **WPA2** from the **Security Mode** list.

Figure 52 Wireless LAN > General: WPA(2)



Common Setup

Network Name (SSID): ZyXEL01

□ Hide Network Name (SSID)

□ Enable Wireless Multicast Forwarding (WMF)

Note:
Only IGMP v2 report message is supported for wireless multicast forwarding function.

BSSID: 00:23:F8:B3:D0:CD

Security Mode: WPA2

□ Active Compatible: WPA Compatible

Encryption: AES

WPA2 Preauthentication: Disabled

Network Re-auth Interval: 36000 sec

Group Key Update Timer: 0 sec

Authentication Server

IP Address: 0.0.0.0

Port Number: 1812

Shared Secret:

MAC Filter: Edit

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

Table 27 Wireless LAN > General: WPA(2)

LABEL	DESCRIPTION
Security Mode	Choose **WPA** or **WPA2** from the drop-down list box.
Active Compatible	This field is only available for WPA2. Select this if you want the ZyXEL Device to support WPA and WPA2 simultaneously.
Encryption	Select the encryption type (**TKIP**, **AES** or **TKIP+AES**) for data encryption. Select **TKIP** if your wireless clients can all use TKIP. Select **AES** if your wireless clients can all use AES. Select **TKIP+AES** to allow the wireless clients to use either TKIP or AES.

Table 27 Wireless LAN > General: WPA(2)

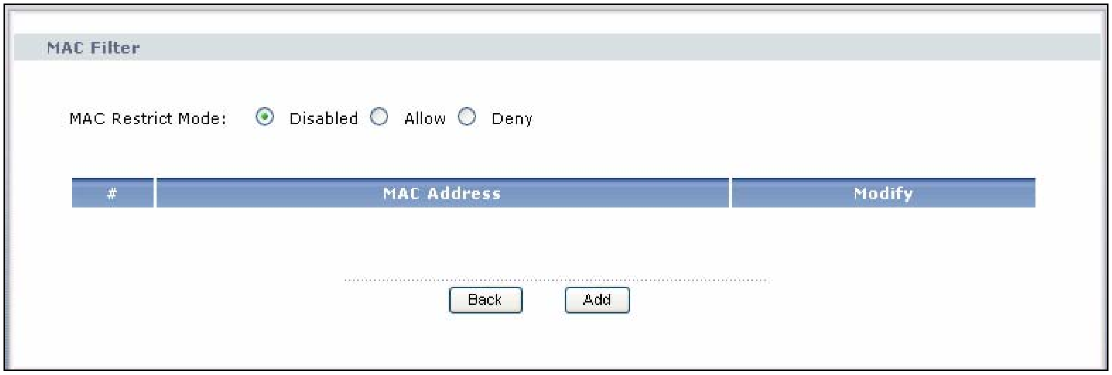
LABEL	DESCRIPTION
WPA2 Preauthentication	This field is available only when you select **WPA2**. Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it. Select **Enabled** to turn on preauthentication in WAP2. Otherwise, select **Disabled**.
Network Re-auth Interval	This field is available only when you select **WPA2**. Specify how often wireless clients have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 2147483647 seconds. Note: If wireless client authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP (if using **WPA(2)-PSK** key management) or **RADIUS** server (if using WPA(2) key management) sends a new group key out to all clients. The re-keying process is the WPA(2) equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in **WPA(2)-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.

7.4.5 MAC Filter

This screen allows you to configure the ZyXEL Device to give exclusive access to specific devices (**Allow**) or exclude specific devices from accessing the ZyXEL Device (**Deny**). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the devices to configure this screen.

Use this screen to change your ZyXEL Device's MAC filter settings. Click the **Edit** button in the **Wireless LAN > General** screen. The following screen displays.

Figure 53 Wireless LAN > MAC Filter



MAC Filter

MAC Restrict Mode: ● Disabled ○ Allow ○ Deny

#	MAC Address	Modify

The following table describes the labels in this screen.

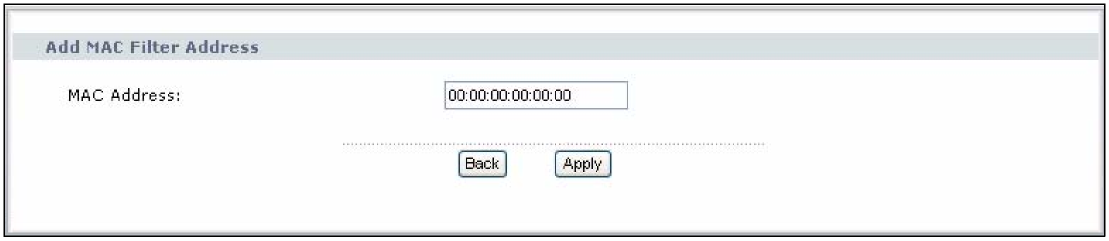
Table 28 Wireless LAN > MAC Filter

LABEL	DESCRIPTION
MAC Restrict Mode	Define the filter action for the list of MAC addresses in the table below. Select **Disabled** to turn off MAC address filtering. Select **Allow** to permit access to the ZyXEL Device, MAC addresses not listed will be denied access to the ZyXEL Device. Select **Deny** to block access to the ZyXEL Device, MAC addresses not listed will be allowed to access the ZyXEL Device
#	This is the index number of the MAC address.
MAC Address	This is the MAC addresses of the wireless devices that are allowed or denied access to the ZyXEL Device.
Modify	Click the **Remove** icon to delete the entry.
Back	Click this to return to the previous screen without saving changes.
Add	Click this to create a new MAC filtering rule.

7.4.6 Adding a New MAC Filtering Rule

Click the **Add** button in the **MAC Filter** screen. The following screen displays.

Figure 54 Wireless LAN > MAC Filter > Add



Add MAC Filter Address

MAC Address: 00:00:00:00:00:00

The following table describes the labels in this screen.

Table 29 Wireless LAN > MAC Filter > Add

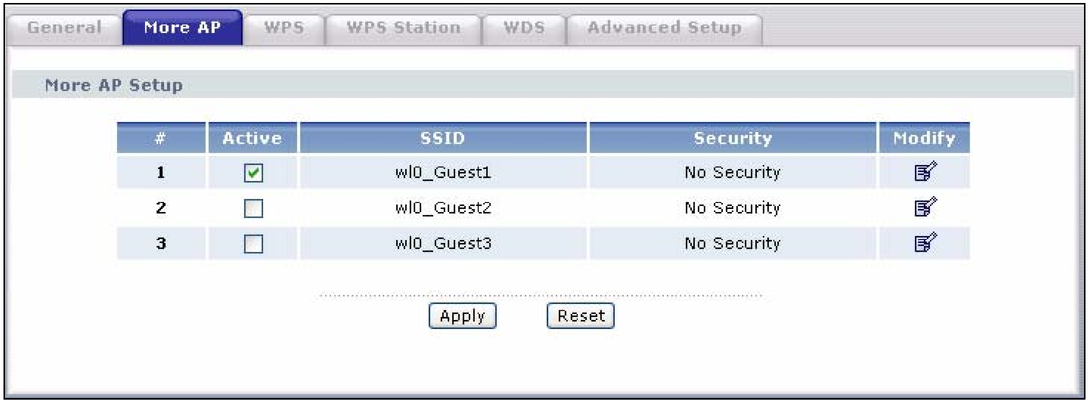
LABEL	DESCRIPTION
MAC Address	Enter the MAC addresses of the wireless devices that are allowed or denied access to the ZyXEL Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Back	Click this to return to the previous screen without saving changes.
Apply	Click this to save your changes and go back to the previous screen.

7.5 The More AP Screen

This screen allows you to enable and configure multiple wireless networks on the ZyXEL Device.

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

Figure 55 Network > Wireless LAN > More AP



More AP Setup

#	Active	SSID	Security	Modify
1	☑	wl0_Guest1	No Security	
2	□	wl0_Guest2	No Security	
3	□	wl0_Guest3	No Security	

The following table describes the labels in this screen.

Table 30 Network > Wireless LAN > More AP

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

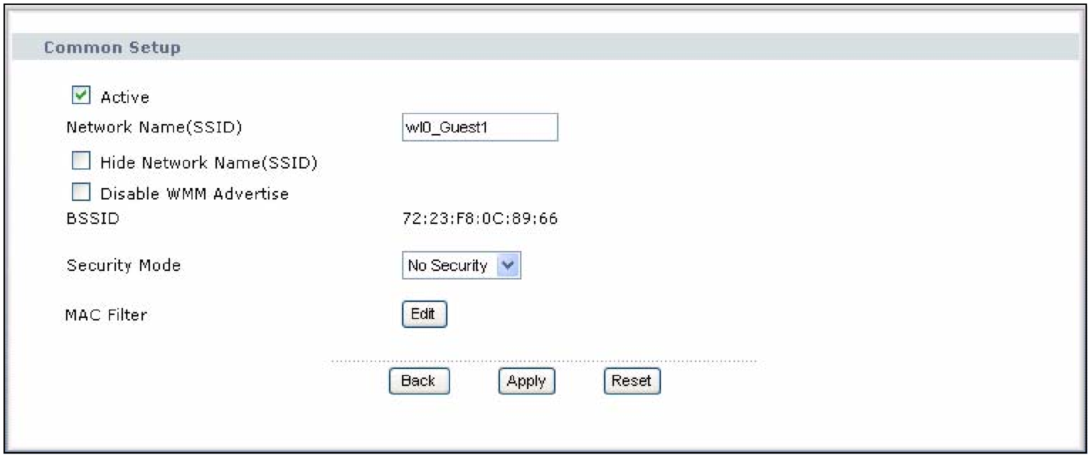
Table 30 Network > Wireless LAN > More AP

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.5.1 More AP Edit

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

Figure 56 Network > Wireless LAN > More AP: Edit



Common Setup

☑ Active

Network Name(SSID): wl0_Guest1

□ Hide Network Name(SSID)

□ Disable WMM Advertise

BSSID: 72:23:F8:0C:89:66

Security Mode: No Security

MAC Filter: Edit

See Section 7.4 on page 105 for more details about the fields in this screen.

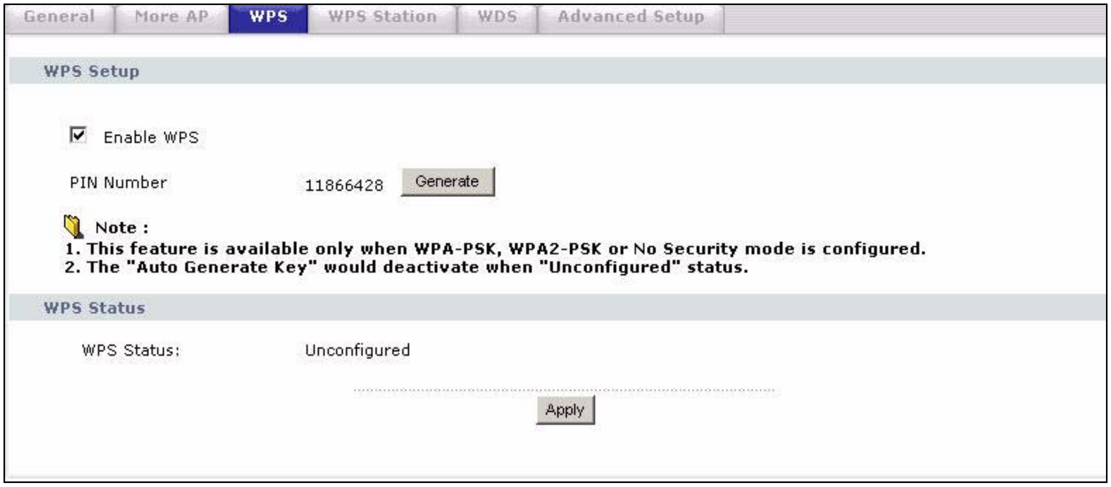
7.6 The WPS Screen

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

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Set up each WPS connection between two devices. Both devices must support WPS.

Click **Network > Wireless LAN >WPS**. The following screen displays.

Figure 57 Network > Wireless LAN > WPS



☑ Enable WPS

PIN Number 11866428

Note :
1. This feature is available only when WPA-PSK, WPA2-PSK or No Security mode is configured.
2. The "Auto Generate Key" would deactivate when "Unconfigured" status.

WPS Status: Unconfigured

The following table describes the labels in this screen.

Table 31 Network > Wireless LAN > WPS

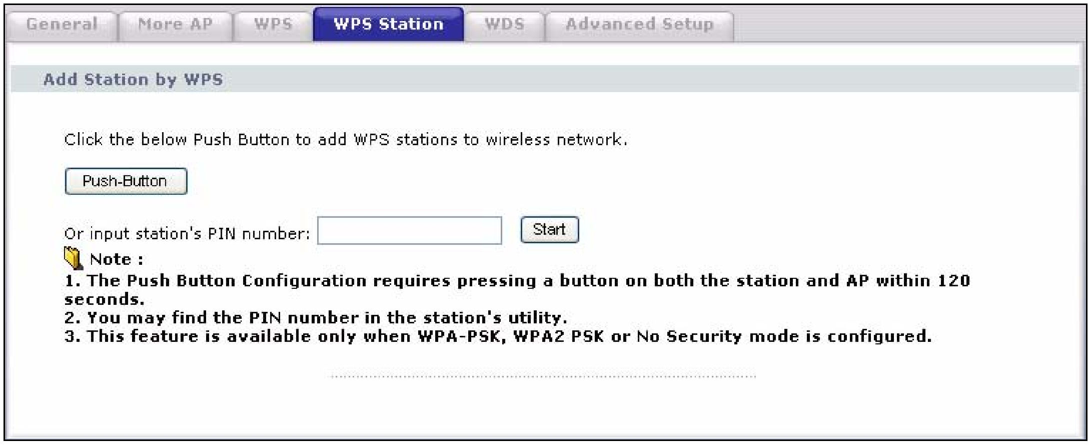
LABEL	DESCRIPTION
WPS Setup	
Enable WPS	Select the check box to activate WPS on the ZyXEL Device.
PIN Number	This shows the PIN (Personal Identification Number) of the ZyXEL Device. Enter this PIN in the configuration utility of the device you want to connect to using WPS. The PIN is not necessary when you use WPS push-button method.
Generate	Click this button to have the ZyXEL Device create a new PIN.
WPS Status	This displays **Configured** when the ZyXEL Device has connected to a wireless network using WPS or **Enable WPS** is selected and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the screen. This displays **Unconfigured** if WPS is disabled and there is no wireless or wireless security changes on the ZyXEL Device.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.

7.7 The WPS Station Screen

Use this screen to set up a WPS wireless network using either Push Button Configuration (PBC) or PIN Configuration.

Click **Network > Wireless LAN > WPS Station**. The following screen displays.

Figure 58 Network > Wireless LAN > WPS Station



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

Or input station's PIN number:

Note :

1. The Push Button Configuration requires pressing a button on both the station and AP within 120 seconds.
2. You may find the PIN number in the station's utility.
3. This feature is available only when WPA-PSK, WPA2 PSK or No Security mode is configured.

The following table describes the labels in this screen.

Table 32 Network > Wireless LAN > WPS Station

LABEL	DESCRIPTION
Push Button	Click this button to add another WPS-enabled wireless device (within wireless range of the ZyXEL Device) to your wireless network. Note: You must press the other wireless device’s WPS button within two minutes of pressing this button.
Or input station's PIN number	Enter the PIN of the device that you are setting up a WPS connection with and click **Start** to authenticate and add the wireless device to your wireless network. You can find the PIN either on the outside of the device, or by checking the device’s settings. Note: You must also activate WPS on that device within two minutes to have it present its PIN to the ZyXEL Device.

7.8 The WDS Screen

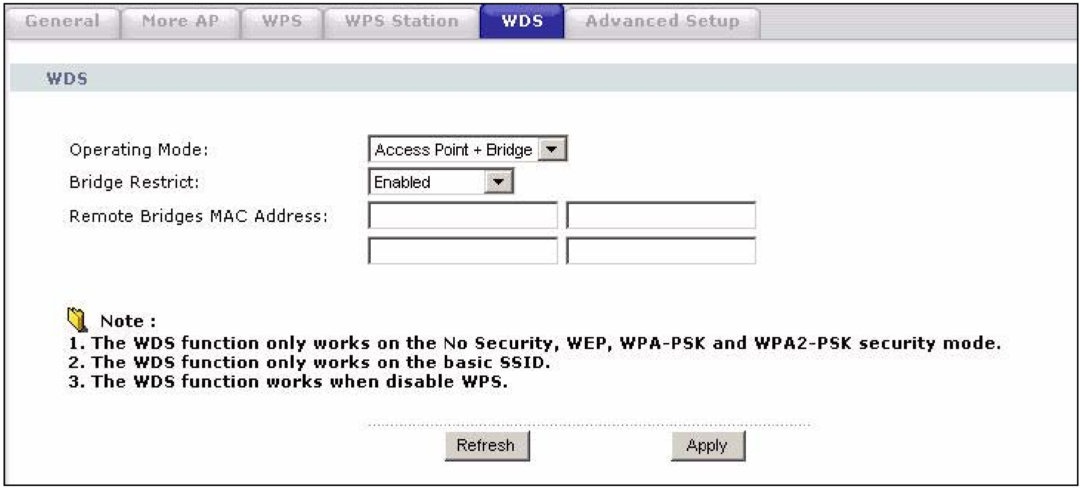
A Wireless Distribution System (WDS) is a wireless connection between two or more APs. Use this screen to set up your WDS links between the ZyXEL Devices. You need to know the MAC address of the peer device. Once the security settings of peer sides match one another, the connection between the devices is made.

Note: You can use WDS only when wireless security is set to “No Security” or “WEP”. The wireless security settings apply to both WDS links and the connections between the ZyXEL Device and any wireless clients.

Note: At the time of writing, WDS is only compatible with other ZyXEL Devices of the same model.

Click **Network > Wireless LAN > WDS**. The following screen displays. WDS is turned on and this screen is configurable when the ZyXEL Device's wireless security mode is **No Security** or **WEP**.

Figure 59 Network > Wireless LAN > WDS



Operating Mode: Access Point + Bridge

Bridge Restrict: Enabled

Remote Bridges MAC Address:

Note :
1. The WDS function only works on the No Security, WEP, WPA-PSK and WPA2-PSK security mode.
2. The WDS function only works on the basic SSID.
3. The WDS function works when disable WPS.

The following table describes the labels in this screen.

Table 33 Network > Wireless LAN > WDS

LABEL	DESCRIPTION
WDS	
Operating Mode	Select the operating mode for your ZyXEL Device. • **Access Point + Bridge -** The ZyXEL Device functions as a bridge and access point simultaneously. • **Wireless Bridge** - The ZyXEL Device acts as a wireless network bridge and establishes wireless links with other APs. In this mode, clients cannot connect to the ZyXEL Device wirelessly. You need to know the MAC address of the peer device, which must be of the same model and also WDS-enabled. The ZyXEL Device can establish up to four wireless links with other APs.
Bridge Restrict	This field is available only when you set operating mode to **Access Point + Bridge**. Select **Enabled** to turn on WDS and enter the peer device’s MAC address manually in the table below. Select **Enabled(Scan)** to turn on WDS, search and display the available APs within range in the table below.
Remote Bridges MAC Address	Enter the MAC address of the peer device that your ZyXEL Device wants to make a bridge connection with. You can connect to up to 4 peer devices.

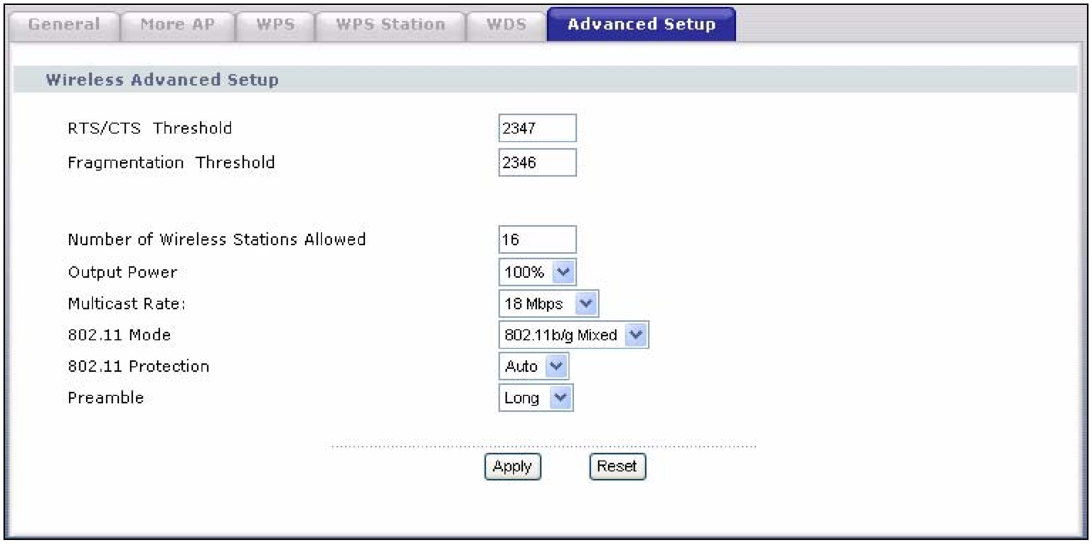
Table 33 Network > Wireless LAN > WDS

LABEL	DESCRIPTION
	This is available only when you select **Enabled(Scan)** in the **Bridge Restrict** field. Select the check box and click **Apply** to have the ZyXEL Device establish a wireless link with the selected wireless device.
SSID	This is available only when you select **Enabled(Scan)** in the **Bridge Restrict** field. This shows the SSID of the available wireless device within range.
BSSID	This is available only when you select **Enabled(Scan)** in the **Bridge Restrict** field. This shows the MAC address of the available wireless device within range.
Refresh	Click **Refresh** to update the **Remote Bridges MAC Address** table when **Bridge Restrict** is set to **Enabled(Scan)**.
Apply	Click **Apply** to save your changes to ZyXEL Device.

7.9 The Advanced Setup Screen

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

Figure 60 Wireless LAN > Advanced Setup



Wireless Advanced Setup

RTS/CTS Threshold: 2347
Fragmentation Threshold: 2346
Number of Wireless Stations Allowed: 16
Output Power: 100%
Multicast Rate: 18 Mbps
802.11 Mode: 802.11b/g Mixed
802.11 Protection: Auto
Preamble: Long

The following table describes the labels in this screen.

Table 34 Wireless LAN > Advanced Setup

LABEL	DESCRIPTION
RTS/CTS Threshold	Enter a value between 0 and 2432.
Fragmentation Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.
Number of Wireless Stations Allowed	Specify the maximum number (from 1 to 64) of the wireless stations that may connect to the ZyXEL Device.
Output Power	Set the output power of the ZyXEL Device. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs. Select one of the following **20%**, **40%**, **60%**, **80%** or **100%**.
Multicast Rate	Select a data rate at which the ZyXEL Device transmits wireless multicast traffic. If you select a high rate, multicast traffic may occupy all the bandwidth and cause network congestion.
802.11 Mode	Select **802.11b Only** to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. In this mode, all wireless devices can only transmit at the data rates supported by IEEE 802.11b. Select **802.11g Only** to allow IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. IEEE 802.11b compliant WLAN devices can associate with the ZyXEL Device only when they use the short preamble type. Select **802.11n Only** to only allow IEEE 802.11n compliant WLAN devices to associate with the ZyXEL Device. This can increase transmission rates, although IEEE 802.11b or IEEE 802.11g clients will not be able to connect to the ZyXEL Device. Select **802.11b/g Mixed** to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. The ZyXEL Device adjusts the transmission rate automatically according to the wireless standard supported by the wireless devices. Select **802.11 b/g/n mixed mode** to allow both IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced.
802.11 Protection	Enabling this feature can help prevent collisions in mixed-mode networks (networks with both IEEE 802.11b and IEEE 802.11g traffic). Select **Auto** to have the wireless devices transmit data after a RTS/CTS handshake. This helps improve IEEE 802.11g performance. Select **Off** to disable 802.11 protection. The transmission rate of your ZyXEL Device might be reduced in a mixed-mode network. This field displays **Off** and is not configurable when you set **802.11 Mode** to **802.11b Only**.

Table 34 Wireless LAN > Advanced Setup

LABEL	DESCRIPTION
Preamble	Select a preamble type from the drop-down list menu. Choices are **Long** or **Short**. The default setting is **Long**. See the appendix for more information. This field is not configurable and the ZyXEL Device uses **Short** when you set **802.11 Mode** to **802.11g Only** or **802.11n Only**.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to reload the previous configuration for this screen.

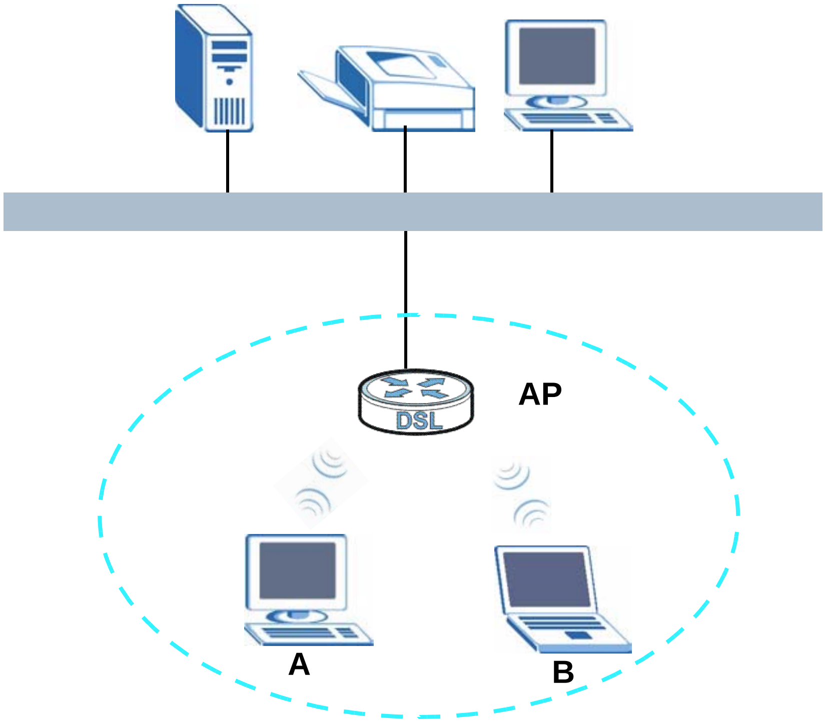
7.10 Technical Reference

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

7.10.1 Wireless Network Overview

The following figure provides an example of a wireless network.

Figure 61 Example of a Wireless Network



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

Every wireless network must follow these basic guidelines.

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

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

  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every device in the same wireless network must use security compatible with the AP.

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

7.10.2 Additional Wireless Terms

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

Table 35 Additional Wireless Terms

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

7.10.3 Wireless Security Overview

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

7.10.3.1 SSID

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

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

7.10.3.2 MAC Address Filter

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

You can use the MAC address filter to tell the ZyXEL Device which devices are allowed or not allowed to use the wireless network. If a device is allowed to use the wireless network, it still has to have the correct information (SSID, channel, and security). If a device is not allowed to use the wireless network, it does not matter if it has the correct information.

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

7.10.3.3 User Authentication

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

[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.

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

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

7.10.3.4 Encryption

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

The types of encryption you can choose depend on the type of authentication. (See Section 7.10.3.3 on page 123 for information about this.)

Table 36 Types of Encryption for Each Type of Authentication

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

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

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

Note: It is recommended that wireless networks use **WPA-PSK**, **WPA**, or stronger encryption. The other types of encryption are better than none at all, but it is still possible for unauthorized wireless devices to figure out the original information pretty quickly.

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

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

7.10.4 WiFi Protected Setup

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

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

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

7.10.4.1 Push Button Configuration

WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button.

Take the following steps to set up WPS using the button.

1. Ensure that the two devices you want to set up are within wireless range of one another.

2. Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the ZyXEL Device, see Section 7.7 on page 116).

3 Press the button on one of the devices (it doesn't matter which). For the ZyXEL Device you must press the WPS button for more than three seconds.

4 Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through an secure connection to the enrollee.

If you need to make sure that WPS worked, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

7.10.4.2 PIN Configuration

Each WPS-enabled device has its own PIN (Personal Identification Number). This may either be static (it cannot be changed) or dynamic (in some devices you can generate a new PIN by clicking on a button in the configuration interface).

Use the PIN method instead of the push-button configuration (PBC) method if you want to ensure that the connection is established between the devices you specify, not just the first two devices to activate WPS in range of each other. However, you need to log into the configuration interfaces of both devices to use the PIN method.

When you use the PIN method, you must enter the PIN from one device (usually the wireless client) into the second device (usually the Access Point or wireless router). Then, when WPS is activated on the first device, it presents its PIN to the second device. If the PIN matches, one device sends the network and security information to the other, allowing it to join the network.

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

1 Ensure WPS is enabled on both devices.

2 Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this.

3 Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide for how to find the WPS PIN - for the ZyXEL Device, see Section 7.6 on page 115).

4 Enter the client's PIN in the AP's configuration interface.

Note: If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client - it does not matter which.

5 Start WPS on both devices within two minutes.

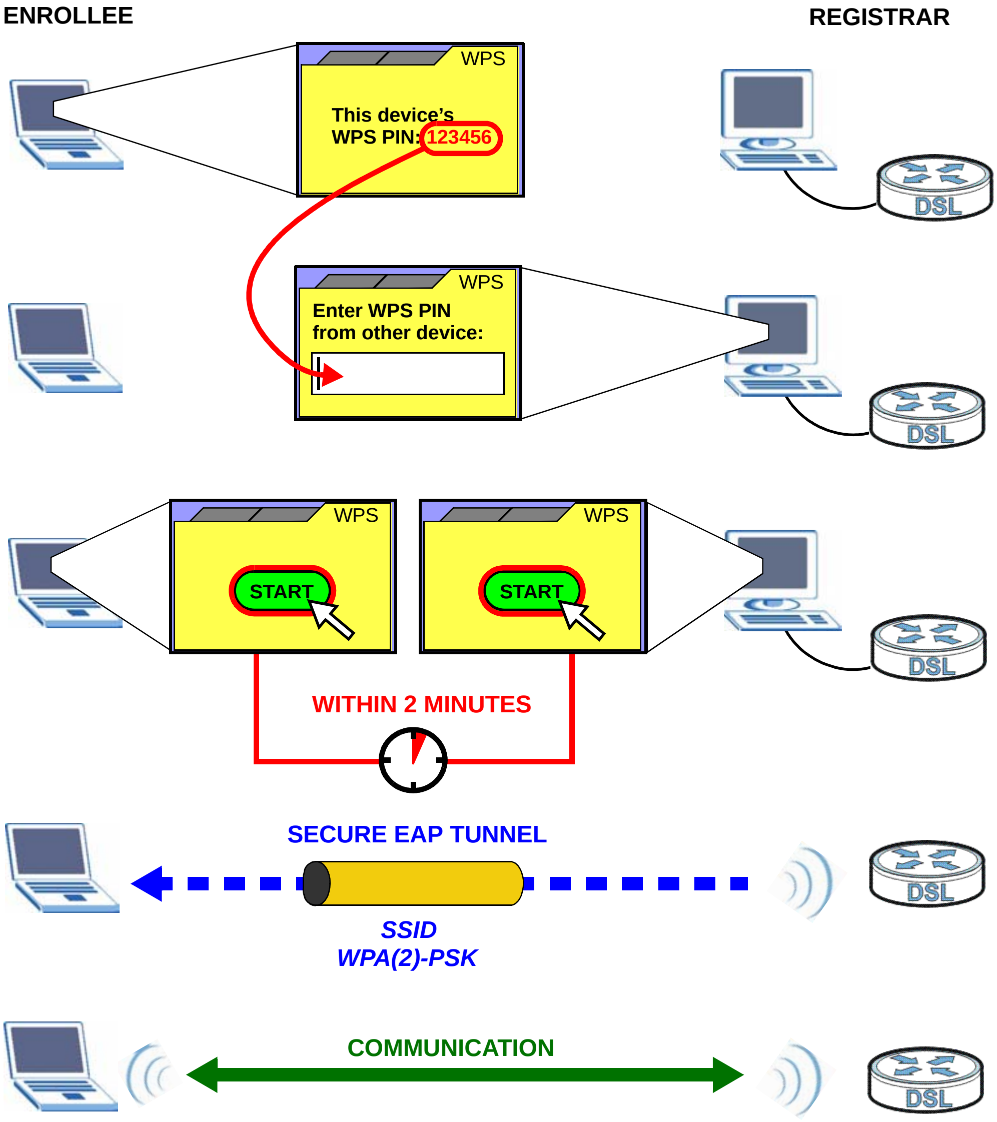
Note: Use the configuration utility to activate WPS, not the push-button on the device itself.

6 On a computer connected to the wireless client, try to connect to the Internet. If you can connect, WPS was successful.

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

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

Figure 62 Example WPS Process: PIN Method

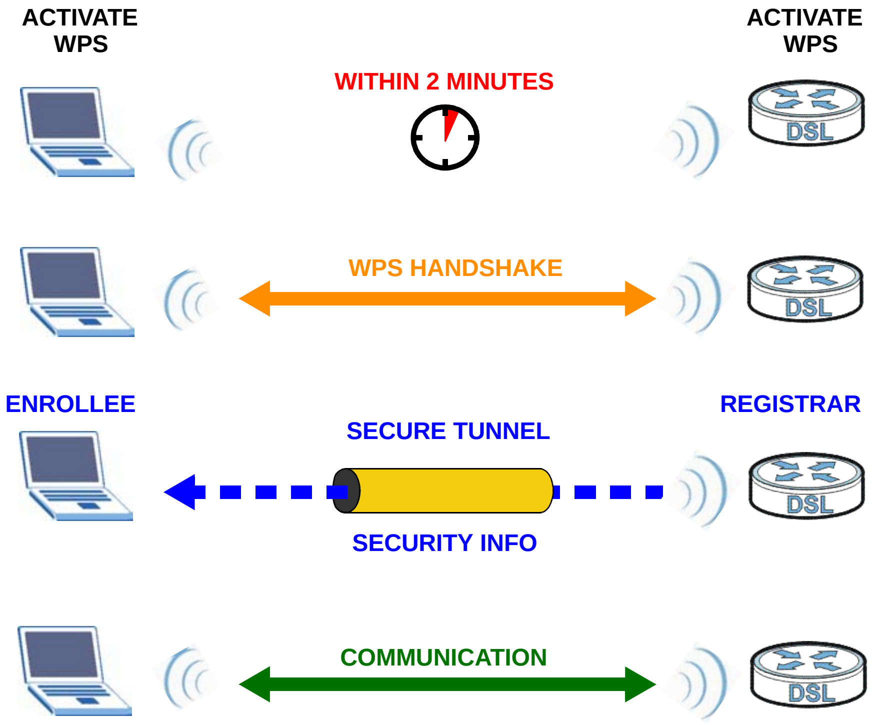


7.10.4.3 How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings. The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPA-PSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is already part of a network, it sends the existing information. If not, it generates the SSID and WPA(2)-PSK randomly.

The following figure shows a WPS-enabled client (installed in a notebook computer) connecting to a WPS-enabled access point.

Figure 63 How WPS works



The roles of registrar and enrollee last only as long as the WPS setup process is active (two minutes). The next time you use WPS, a different device can be the registrar if necessary.

The WPS connection process is like a handshake; only two devices participate in each WPS transaction. If you want to add more devices you should repeat the process with one of the existing networked devices and the new device.

Note that the access point (AP) is not always the registrar, and the wireless client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled wireless clients.

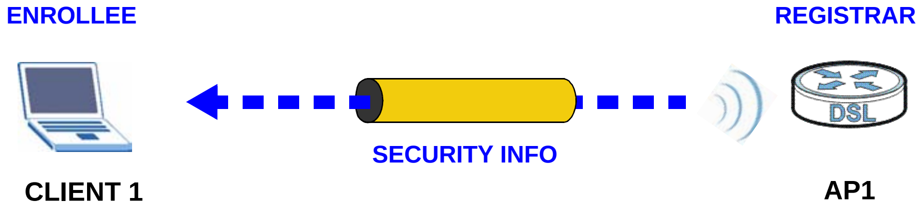
By default, a WPS devices is “unconfigured”. This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled device has connected to another device using WPS, it becomes “configured”. A configured wireless client can still act as enrollee or registrar in subsequent WPS connections, but a configured access point can no longer act as enrollee. It will be the registrar in all subsequent WPS connections in which it is involved. If you want a configured AP to act as an enrollee, you must reset it to its factory defaults.

7.10.4.4 Example WPS Network Setup

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

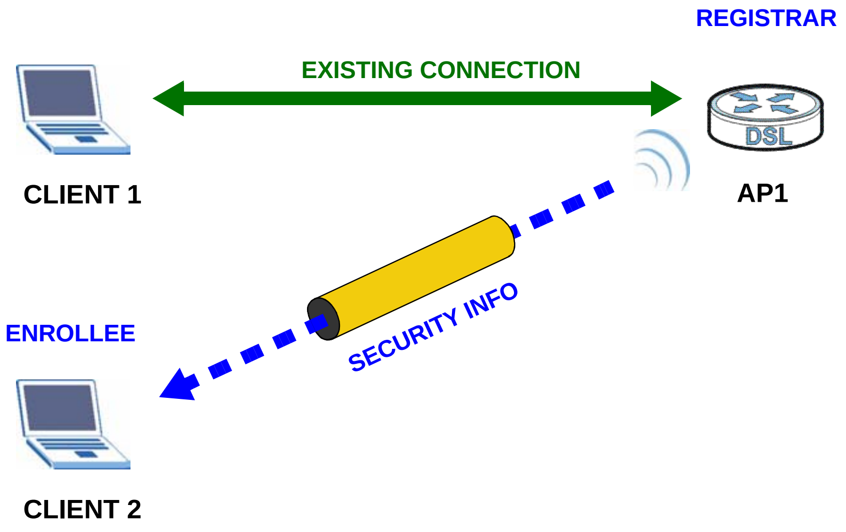
The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information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

Figure 64 WPS: Example Network Step 1



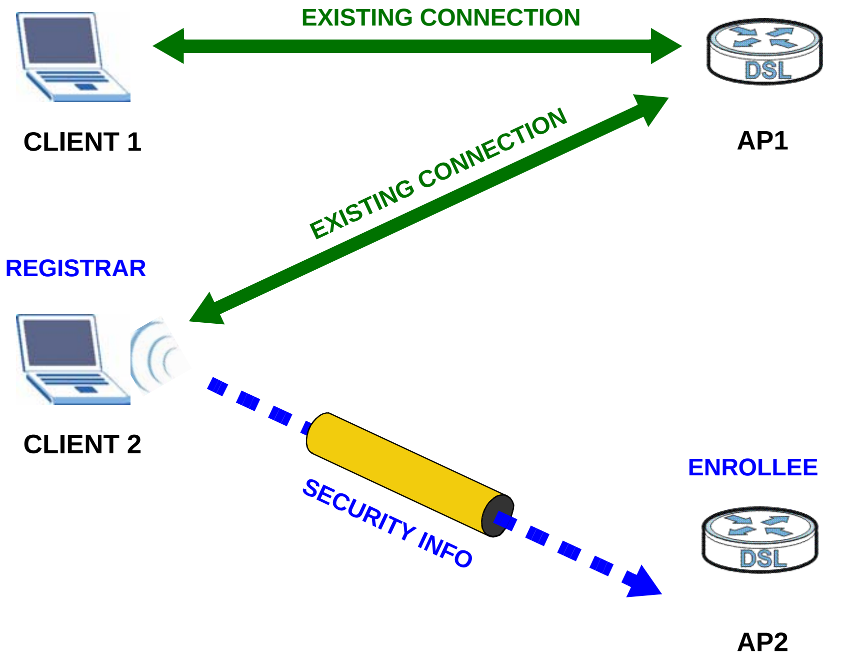
In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the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

Figure 65 WPS: Example Network Step 2



In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

Figure 66 WPS: Example Network Step 3



7.10.4.5 Limitations of WPS

WPS has some limitations of which you should be aware.

- WPS works in Infrastructure networks only (where an AP and a wireless client communicate). It does not work in Ad-Hoc networks (where there is no AP).
- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously, you must enroll one after the other.

  For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way.
- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

  WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices. Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).
- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the “correct” enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

  You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point’s configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the access point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.

8

Network Address Translation (NAT)

8.1 Overview

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

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

8.1.1 What You Can Do in this Chapter

- The **Port Forwarding** screen lets you configure forward incoming service requests to the server(s) on your local network (Section 8.3 on page 134).
- The **Trigger Port** screen lets you change the ZyXEL Device's trigger port settings (Section 8.4 on page 137).
- The **DMZ Host** screen lets you configure a default server (Section 8.5 on page 142).
- The **ALG** screen lets you enable SIP ALG on the ZyXEL Device (Section 8.6 on page 142).

8.2 What You Need to Know

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

NAT

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

Port Forwarding

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

8.3 The Port Forwarding Screen

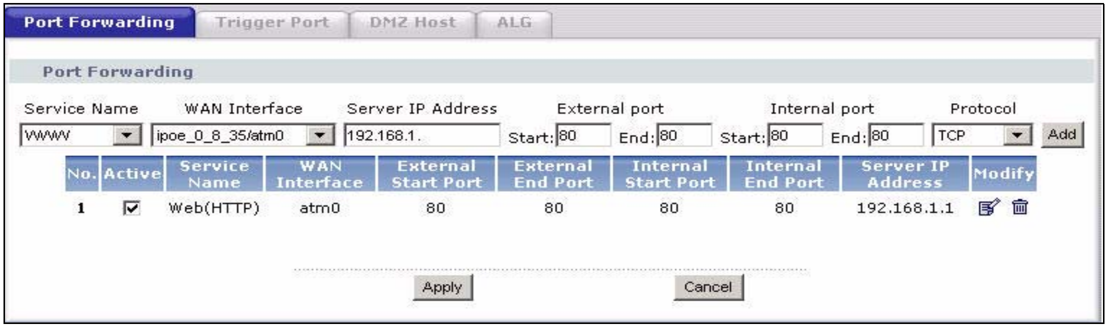
This summary screen provides a summary of all port forwarding rules and their configuration. In addition, this screen allows you to create new port forwarding rules and delete existing rules.

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

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

To access this screen, click **Network > NAT**. The following screen appears.

Figure 67 NAT Port Forwarding



Port Forwarding

Service Name	WAN Interface	Server IP Address	External port		Internal port		Protocol	
WWW	ipoe_0_8_35/atm0	192.168.1.	Start: 80	End: 80	Start: 80	End: 80	TCP	Add

No.	Active	Service Name	WAN Interface	External Start Port	External End Port	Internal Start Port	Internal End Port	Server IP Address	Modify
1	☑	Web(HTTP)	atm0	80	80	80	80	192.168.1.1	✎ 🗑

The following table describes the labels in this screen.

Table 37 NAT Port Forwarding

LABEL	DESCRIPTION
Service Name	Select a pre-defined service from the drop-down list box. The pre-defined service port number(s) and protocol will display in the **External port**, **Internal port** and **Protocol** fields. Otherwise, select **User Define** to open the **Rule Setup** screen where you can manually enter the port number(s) and select the IP protocol.
WAN Interface	Select the WAN interface through which the service is forwarded. You must have already configured a WAN connection with NAT enabled.
Server IP Address	Enter the IP address of the server for the specified service.
External Port Start	Enter the original destination port for the packets. To forward only one port, enter the port number again in the **External Port End** field. To forward a series of ports, enter the start port number here and the end port number in the **External Port End** field.
External Port End	Enter the last port of the original destination port range. To forward only one port, enter the port number in the **External Port Start** field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the **External Port Start** field above.
Internal Port Start	Enter the port number to which you want the ZyXEL Device to translate the incoming port. To forward only one port, enter the port number again in the **Internal Port End** field. For a range of ports, enter the first number of the range to which you want the incoming ports translated.
Internal Port End	Enter the last port of the translated port range.
Protocol	This is the IP protocol.
Add	Click this button to add a rule to the table below.
No.	This is the rule index number (read-only).
Active	This field indicates whether the rule is active or not. Clear the check box to disable the rule. Select the check box to enable it.
Service Name	This field displays the name of the service used by the packets for this virtual server.
WAN Interface	This field displays the WAN interface through which the service is forwarded.
External Start Port	This is the first external port number that identifies a service.
External End Port	This is the last external port number that identifies a service.

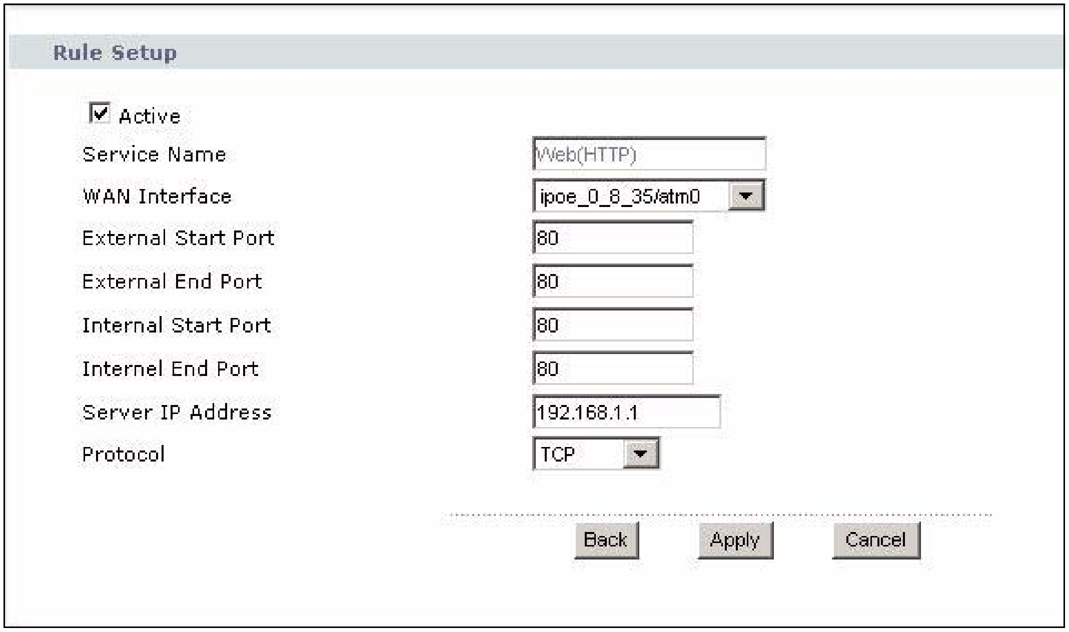
Table 37 NAT Port Forwarding (continued)

LABEL	DESCRIPTION
Internal Start Port	This is the first internal port number that identifies a service.
Internal End Port	This is the last internal port number that identifies a service.
Server IP Address	This field displays the inside IP address of the server.
Modify	Click the **Edit** icon to go to the screen where you can edit the port forwarding rule. Click the **Remove** icon to delete an existing port forwarding rule. Note that subsequent rules move up by one when you take this action.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to return to the previous configuration.

8.3.1 The Port Forwarding Edit Screen

This screen lets you create or edit a port forwarding rule. Select **User Define** in the **Service Name** field or click the rule's **Edit** icon in the **Port Forwarding** screen to open the following screen.

Figure 68 Port Forwarding Edit



Rule Setup

☑ Active

Service Name	Web(HTTP)
WAN Interface	ipoe_0_8_35/atm0
External Start Port	80
External End Port	80
Internal Start Port	80
Internel End Port	80
Server IP Address	192.168.1.1
Protocol	TCP

The following table describes the labels in this screen.

Table 38 Port Forwarding Edit

LABEL	DESCRIPTION
Active	Clear the check box to disable the rule. Select the check box to enable it. This field is not editable if you are configuring a **User Define** rule.
Service Name	Enter a name to identify this rule. This field is read-only if you click the **Edit** icon in the **Port Forwarding** screen.
WAN Interface	Select a WAN interface for which you want to configure port forwarding rules.
External Start Port	Enter the original destination port for the packets. To forward only one port, enter the port number again in the **External End Port** field. To forward a series of ports, enter the start port number here and the end port number in the **External End Port** field.
External End Port	Enter the last port of the original destination port range. To forward only one port, enter the port number in the **External Start Port** field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the **External Start Port** field above.
Internal Start Port	Enter the port number here to which you want the ZyXEL Device to translate the incoming port. For a range of ports, enter the first number of the range to which you want the incoming ports translated.
Internal End Port	Enter the last port of the translated port range.
Server IP Address	Enter the inside IP address of the virtual server here.
Protocol	Select the protocol supported by this virtual server. Choices are **TCP**, **UDP**, or **TCP/UDP**.
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.

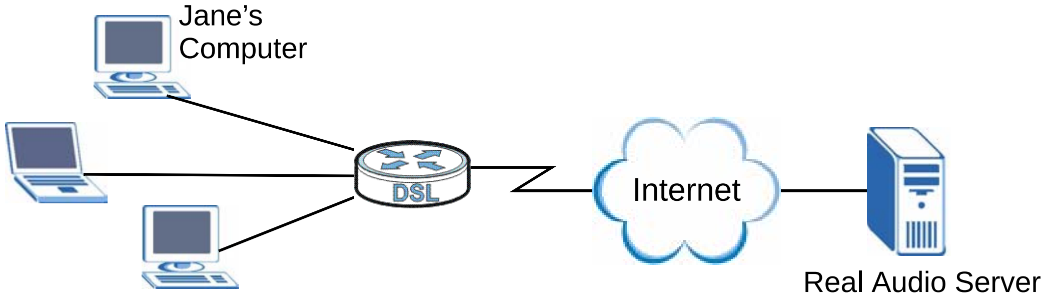
8.4 The Trigger Port Screen

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The ZyXEL Device records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the ZyXEL Device's WAN port receives a response with a specific port number and protocol ("open" port), the ZyXEL Device forwards the traffic to the LAN IP address of the computer that sent the request. After that computer’s connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

For example:

Figure 69 Trigger Port Forwarding Process: Example



1 Jane requests a file from the Real Audio server (port 7070).

2 Port 7070 is a “trigger” port and causes the ZyXEL Device to record Jane’s computer IP address. The ZyXEL Device associates Jane's computer IP address with the "open" port range of 6970-7170.

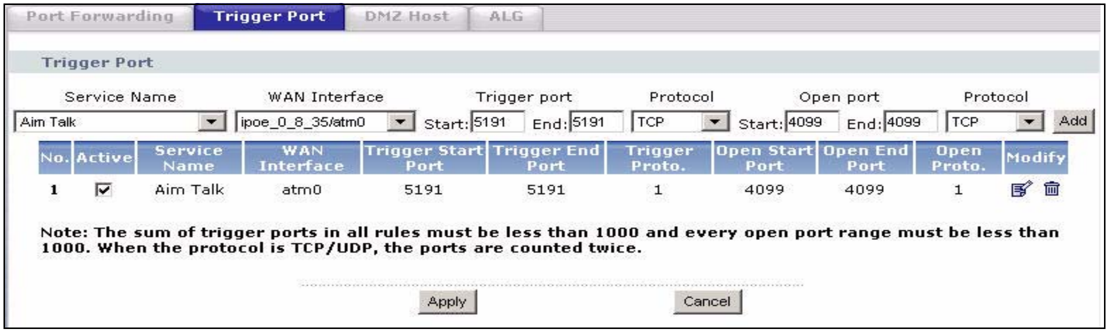
3 The Real Audio server responds using a port number ranging between 6970-7170.

4 The ZyXEL Device forwards the traffic to Jane’s computer IP address.

5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The ZyXEL Device times out in three minutes with UDP (User Datagram Protocol) or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

Click **NAT** > **Trigger Port** to open the following screen. Use this screen to view and configure your ZyXEL Device’s trigger port settings.

Figure 70 Trigger Port



Trigger Port

Service Name: Aim Talk
WAN Interface: ipoe_0_8_35/atm0
Trigger port Start: 5191 End: 5191
Protocol: TCP
Open port Start: 4099 End: 4099
Protocol: TCP

No.	Active	Service Name	WAN Interface	Trigger Start Port	Trigger End Port	Trigger Proto.	Open Start Port	Open End Port	Open Proto.	Modify
1	☑	Aim Talk	atm0	5191	5191	1	4099	4099	1	

Note: The sum of trigger ports in all rules must be less than 1000 and every open port range must be less than 1000. When the protocol is TCP/UDP, the ports are counted twice.

The following table describes the labels in this screen.

Table 39 NAT Trigger Port

LABEL	DESCRIPTION
Service Name	Select a pre-defined service from the drop-down list box. The pre-defined service port number(s) and protocol will display in the **Trigger port**, **Open port** and **Protocol** fields. Otherwise, select **User Define** to open the **Rule Setup** screen where you can manually enter the port number(s) and select the IP protocol.
WAN Interface	Select the WAN interface through which the service is forwarded.
Trigger Port	The trigger port is a port (or a range of ports) that causes (or triggers) the ZyXEL Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start	This is the first port number that identifies a service.
End	This is the last port number that identifies a service.
Protocol	This is the IP protocol.
Open Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ZyXEL Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start	This is the first port number that identifies a service.
End	This is the last port number that identifies a service.
Protocol	This is the IP protocol.
Add	Click this button to add a rule to the table below.
No.	This is the rule index number (read-only).
Active	This field indicates whether the rule is active or not. Clear the check box to disable the rule. Select the check box to enable it.
Server Name	This field displays the name of the service used by the packets for this virtual server.
WAN Interface	This field displays the WAN interface through which the service is forwarded.

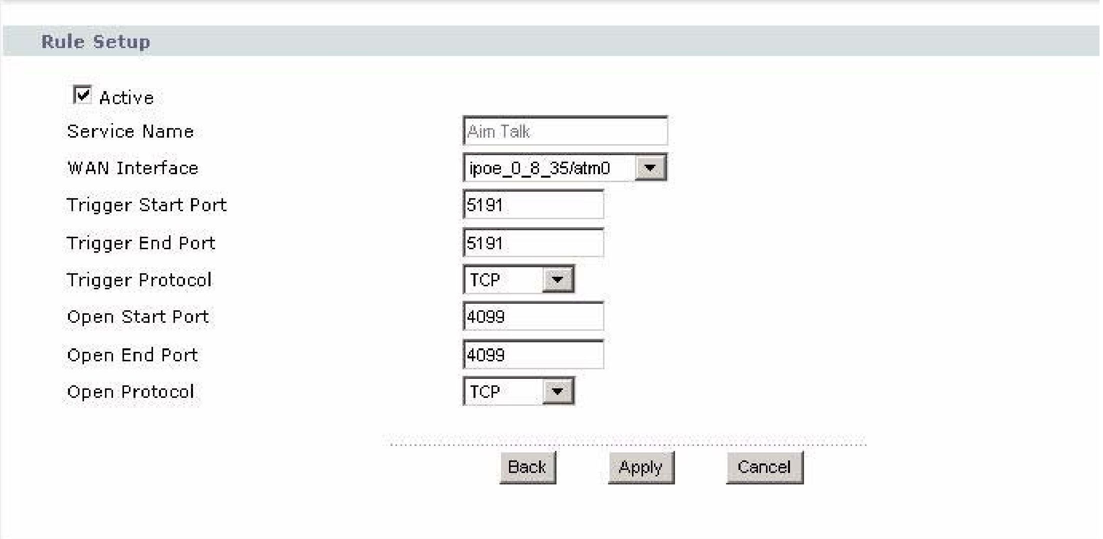
Table 39 NAT Trigger Port (continued)

LABEL	DESCRIPTION
Trigger Start Port	This is the first trigger port number that identifies a service.
Trigger End Port	This is the last trigger port number that identifies a service.
Trigger Proto.	This is the trigger IP protocol. **1** means TCP, **2** means UDP and **3** means TCP/UDP.
Open Start Port	This is the first open port number that identifies a service.
Open End Port	This is the last open port number that identifies a service.
Open Proto.	This is the open IP protocol. **1** means TCP, **2** means UDP and **3** means TCP/UDP.
Modify	Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Remove** icon to delete an existing rule. Note that subsequent rules move up by one when you take this action.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to return to the previous configuration.

8.4.1 Trigger Port Configuration

This screen lets you create new port triggering rules. Click the **Add** icon in the **NAT - Trigger Port** screen to open the following screen.

Figure 71 NAT > Trigger Port > Add



Rule Setup

☑ Active

Service Name	Aim Talk
WAN Interface	ipoe_0_8_35/atm0
Trigger Start Port	5191
Trigger End Port	5191
Trigger Protocol	TCP
Open Start Port	4099
Open End Port	4099
Open Protocol	TCP

The following table describes the labels in this screen.

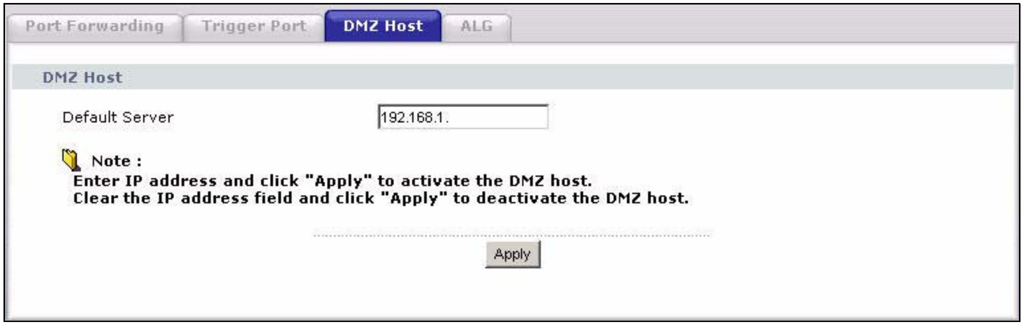
Table 40 NAT > Port Triggering > Add

LABEL	DESCRIPTION
Active	Clear the check box to disable the rule. Select the check box to enable it. This field is not editable if you are configuring a **User Define** rule.
Service Name	Enter a name to identify this rule. This field is read-only if you click the **Edit** icon in the **Trigger Port** screen.
WAN Interface	Select a WAN interface for which you want to configure port triggering rules.
Trigger Start Port	The trigger port is a port (or a range of ports) that causes (or triggers) the ZyXEL Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN. Type a port number or the starting port number in a range of port numbers.
Trigger End Port	Type a port number or the ending port number in a range of port numbers.
Trigger Protocol	Select the IP protocol from **TCP**, **UDP**, or **TCP/UDP**.
Open Start Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ZyXEL Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. Type a port number or the starting port number in a range of port numbers.
Open End Port	Type a port number or the ending port number in a range of port numbers.
Open Protocol	Select the IP protocol from **TCP**, **UDP**, or **TCP/UDP**.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

8.5 The DMZ Host Screen

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

Figure 72 NAT > DMZ Host



Default Server 192.168.1.

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

The following table describes the fields in this screen.

Table 41 NAT > DMZ Host

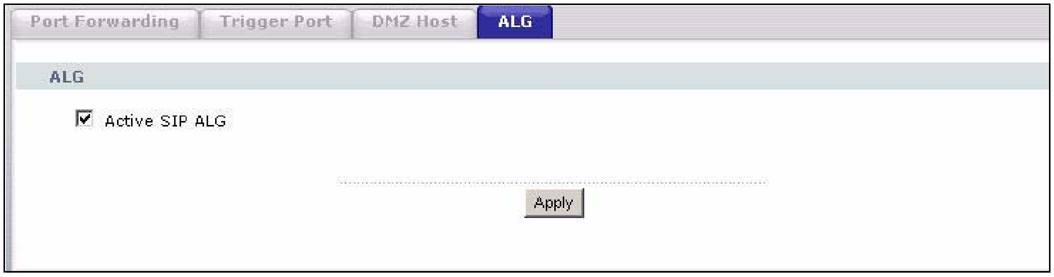
LABEL	DESCRIPTION
Default Server	Enter the IP address of the default server which receives packets from ports that are not specified in the **NAT Port Forwarding** screen. Note: If you do not assign a **Default Server**, the ZyXEL Device discards all packets received for ports that are not specified in the **NAT Port Forwarding** screen.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.

8.6 The ALG Screen

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

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

Figure 73 NAT > ALG



☑ Active SIP ALG

Each field is described in the following table.

Table 42 NAT > ALG

LABEL	DESCRIPTION
Active SIP ALG	Select this check box to allow SIP sessions to pass through the ZyXEL Device. SIP is a signaling protocol used in VoIP (Voice over IP), the sending of voice signals over Internet Protocol.
Apply	Click **Apply** to save your customized settings.

8.7 Technical Reference

The following section contains additional technical information about the ZyXEL Device features described in this chapter.

Port Forwarding: Services and Port Numbers

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Please also refer to the Supporting CD for more examples and details on port forwarding and NAT.

Table 43 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

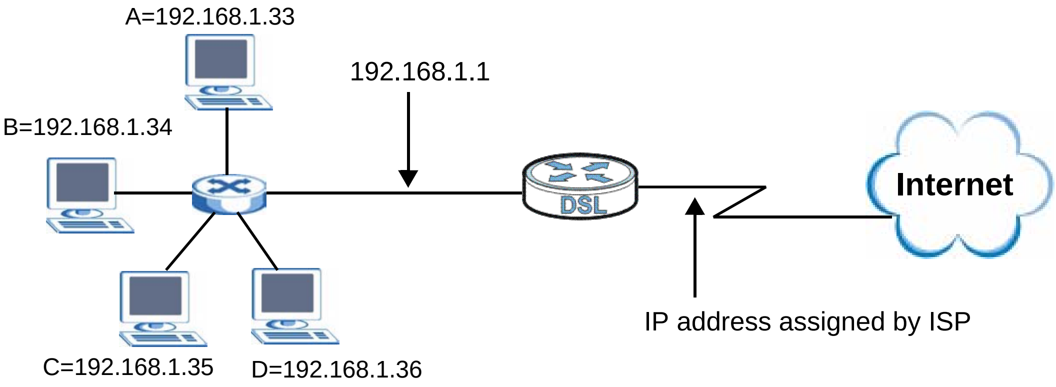
Table 43 Services and Port Numbers

SERVICES	PORT NUMBER
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

Port Forwarding Example

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

Figure 74 Multiple Servers Behind NAT Example



PART III

Security

9

Firewall

9.1 Overview

This chapter shows you how to enable and configure the ZyXEL Device firewall settings.

The ZyXEL Device firewall is a packet filtering firewall and restricts access based on the source/destination computer network address of a packet and the type of application.

9.1.1 What You Can Do in this Chapter

The **Incoming** screen lets you view and configure incoming IP filtering rules (Section 9.3 on page 148).

9.2 What You Need to Know

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

Basics

Computers share information over the Internet using a common language called TCP/IP. TCP/IP, in turn, is a set of application protocols that perform specific functions. An “extension number”, called the "TCP port" or "UDP port" identifies these protocols, such as HTTP (Web), FTP (File Transfer Protocol), POP3 (E-mail), etc. For example, Web traffic by default uses TCP port 80.

When computers communicate on the Internet, they are using the client/server model, where the server "listens" on a specific TCP/UDP port for information requests from remote client computers on the network. For example, a Web server typically listens on port 80. Please note that while a computer may be intended for use over a single port, such as Web on port 80, other ports are also active. If the person configuring or managing the computer is not careful, a hacker could attack it over an unprotected port.

Some of the most common IP ports are:

Table 44 Common IP Ports

21	FTP	53	DNS
23	Telnet	80	HTTP
25	SMTP	110	POP3

Default Filtering Policies

Filtering rules are grouped based on the direction of travel of packets to which they apply.

The default rule for incoming traffic blocks all incoming connections from the WAN to the LAN. If you wish to allow certain WAN users to have access to your LAN, you will need to create custom rules to allow it.

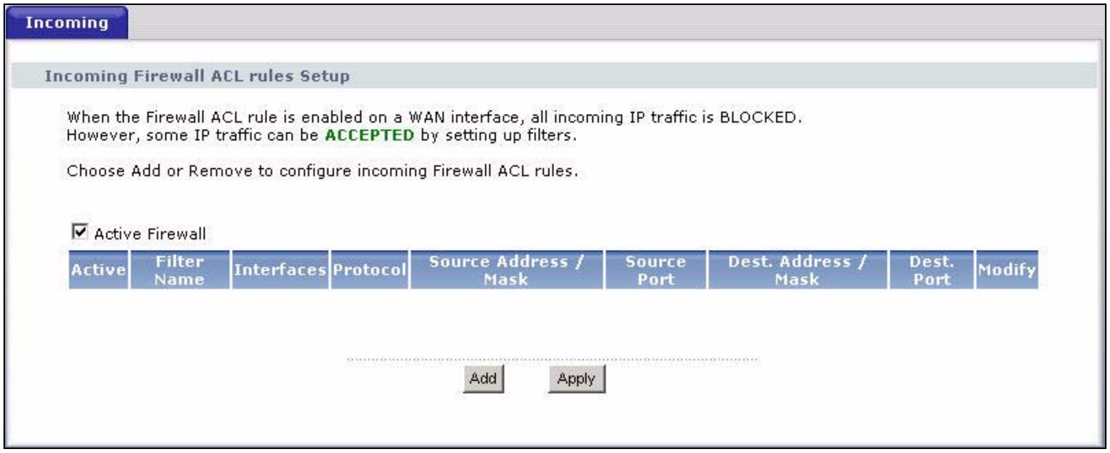
Note: If you configure filtering rules without a good understanding of how they work, you might inadvertently introduce security risks to the firewall and to the protected network. Make sure you test your rules after you configure them.

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

9.3 The Firewall Screen

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

Figure 75 Firewall > Incoming



Incoming Firewall ACL rules Setup

When the Firewall ACL rule is enabled on a WAN interface, all incoming IP traffic is BLOCKED.
However, some IP traffic can be ACCEPTED by setting up filters.

Choose Add or Remove to configure incoming Firewall ACL rules.

☑ Active Firewall

Active	Filter Name	Interfaces	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Modify

The following table describes the labels in this screen.

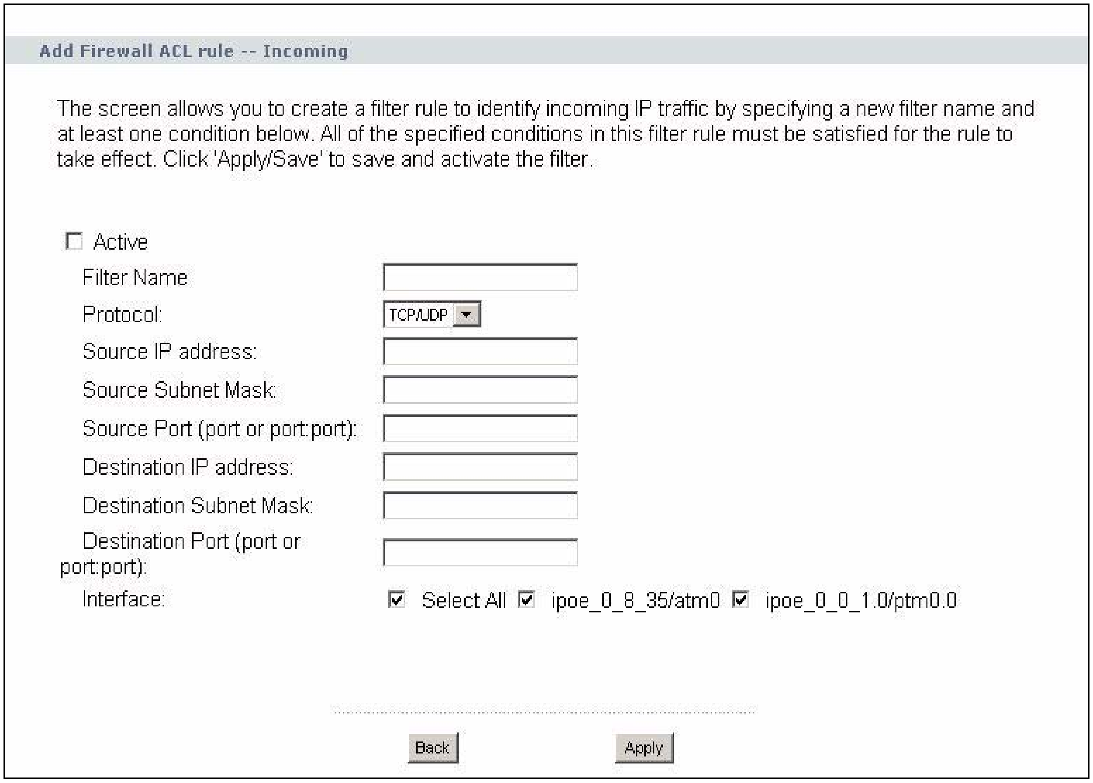
Table 45 Firewall > Incoming

LABEL	DESCRIPTION
Active Firewall	Select this check box to enable the firewall on the ZyXEL Device. When the firewall is enabled, the ZyXEL Device blocks all incoming traffic from the WAN to the LAN. Create custom rules below to allow certain WAN users to access your LAN or to allow traffic from the WAN to a certain computer on the LAN.
Active	Select this check box to enable the rule.
Filter Name	This displays the name of the rule.
Interfaces	This displays the WAN interface(s) to which this rule is applied.
Protocol	This displays the IP protocol that defines the service to which this rule applies.
Source Address / Mask	This displays the source IP addresses and subnet mask to which this rule applies. Please note that a blank source address is equivalent to **Any**.
Source Port	This is the source port number.
Dest. Address / Mask	This displays the destination IP addresses and subnet mask to which this rule applies. Please note that a blank destination address is equivalent to **Any**.
Dest. Port	This is the destination port number.
Modify	Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Remove** icon to delete an existing rule. Note that subsequent rules move up by one when you take this action.
Add	Click **Add** to create a new rule.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.

9.3.1 Creating Incoming Firewall Rules

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

Figure 76 Firewall > Incoming: Add



Add Firewall ACL rule -- Incoming

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

□ Active

Filter Name:

Protocol: TCP/UDP

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

Interface: ☑ Select All ☑ ipoe_0_8_35/atm0 ☑ ipoe_0_0_1.0/ptm0.0

The following table describes the labels in this screen.

Table 46 Firewall > Incoming: Add

LABEL	DESCRIPTION
Active	Select this check box to enable the rule.
Filter Name	Enter a descriptive name of up to 16 printable English keyboard characters, including spaces. To add a firewall rule, you need to configure at least one of the following fields (except the **Interface** field).
Protocol	Select the IP protocol (**TCP/UDP**, **TCP**, **UDP** or **ICMP**) and enter the protocol (service type) number in the port field. Select **NONE** to apply the rule to any protocol.
Source IP Address	Enter the source IP address in dotted decimal notation.
Source Subnet Mask	Enter the source subnet mask.
Source Port	Enter a single port number or the range of port numbers of the source.
Destination IP Address	Enter the destination IP address in dotted decimal notation.

Table 46 Firewall > Incoming: Add (continued)

LABEL	DESCRIPTION
Destination Subnet Mask	Enter the destination subnet mask.
Destination Port	Enter the port number of the destination.
Interface	Select **Select All** to apply the rule to all interfaces on the ZyXEL Device or select the specific WAN interface(s) to which this rule applies.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your customized settings and exit this screen.

10

Certificate

10.1 Overview

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

10.1.1 What You Can Do in this Chapter

- The **Local Certificates** screen lets you generate certification requests and import the ZyXEL Device's CA-signed certificates (Section 10.4 on page 161).
- The **Trusted CA** screen lets you save the certificates of trusted CAs to the ZyXEL Device (Section 10.4 on page 161).

10.2 What You Need to Know

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

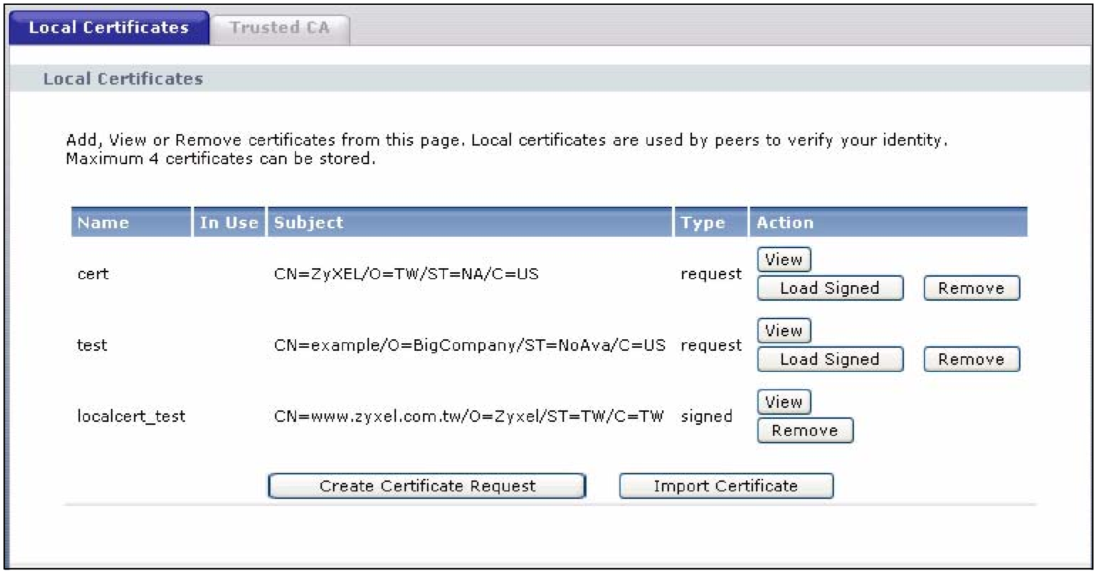
Certification Authority

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

10.3 The Local Certificates Screen

Click **Security > Certificates** to open the **Local Certificates** screen. This is the ZyXEL Device's summary list of certificates and certification requests.

Figure 77 Local Certificates



Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity.
Maximum 4 certificates can be stored.

Name	In Use	Subject	Type	Action
cert		CN=ZyXEL/O=TW/ST=NA/C=US	request	View Load Signed Remove
test		CN=example/O=BigCompany/ST=NoAva/C=US	request	View Load Signed Remove
localcert_test		CN=www.zyxel.com.tw/O=Zyxel/ST=TW/C=TW	signed	View Remove

The following table describes the labels in this screen.

Table 47 Local Certificates

LABEL	DESCRIPTION
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
In Use	This field displays how many applications use the certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Type	This field displays what kind of certificate this is. **request** represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the **Load Certificate** screen to import the certificate and replace the request. **signed** represents a certificate issued by a certification authority.
Modify	Click the **View** button to open a screen with an in-depth list of information about the certificate (or certification request). Click the **Load Signed** button to import a valid certification to replace the request. Click the **Remove** button to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

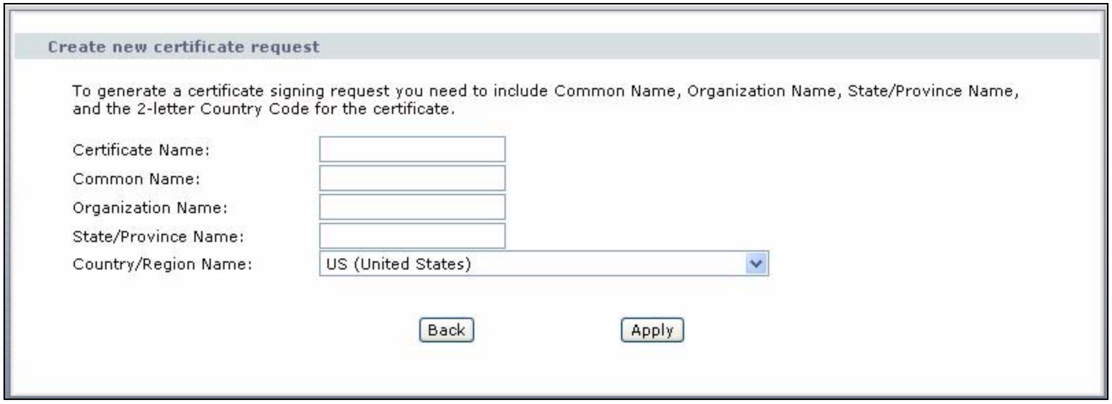
Table 47 Local Certificates (continued)

LABEL	DESCRIPTION
Create Certificate Request	Click this button to go to the screen where you can have the ZyXEL Device generate a certification request.
Import Certificate	Click this button to open a screen where you can save the certificate that you have enrolled from a certification authority from your computer to the ZyXEL Device.

10.3.1 Create Certificate Request

Click **Security** > **Certificates** > **Local Certificates** and then **Create Certificate Request** to open the **My Certificate Create** screen. Use this screen to have the ZyXEL Device generate a certification request.

Figure 78 Create Certificate Request



Create new certificate request

To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate.

Certificate Name:

Common Name:

Organization Name:

State/Province Name:

Country/Region Name: US (United States)

The following table describes the labels in this screen.

Table 48 Create Certificate Request

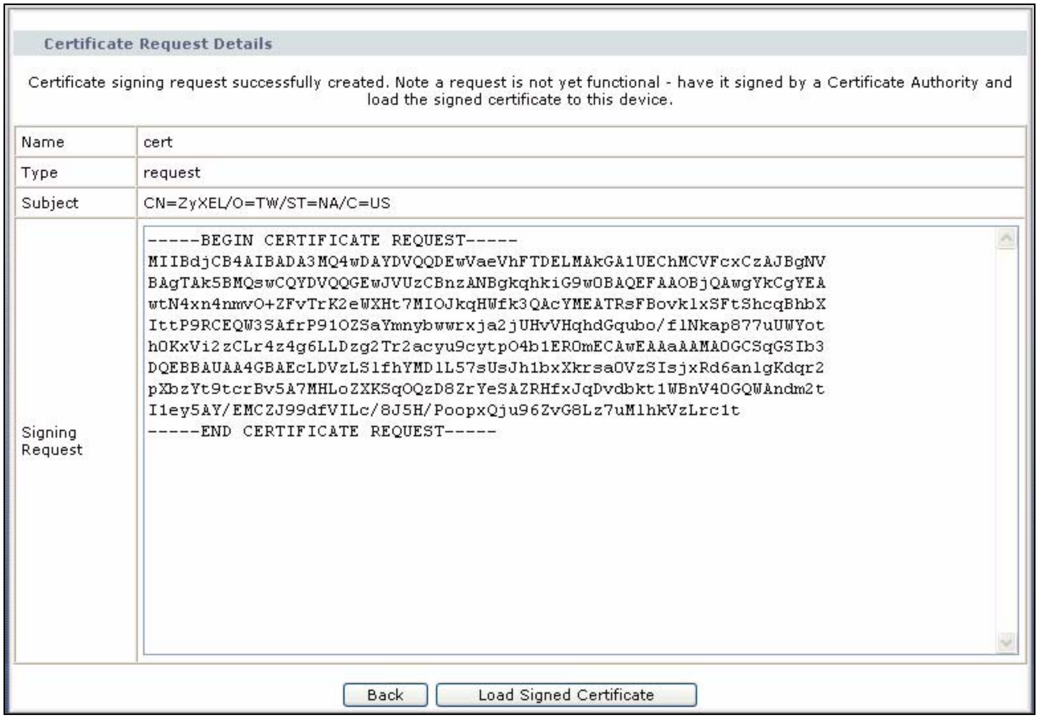
LABEL	DESCRIPTION
Certificate Name	Type up to 31 ASCII characters (not including spaces) to identify this certificate.
Common Name	Select a radio button to identify the certificate’s owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 31 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Organization Name	Type up to 127 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
State/Province Name	Type up to 127 characters to identify the state or province where the certificate owner is located. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
Country/Region Name	Select a country to identify the nation where the certificate owner is located.

Table 48 Create Certificate Request (continued)

LABEL	DESCRIPTION
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to begin certificate or certification request generation.

After you click **Apply**, the **Certificate Request Details** screen displays. Click **Load Signed Certificate** to import a certificate signed by the CA to replace the request (see Section 10.3.4 on page 160). Otherwise, click **Back** to return to the **Local Certificates** screen. See Section 10.3.3 on page 158 for field information.

Figure 79 Certificate Request Details



Certificate Request Details

Certificate signing request successfully created. Note a request is not yet functional - have it signed by a Certificate Authority and load the signed certificate to this device.

Name	cert
Type	request
Subject	CN=ZyXEL/O=TW/ST=NA/C=US
Signing Request	

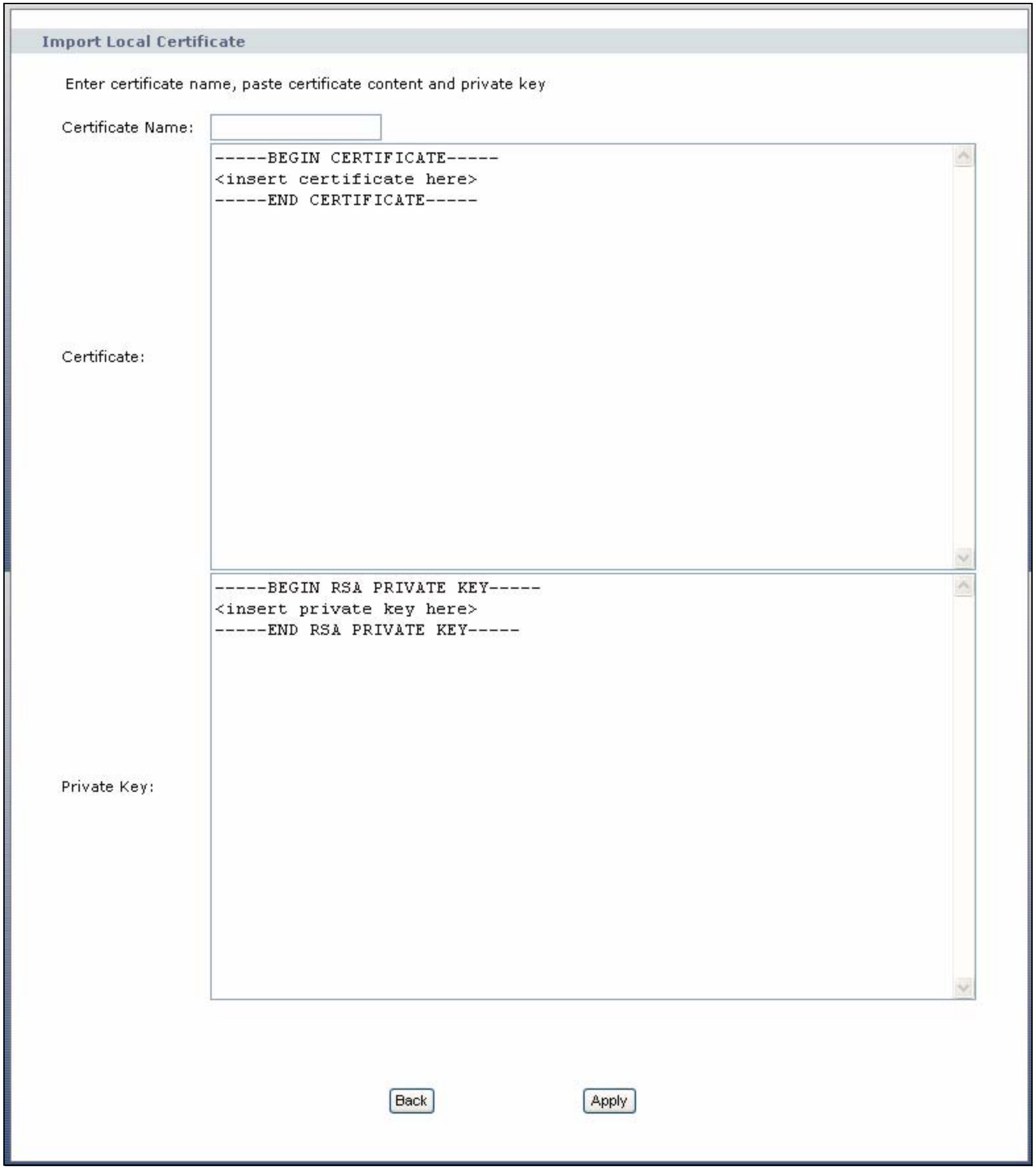
```
-----BEGIN CERTIFICATE REQUEST-----
MIIBdjCB4AIBADA3MQ4wDAYDVQQDEwVaeVhFTDELMAkGA1UEChMCVFcxCzAJBgNV
BAgTAk5BMQswCQYDVQQGEwJVUzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
wtN4xn4nmvO+ZFvTrK2eWXHt7MIOJkqHWfk3QAcYMEATRsFBovklxSFtShcqBhbX
IttP9RCEQW3SAfrP91OZSaYmnybwwrxja2jUHvVHqhdGqubo/flNkap877uUWYot
hOKxVi2zCLr4z4g6LLDzg2Tr2acyu9cytpO4b1EROmECAwEAAaAAMA0GCSqGSIb3
DQEBBAUAA4GBAEcLDVzLSlfhYMDlL57sUsJh1bxXkrsa0VzSIsjxRd6anlgKdqr2
pXbzYt9tcrBv5A7MHLoZXKSqOQzD8ZrYeSAZRHfxJqDvdbkt1WBnV4OGQWAndm2t
I1ey5AY/EMCZJ99dfVILc/8J5H/PoopxQju96ZvG8Lz7uMlhkVzLrc1t
-----END CERTIFICATE REQUEST-----
```

10.3.2 Import Certificate

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

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

Figure 80 Import Local Certificate



Import Local Certificate

Enter certificate name, paste certificate content and private key

Certificate Name:

Certificate:

```
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
```

Private Key:

```
-----BEGIN RSA PRIVATE KEY-----
<insert private key here>
-----END RSA PRIVATE KEY-----
```

The following table describes the labels in this screen.

Table 49 Import Local Certificate

LABEL	DESCRIPTION
Certificate Name	Type up to 31 ASCII characters (not including spaces) to identify this certificate.
Certificate	Copy and paste the certificate into the text box to store it on the ZyXEL Device.

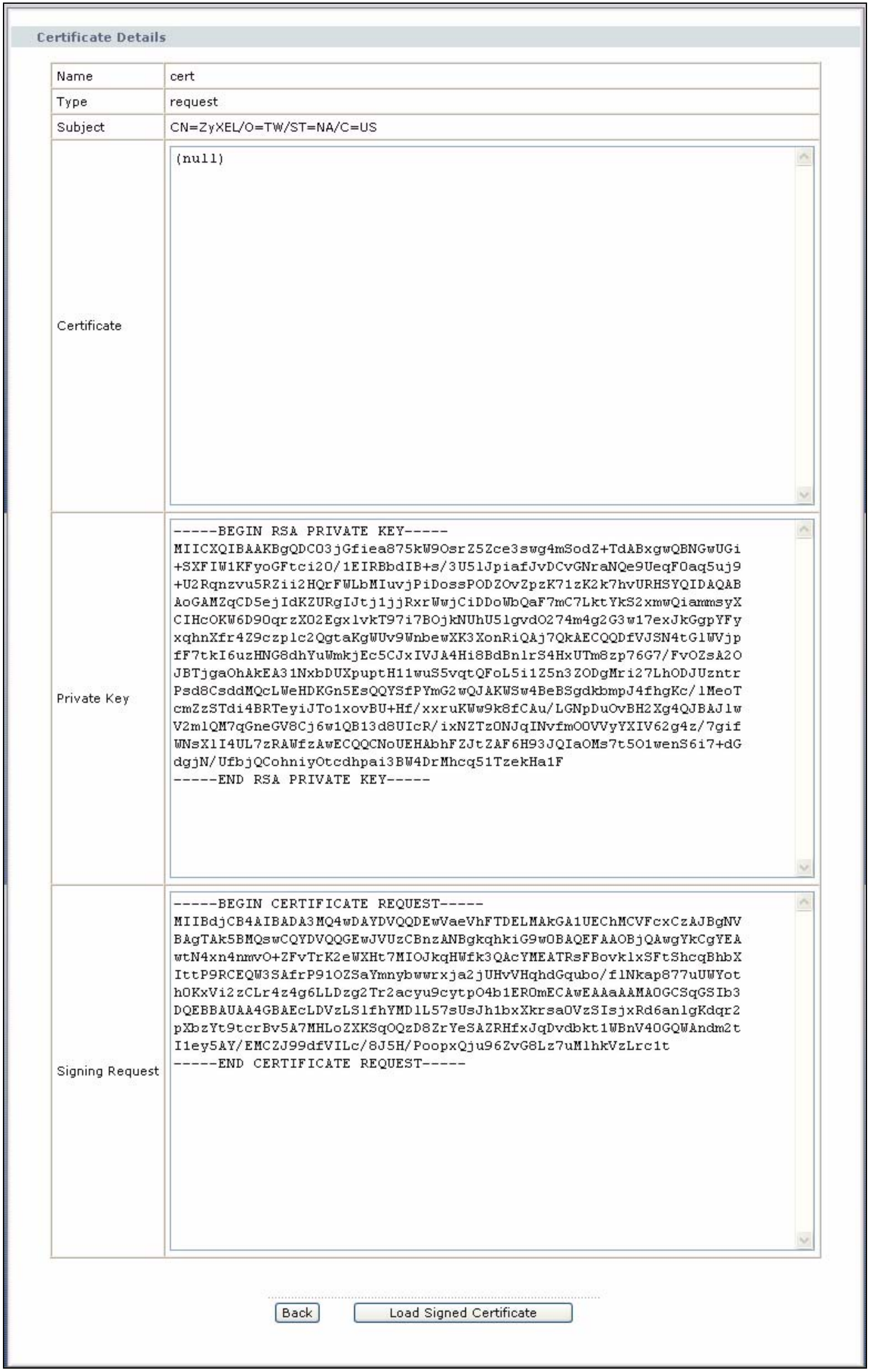
Table 49 Import Local Certificate

LABEL	DESCRIPTION
Private Key	Copy and paste the private key into the text box to store it on the ZyXEL Device.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save the certificate on the ZyXEL Device.

10.3.3 Certificate Details

Click **Security** > **Certificates** > **Local Certificates** to open the **My Certificates** screen (see Figure 77 on page 154). Click the **View** icon to open the **Certificate Details** screen. Use this screen to view in-depth certificate information and change the certificate's name.

Figure 81 Certificate Details



Certificate Details

Name	cert
Type	request
Subject	CN=ZyXEL/O=TW/ST=NA/C=US

Certificate

```
(null)
```

Private Key

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDCO3jGfiea875kW9OsrZ5Zce3swg4mSodZ+TdABxgwQBNGwUGi
+SXFIW1KFyoGFtci2O/1EIRBbdIB+s/3U5lJpiafJvDCvGNraNQe9UeqFOaq5uj9
+U2Rqnzvu5RZii2HQrFWLbMIuvjPiDossPODZOvZpzK71zK2k7hvURHSYQIDAQAB
AoGAMZqCD5ejIdKZURgIJtj1jjRxrWwjCiDDoWbQaF7mC7LktYkS2xmwQiammsyX
CIHcOKW6D9OqrzXO2Egx1vkT97i7BOjkNUhU5lgvdO274m4g2G3w17exJkGgpYFy
xqhnXfr4Z9czplc2QgtaKgWUv9WnbewXK3XonRiQAj7QkAECQQDfVJSN4tGlWVjp
fF7tkI6uzHNG8dhYuWmkjEc5CJxIVJA4Hi8BdBnlrS4HxUTm8zp76G7/FvOZsA2O
JBTjgaOhAkEA31NxbDUXpuptH11wuS5vqtQFoL5i1Z5n3ZODgMri27LhODJUzntr
Psd8CsddMQcLWeHDKGn5EsQQYSfPYmG2wQJAKWSw4BeBSgdkbmpJ4fhgKc/lMeoT
cmZzSTdi4BRTeyiJTo1xovBU+Hf/xxruKWw9k8fCAu/LGNpDuOvBH2Xg4QJBAJlw
V2mlQM7qGneGV8Cj6w1QB13d8UIcR/ixNZTzONJqINvfmOOVVyYXIV62g4z/7gif
WNsXlI4UL7zRAWfzAwECQQCNoUEHAbhFZJtZAF6H93JQIaOMs7t5O1wenS6i7+dG
dgjN/UfbjQCohniyOtcdhpai3BW4DrMhcq51TzekHa1F
-----END RSA PRIVATE KEY-----
```

Signing Request

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBdjCB4AIBADA3MQ4wDAYDVQQDEwVaeVhFTDELMAkGA1UEChMCVFcxCzAJBgNV
BAgTAk5BMQswCQYDVQQGEwJVUzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
wtN4xn4nmvO+ZFvTrK2eWXHt7MIOJkqHWfk3QAcYMEATRsFBovklxSFtShcqBhbX
IttP9RCEQW3SAfrP91OZSaYmnybwwrxja2jUHvVHqhdGqubo/flNkap877uUWYot
hOKxVi2zCLr4z4g6LLDzg2Tr2acyu9cytpO4b1EROmECAwEAAaAAMA0GCSqGSIb3
DQEBBAUAA4GBAEcLDVzLSlfhYMDlL57sUsJh1bxXkrsaOVzSIsjxRd6anlgKdqr2
pXbzYt9tcrBv5A7MHLoZXKSqOQzD8ZrYeSAZRHfxJqDvdbkt1WBnV4OGQWAndm2t
I1ey5AY/EMCZJ99dfVILc/8J5H/PoopxQju96ZvG8Lz7uMlhkVzLrc1t
-----END CERTIFICATE REQUEST-----
```

Back Load Signed Certificate

The following table describes the labels in this screen.

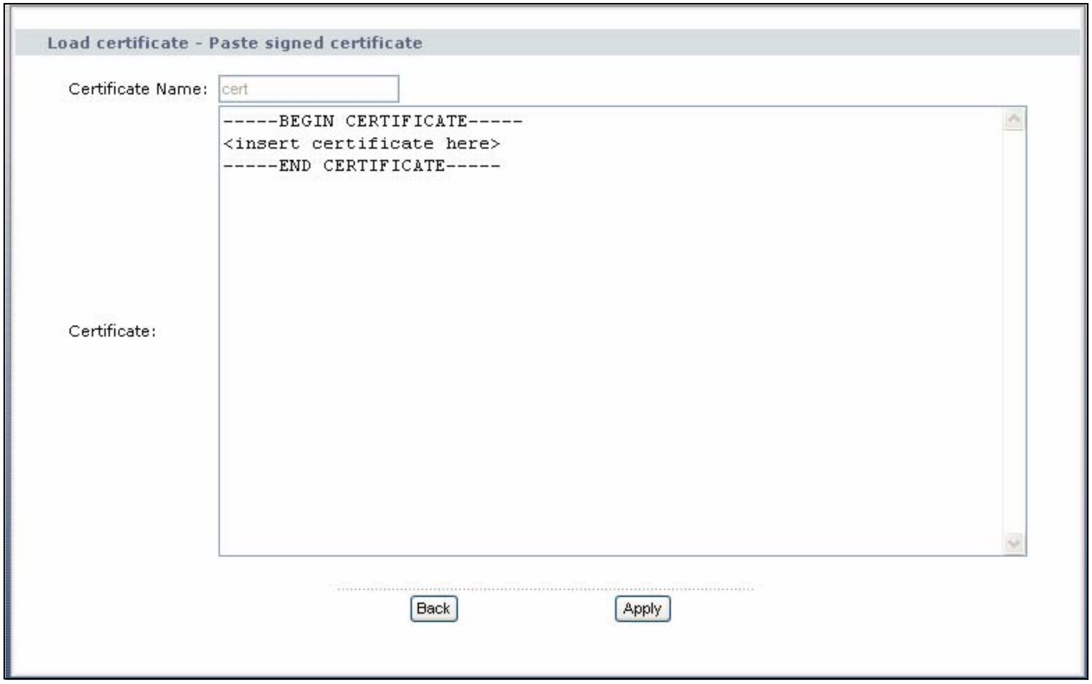
Table 50 Certificate Details

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this certificate. You may use any character (not including spaces).
Type	This field displays general information about the certificate. **signed** means that a Certification Authority signed the certificate. **request** means this is a certification request.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organization (O), State (ST) and Country (C).
Certificate	This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. This displays **null** in a certification request. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Private Key	This read-only text box displays the private key in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the private key into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Signing Request	This read-only text box displays the request information in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. This displays **null** in a signed certificate.
Back	Click **Back** to return to the previous screen.
Load Signed Certificate	This button is available only in a certification request details screen Click this to import a certificate signed by the CA to replace the request.

10.3.4 Load Signed Certificate

Click **Security > Certificates > Local Certificates** and then **Load Signed** or the **Load Signed Certificate** button in the **Certificate Details** screen of a certification request to open the **Load Certificate** screen. Follow the instructions in this screen to save a valid certificate to replace the request.

Figure 82 Load Certificate



Load certificate - Paste signed certificate

Certificate Name: cert

Certificate:

```
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
```

The following table describes the labels in this screen.

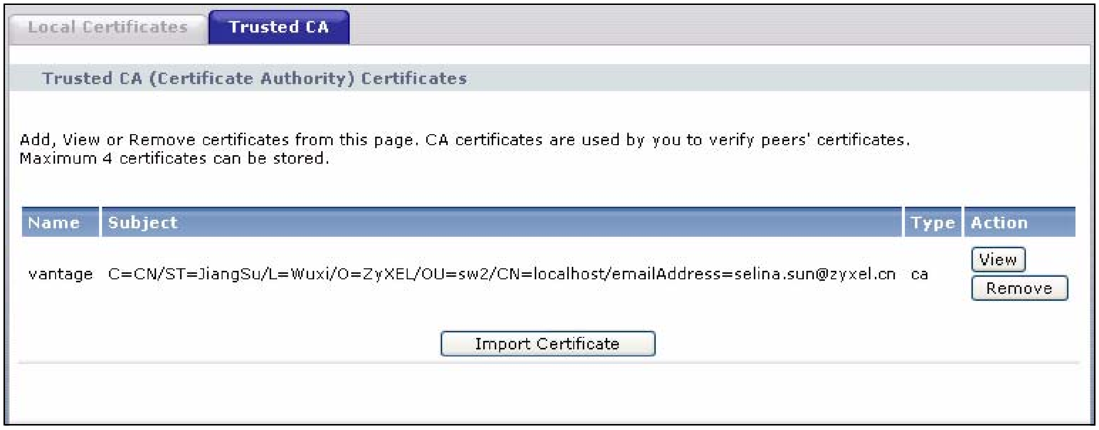
Table 51 Load Certificate

LABEL	DESCRIPTION
Certificate Name	This field is read-only and displays the identifying name of this certificate.
Certificate	Copy and paste the certificate into the text box to store it on the ZyXEL Device.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save the certificate on the ZyXEL Device.

10.4 The Trusted CA Screen

Click **Advanced Setup > Certificates > Trusted CA** to open the following screen. This screen displays a summary list of certificates of the certification authorities that you have set the ZyXEL Device to accept as trusted. The ZyXEL Device accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

Figure 83 Trusted CA



Trusted CA (Certificate Authority) Certificates

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates.
Maximum 4 certificates can be stored.

Name	Subject	Type	Action
vantage	C=CN/ST=JiangSu/L=Wuxi/O=ZyXEL/OU=sw2/CN=localhost/emailAddress=selina.sun@zyxel.cn	ca	View Remove

The following table describes the fields in this screen.

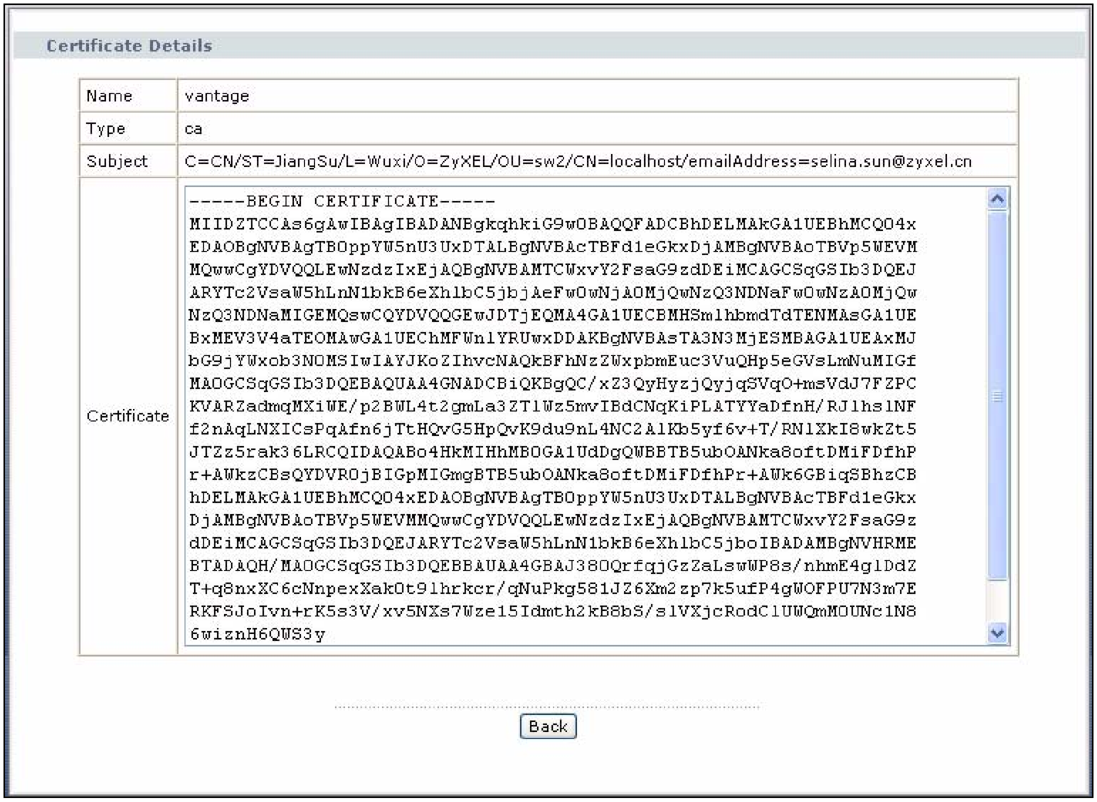
Table 52 Trusted CA

LABEL	DESCRIPTION
Name	This field displays the name used to identify this certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), OU (Organizational Unit or department), Organization (O), State (ST) and Country (C). It is recommended that each certificate have unique subject information.
Type	This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate.
Action	Click **View** to open a screen with an in-depth list of information about the certificate. Click **Remove** to delete the certificate.
Import Certificate	Click this button to open a screen where you can save the certificate of a certification authority that you trust to the ZyXEL Device.

10.4.1 View Trusted CA Certificate

Click the **View** button in the **Trusted CA** screen to open the following screen. Use this screen to view in-depth information about the certification authority’s certificate.

Figure 84 Trusted CA: View



Certificate Details

Name	vantage
Type	ca
Subject	C=CN/ST=JiangSu/L=Wuxi/O=ZyXEL/OU=sw2/CN=localhost/emailAddress=selina.sun@zyxel.cn
Certificate	(see below)

```
-----BEGIN CERTIFICATE-----
MIIDZTCCAs6gAwIBAgIBADANBgkqhkiG9w0BAQQFADCBhDELMAkGA1UEBhMCQ04x
EDAOBgNVBAgTB0ppYW5nU3UxDTALBgNVBAcTBFd1eGkxDjAMBgNVBAoTBVp5WEVM
MQwwCgYDVQQLEwNzdzIxEjAQBgNVBAMTCWxvY2FsaG9zdDEiMCAGCSqGSIb3DQEJ
ARYTc2VsaW5hLnN1bkB6eXhlbC5jbjAeFw0wNjA0MjQwNzQ3NDNaFw0wNzA0MjQw
NzQ3NDNaMIGEMQswCQYDVQQGEwJDTjEQMA4GA1UECBMHSmlhbmdTdTENMAsGA1UE
BxMEV3V4aTEOMAwGA1UEChMFWnlYRUwxDDAKBgNVBAsTA3N3MjESMBAGA1UEAxMJ
bG9jYWxob3N0MSIwIAYJKoZIhvcNAQkBFhNzZWxpbmEuc3VuQHp5eGVsLmNuMIGf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/xZ3QyHyzjQyjqSVqO+msVdJ7FZPC
KVARZadmqMXiWE/p2BWL4t2gmLa3ZTlWz5mvIBdCNqKiPLATYYaDfnH/RJlhslNF
f2nAqLNXICsPqAfn6jTtHQvG5HpQvK9du9nL4NC2AlKb5yf6v+T/RNlXkI8wkZt5
JTZz5rak36LRCQIDAQABo4HkMIHhMB0GA1UdDgQWBBTB5ubOANka8oftDMiFDfhP
r+AWkzCBsQYDVR0jBIGpMIGmgBTB5ubOANka8oftDMiFDfhPr+AWk6GBiqSBhzCB
hDELMAkGA1UEBhMCQ04xEDAOBgNVBAgTB0ppYW5nU3UxDTALBgNVBAcTBFd1eGkx
DjAMBgNVBAoTBVp5WEVMMQwwCgYDVQQLEwNzdzIxEjAQBgNVBAMTCWxvY2FsaG9z
dDEiMCAGCSqGSIb3DQEJARYTc2VsaW5hLnN1bkB6eXhlbC5jboIBADAMBgNVHRME
BTADAQH/MA0GCSqGSIb3DQEBBAUAA4GBAJ38OQrfqjGzZaLswWP8s/nhmE4glDdZ
T+q8nxXC6cNnpexXak0t9lhrkcr/qNuPkg581JZ6Xm2zp7k5ufP4gWOFPU7N3m7E
RKFSJoIvn+rK5s3V/xv5NXs7Wze15Idmth2kB8bS/slVXjcRodClUWQmMOUNc1N8
6wiznH6QWS3y
```

The following table describes the fields in this screen.

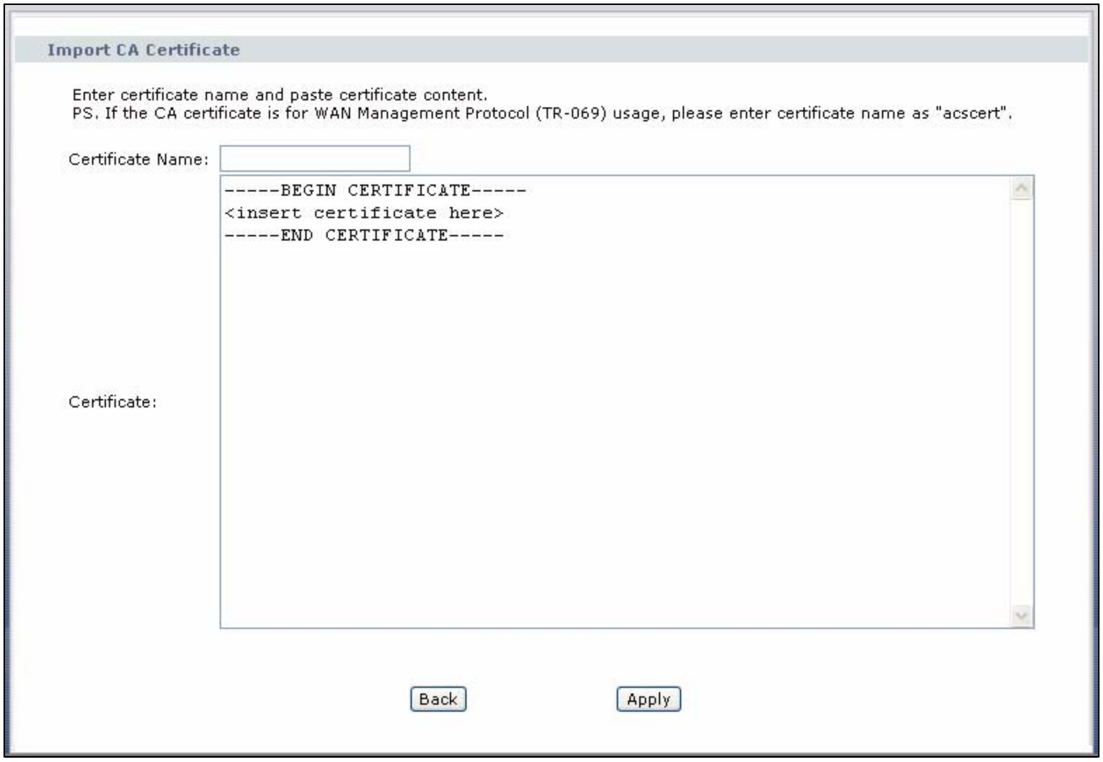
Table 53 Trusted CA: View

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate.
Type	This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Certificate	This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Back	Click this button to return to the previous screen.

10.4.2 Import Trusted CA Certificate

Click the **Import Certificate** button in the **Trusted CA** screen to open the following screen. The ZyXEL Device trusts any valid certificate signed by any of the imported trusted CA certificates.

Figure 85 Trusted CA: Import Certificate



Import CA Certificate

Enter certificate name and paste certificate content.
PS. If the CA certificate is for WAN Management Protocol (TR-069) usage, please enter certificate name as "acscert".

Certificate Name:

Certificate:

```
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
```

The following table describes the fields in this screen.

Table 54 Trusted CA: Import Certificate

LABEL	DESCRIPTION
Certificate Name	Enter the name that identifies this certificate.
Certificate	Copy and paste the certificate into the text box to store it on the ZyXEL Device.
Back	Click this button to return to the previous screen.
Apply	Click this button to save your changes back to the ZyXEL Device.

PART IV
Advanced

11

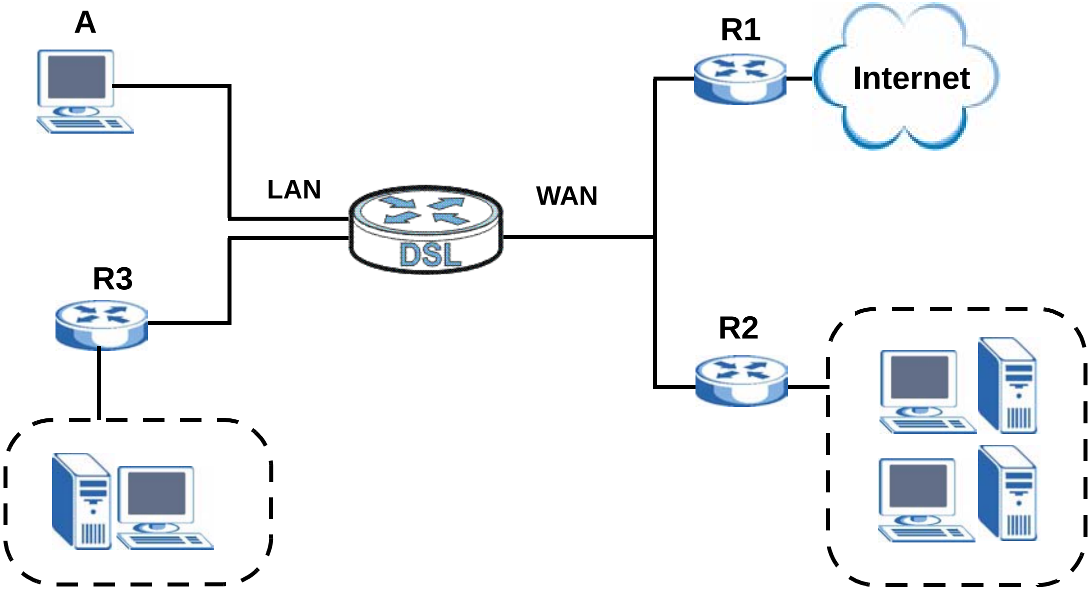
Static Route

11.1 Overview

The ZyXEL Device usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the ZyXEL Device send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the ZyXEL Device's LAN interface. The ZyXEL Device routes most traffic from **A** to the Internet through the ZyXEL Device's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the LAN.

Figure 86 Example of Static Routing Topology



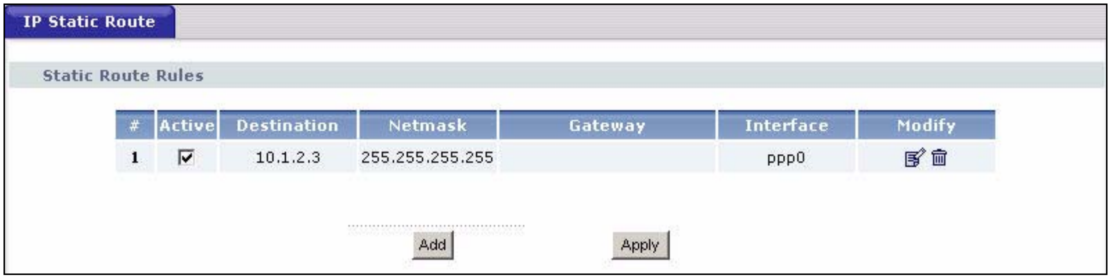
11.1.1 What You Can Do in this Chapter

The **Static Route** screens let you view and configure IP static routes on the ZyXEL Device (Section 11.2 on page 168).

11.2 The Static Route Screen

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

Figure 87 Advanced > Static Route



#	Active	Destination	Netmask	Gateway	Interface	Modify
1	☑	10.1.2.3	255.255.255.255		ppp0	

The following table describes the labels in this screen.

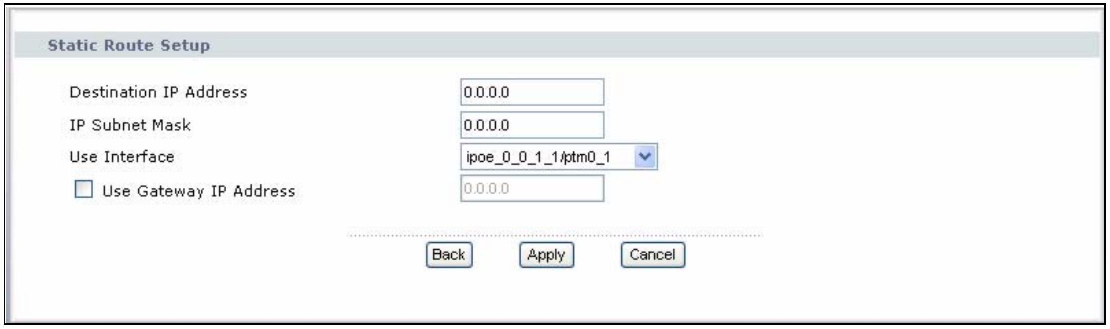
Table 55 Advanced > Static Route

LABEL	DESCRIPTION
#	This is the number of an individual static route.
Active	This field indicates whether the rule is active or not. Clear the check box to disable the rule. Select the check box to enable it.
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Netmask	This parameter specifies the IP network subnet mask of the final destination.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Interface	This is the WAN interface through which the traffic is routed.
Modify	Click the Edit icon to go to the screen where you can set up a static route on the ZyXEL Device. Click the Remove icon to remove a static route from the ZyXEL Device. A window displays asking you to confirm that you want to delete the route.
Add	Click this to create a new rule.
Apply	Click this to apply your changes to the ZyXEL Device.

11.2.1 Static Route Edit

Click the **Add** button in the **Static Route** screen. Use this screen to configure the required information for a static route.

Figure 88 Static Route: Add



Static Route Setup

Destination IP Address	0.0.0.0
IP Subnet Mask	0.0.0.0
Use Interface	ipoe_0_0_1_1/ptm0_1
□ Use Gateway IP Address	0.0.0.0

The following table describes the labels in this screen.

Table 56 Static Route: Add

LABEL	DESCRIPTION
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Use Interface	Select a WAN interface through which the traffic is sent. You must have the WAN interface(s) already configured in the **WAN** screens.
Use Gateway IP Address	Select this option and enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your ZyXEL Device's interface(s). The gateway helps forward packets to their destinations.
Back	Click **Back** to return to the previous screen without saving.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

12

Policy Forwarding

12.1 Overview

Traditionally, routing is based on the destination address only and the ZyXEL Device takes the shortest path to forward a packet. Policy forwarding allows the ZyXEL Device to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to outgoing packets, prior to the normal routing.

You can use source-based policy forwarding to direct traffic from different users through different connections or distribute traffic among multiple paths for load sharing.

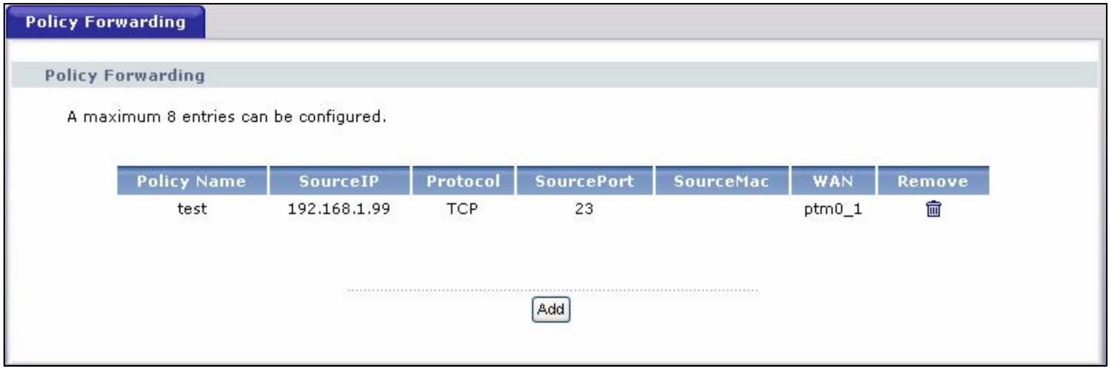
12.1.1 What You Can Do in this Chapter

The **Policy Forwarding** screens let you view and configure routing policies on the ZyXEL Device (Section 12.2 on page 171).

12.2 The Static Route Screen

Click **Advanced > Policy Forwarding** to open the **Policy Forwarding** screen.

Figure 89 Advanced > Policy Forwarding



Policy Forwarding

Policy Forwarding

A maximum 8 entries can be configured.

Policy Name	SourceIP	Protocol	SourcePort	SourceMac	WAN	Remove
test	192.168.1.99	TCP	23		ptm0_1	🗑

The following table describes the labels in this screen.

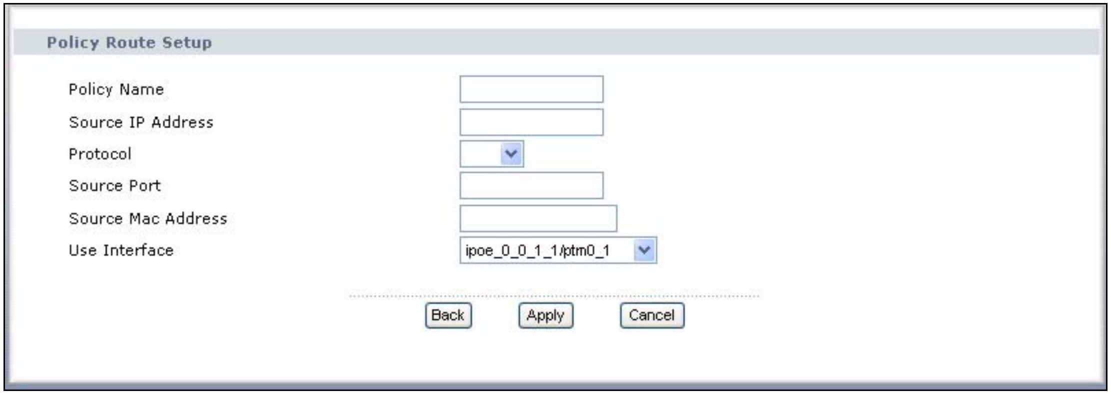
Table 57 Advanced > Policy Forwarding

LABEL	DESCRIPTION
Policy Name	This is the name of the rule.
SourceIP	This is the source IP address.
Protocol	This is the IP protocol.
SourcePort	This is the source port number.
SourceMAC	This is the source MAC address.
Interface	This is the WAN interface through which the traffic is routed.
Remove	Click the icon to remove a rule from the ZyXEL Device. A window displays asking you to confirm that you want to delete the rule.
Add	Click this to create a new rule.

12.2.1 Policy Forwarding Setup

Click the **Add** button in the **Policy Forwarding** screen. Use this screen to configure the required information for a policy route.

Figure 90 Policy Forwarding: Add



Policy Route Setup

Policy Name

Source IP Address

Protocol

Source Port

Source Mac Address

Use Interface: ipoe_0_0_1_1/ptm0_1

The following table describes the labels in this screen.

Table 58 Policy Forwarding: Add

LABEL	DESCRIPTION
Policy Name	Enter a descriptive name of up to 16 printable English keyboard characters, including spaces.
Source IP Address	Enter the source IP address.
Protocol	Select the IP protocol (**TCP** or **UDP**).
Source Port	Enter the source port number.
Use Interface	Select a WAN interface through which the traffic is sent. You must have the WAN interface(s) already configured in the **WAN** screens.
Back	Click **Back** to return to the previous screen without saving.

Table 58 Policy Forwarding: Add

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

13

RIP

13.1 Overview

Routing Information Protocol (RIP, RFC 1058 and RFC 1389) allows a device to exchange routing information with other routers.

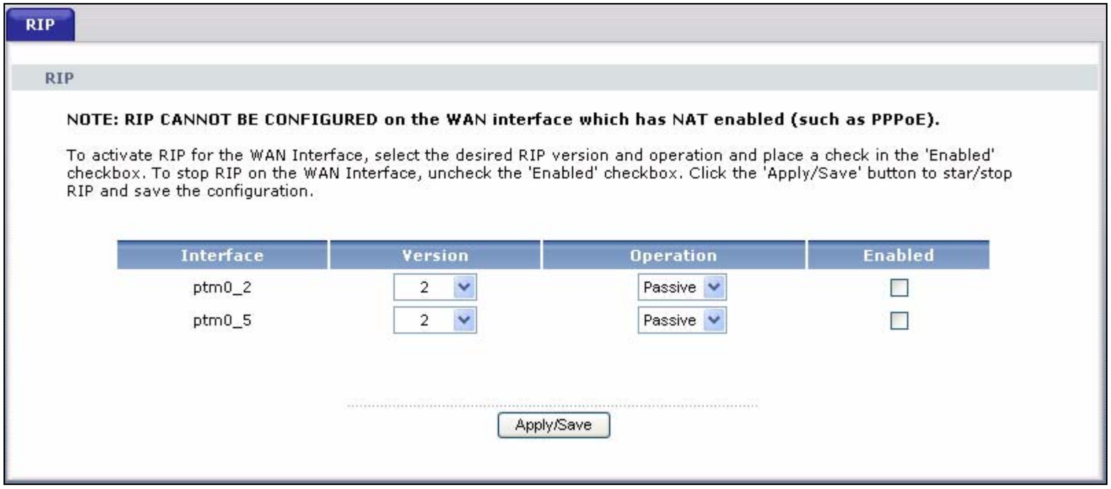
13.1.1 What You Can Do in this Chapter

The **RIP** screen lets you set up RIP settings on the ZyXEL Device (Section 13.2 on page 175).

13.2 The RIP Screen

Click **Advanced > RIP** to open the **RIP** screen.

Figure 91 Advanced > RIP



RIP

NOTE: RIP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled (such as PPPoE).

To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to star/stop RIP and save the configuration.

Interface	Version	Operation	Enabled
ptm0_2	2	Passive	□
ptm0_5	2	Passive	□

The following table describes the labels in this screen.

Table 59 Advanced > RIP

LABEL	DESCRIPTION
Interface	This is the name of the interface in which the RIP setting is used.
Version	The RIP version controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). RIP version **1** is universally supported but RIP version **2** carries more information. RIP version **1** is probably adequate for most networks, unless you have an unusual network topology.
Operation	Select **Passive** to have the ZyXEL Device update the routing table based on the RIP packets received from neighbors but not advertise its route information to other routers in this interface. Select **Active** to have the ZyXEL Device advertise its route information and also listen for routing updates from neighboring routers.
Enabled	Select the check box to activate the settings.
Apply/Save	Click **Apply/Save** to save your changes back to the ZyXEL Device.

14

Quality of Service (QoS)

14.1 Overview

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

Configure QoS on the ZyXEL Device to group and prioritize application traffic and fine-tune network performance. Setting up QoS involves these steps:

1. Configure classifiers to sort traffic into different flows.

2. Assign priority and define actions to be performed for a classified traffic flow.

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

This chapter contains information about configuring QoS and editing classifiers.

14.1.1 What You Can Do in this Chapter

- The **General** screen lets you lets you enable or disable QoS and set the default DSCP value for incoming traffic does not match a class (Section 14.3 on page 178).
- The **Queue Setup** screen lets you lets you configure QoS queue assignment (Section 14.4 on page 180).
- The **Class Setup** screen lets you add, edit or delete QoS classifiers (Section 14.5 on page 182).

- The **Monitor** screen lets you view the ZyXEL Device's QoS-related packet statistics (Section 14.6 on page 188).

14.2 What You Need to Know

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

QoS versus Cos

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

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

Tagging and Marking

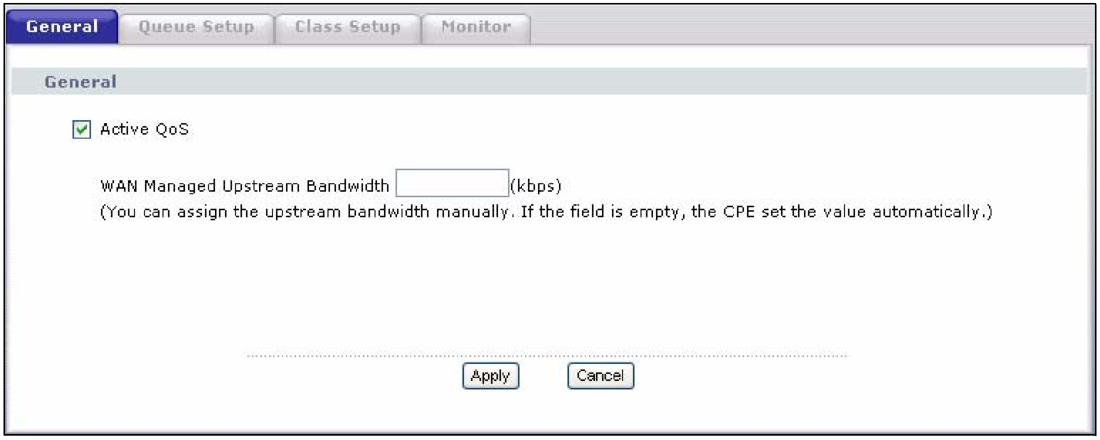
In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or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

14.3 The Quality of Service General Screen

Click **Advanced Setup** > **Quality of Service** to open the screen as shown next.

Use this screen to enable or disable QoS and set the default DSCP value for incoming traffic does not match a class. See Section 14.1 on page 177 for more information.

Figure 92 QoS General



☑ Active QoS

WAN Managed Upstream Bandwidth (kbps)

(You can assign the upstream bandwidth manually. If the field is empty, the CPE set the value automatically.)

The following table describes the labels in this screen.

Table 60 QoS General

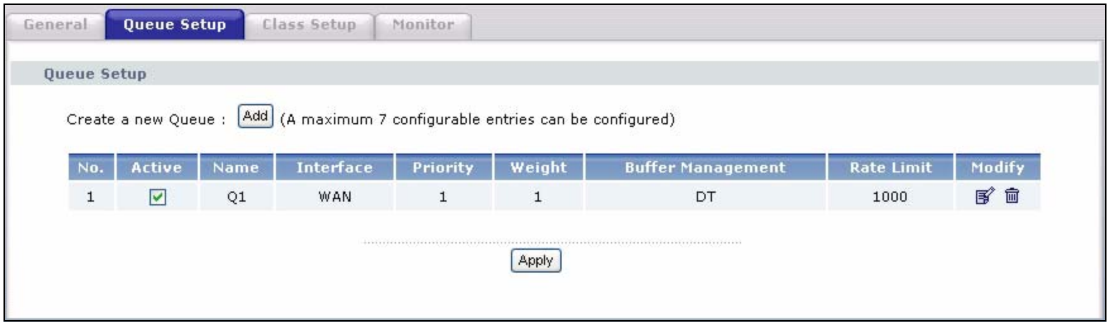
LABEL	DESCRIPTION
Active QoS	Select the check box to turn on QoS to improve your network performance.
WAN Managed Upstream Bandwidth	Enter the amount of upstream bandwidth for the WAN interface that you want to allocate using QoS. The recommendation is to set this speed to match the interface's actual transmission speed. For example, set the WAN interface speed to 100000 kbps if your Internet connection has an upstream transmission speed of 100 Mbps. You can set this number higher than the interface's actual transmission speed. The ZyXEL Device uses up to 95% of the DSL port's actual upstream transmission speed even if you set this number higher than the DSL port's actual transmission speed. You can also set this number lower than the interface's actual transmission speed. This will cause the ZyXEL Device to not use some of the interface's available bandwidth. If you leave this field blank, the ZyXEL Device automatically sets this number to be 95% of the DSL port's actual upstream transmission speed.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

14.4 The Queue Setup Screen

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

Use this screen to configure QoS queue assignment.

Figure 93 QoS Queue Setup



Create a new Queue : Add (A maximum 7 configurable entries can be configured)

No.	Active	Name	Interface	Priority	Weight	Buffer Management	Rate Limit	Modify
1	☑	Q1	WAN	1	1	DT	1000	✎ 🗑

The following table describes the labels in this screen.

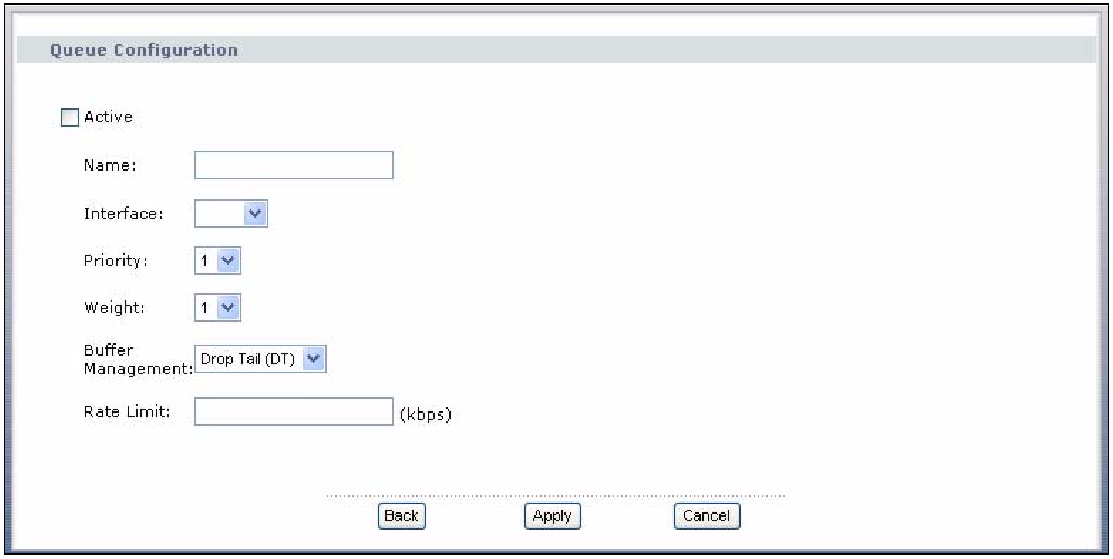
Table 61 QoS Queue Setup

LABEL	DESCRIPTION
Add	Click this button to create a new entry.
No.	This is the index number of this entry.
Active	Select the check box to enable the queue.
Name	This shows the descriptive name of this queue.
Interface	This shows the name of the ZyXEL Device's interface through which traffic in this queue passes.
Priority	This shows the priority of this queue.
Weight	This shows the weight of this queue.
Buffer Management	This shows the queue management algorithm used by the ZyXEL Device.
Rate Limit	This shows the maximum transmission rate allowed for traffic on this queue.
Modify	Click the **Edit** icon to go to the screen where you can edit the queue. Click the **Remove** icon to delete an existing queue. Note that subsequent rules move up by one when you take this action.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.

14.4.1 Adding a QoS Queue

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

Figure 94 QoS Queue Setup: Add



Queue Configuration

□ Active

Name:

Interface:

Priority: 1

Weight: 1

Buffer Management: Drop Tail (DT)

Rate Limit: (kbps)

The following table describes the labels in this screen.

Table 62 QoS Queue Setup: Add

LABEL	DESCRIPTION
Active	Select to enable or disable this queue.
Name	Enter the descriptive name of this queue.
Interface	Select the interface to which this queue is applied.
Priority	Select the priority level (from 1 to 3) of this queue. The smaller the number, the higher the priority level. Traffic assigned to higher priority queues gets through faster while traffic in lower priority queues is dropped if the network is congested.
Weight	Select the weight (from 1 to 8) of this queue. If two queues have the same priority level, the ZyXEL Device divides the bandwidth across the queues according to their weights. Queues with larger weights get more bandwidth than queues with smaller weights.
Buffer Management	This field displays **Drop Tail (DT)** and the ZyXEL Device drops the newly arriving packet when the queue is full.
Rate Limit	Specify the maximum transmission rate (in Kbps) allowed for traffic on this queue.
Back	Click **Back** to return to the previous screen without saving.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

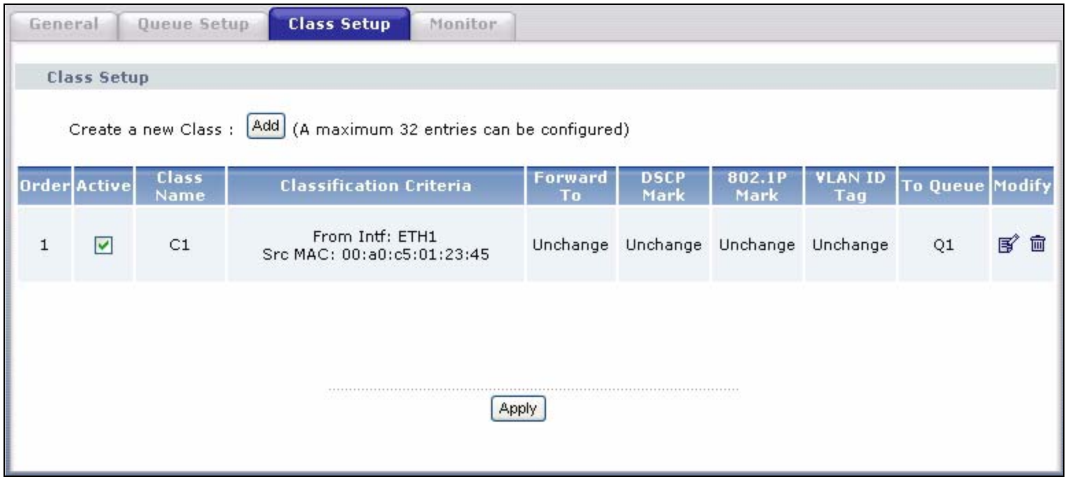
14.5 The Class Setup Screen

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

You can give different priorities to traffic that the ZyXEL Device forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.

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

Figure 95 QoS Class Setup



Create a new Class : Add (A maximum 32 entries can be configured)

Order	Active	Class Name	Classification Criteria	Forward To	DSCP Mark	802.1P Mark	VLAN ID Tag	To Queue	Modify
1	☑	C1	From Intf: ETH1 Src MAC: 00:a0:c5:01:23:45	Unchange	Unchange	Unchange	Unchange	Q1	

The following table describes the labels in this screen.

Table 63 QoS Class Setup

LABEL	DESCRIPTION
Add	Click this button to create a new classifier.
Order	This field displays the index number of the classifier.
Active	Select the check box to enable the classifier.
Class Name	This is the name of the classifier.
Classification Criteria	This shows criteria specified in this classifier, for example the interface from which traffic of this class should come and the source MAC address of traffic that matches this classifier.
Forward To	This is the interface through which traffic that matches this classifier is forwarded out.
DSCP Mark	This is the DSCP number added to traffic of this classifier.
802.1P Mark	This is the IEEE 802.1p priority level assigned to traffic of this classifier.

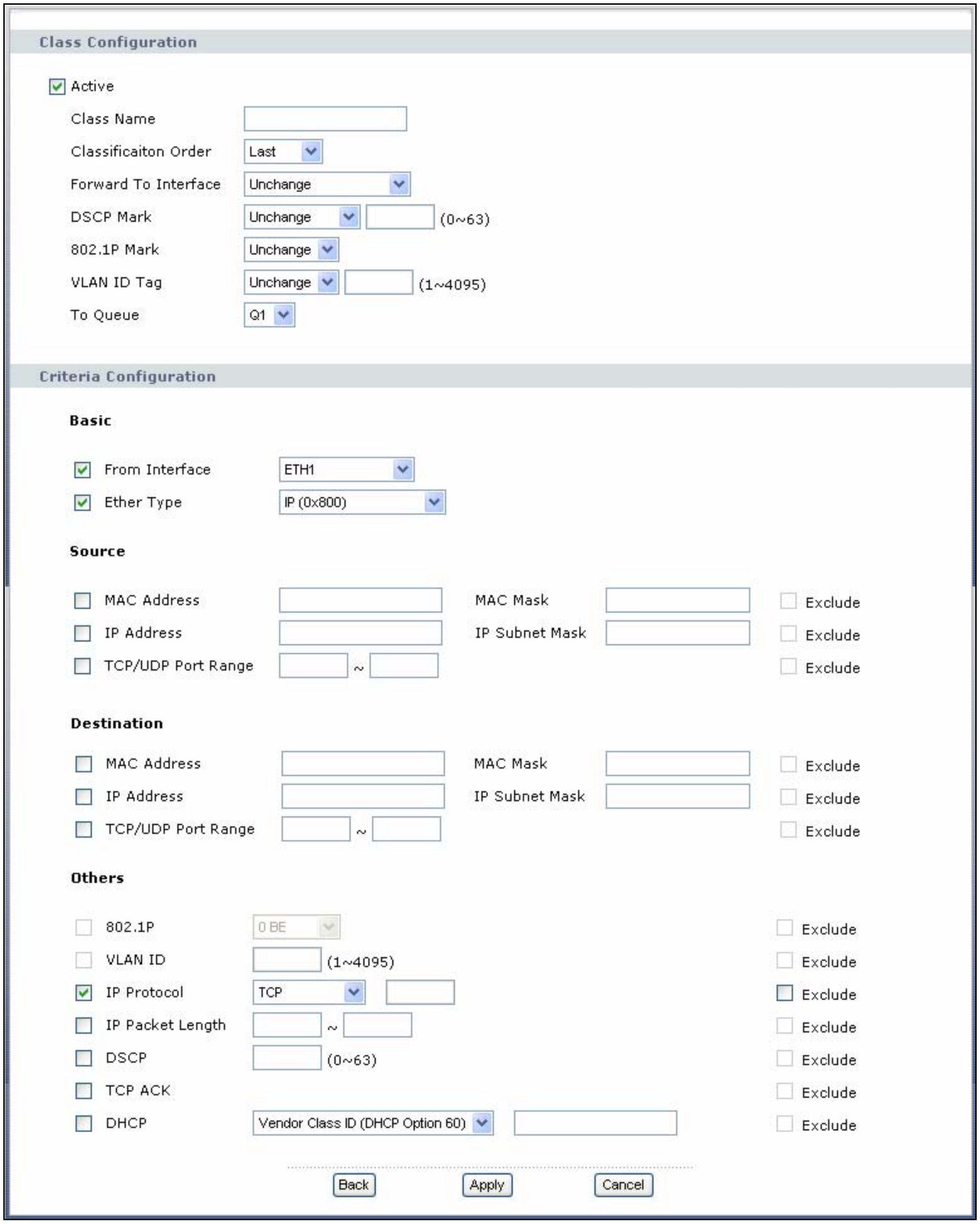
Table 63 QoS Class Setup (continued)

LABEL	DESCRIPTION
VLAN ID Tag	This is the VLAN ID number assigned to traffic of this classifier.
To Queue	This is the name of the queue in which traffic of this classifier is put.
Modify	Click the **Edit** icon to go to the screen where you can edit the classifier. Click the **Remove** icon to delete an existing classifier. Note that subsequent rules move up by one when you take this action.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.

14.5.1 QoS Class Edit

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

Figure 96 QoS Class Setup: Add



Class Configuration

☑ Active

Class Name

Classificaiton Order: Last

Forward To Interface: Unchange

DSCP Mark: Unchange (0~63)

802.1P Mark: Unchange

VLAN ID Tag: Unchange (1~4095)

To Queue: Q1

Criteria Configuration

Basic

☑ From Interface: ETH1

☑ Ether Type: IP (0x800)

Source

☐ MAC Address | MAC Mask | ☐ Exclude

☐ IP Address | IP Subnet Mask | ☐ Exclude

☐ TCP/UDP Port Range ~ | ☐ Exclude

Destination

☐ MAC Address | MAC Mask | ☐ Exclude

☐ IP Address | IP Subnet Mask | ☐ Exclude

☐ TCP/UDP Port Range ~ | ☐ Exclude

Others

☐ 802.1P: 0 BE | ☐ Exclude

☐ VLAN ID (1~4095) | ☐ Exclude

☑ IP Protocol: TCP | ☐ Exclude

☐ IP Packet Length ~ | ☐ Exclude

☐ DSCP (0~63) | ☐ Exclude

☐ TCP ACK | ☐ Exclude

☐ DHCP: Vendor Class ID (DHCP Option 60) | ☐ Exclude

The following table describes the labels in this screen.

Table 64 QoS Class Configuration

LABEL	DESCRIPTION
Class Configuration	
Active	Select to enable or disable this classifier.
Class Name	Enter a descriptive name of up to 20 printable English keyboard characters, including spaces.
Classification Order	Select an existing number for where you want to put this classifier to move the classifier to the number you selected after clicking **Apply**. Select **Last** to put this rule in the back of the classifier list.
Forward to Interface	Select a WAN interface through which traffic of this class will be forwarded out. If you select **Unchange**, the ZyXEL Device forward traffic of this class according to the default routing table.
DSCP Mark	This field is available only when you select the **Ether Type** check box. If you select **Mark**, enter a DSCP value with which the ZyXEL Device replaces the DSCP field in the packets. If you select **Auto Mapping** and there is a VLAN tag carried in the matched packets, the ZyXEL Device will replace the IP ToS field with the 802.1p priority field. If you select **Unchange**, the ZyXEL Device keep the DSCP field in the packets.
802.1p Mark	Select a priority level with which the ZyXEL Device replaces the IEEE 802.1p priority field in the packets. If you select **Unchange**, the ZyXEL Device keep the 802.1p priority field in the packets.
VLAN ID Tag	If you select **Remark**, enter a VLAN ID number (between 1 and 4095) with which the ZyXEL Device replaces the VLAN ID of the frames. If you select **Remove**, the ZyXEL Device deletes the VLAN ID of the frames before forwarding them out. If you select **Add**, the ZyXEL Device treat all matched traffic untagged and add a second VLAN ID. If you select **Unchange**, the ZyXEL Device keep the VLAN ID in the packets.
To Queue	Select a queue that applies to this class. You should have configured a queue in the **Queue Setup** screen already.
Criteria Configuration Use the following fields to configure the criteria for traffic classification.	
Basic	
From Interface	Select from which Ethernet port or wireless interface traffic of this class should come.

Table 64 QoS Class Configuration (continued)

LABEL	DESCRIPTION
Ether Type	Select a predefined application to configure a class for the matched traffic. If you select **IP**, you also need to configure source or destination MAC address, IP address, DHCP options, DSCP value or the protocol type. If you select **8021Q**, you can configure an 802.1p priority level and VLAN ID in the **Others** section.
Source	
MAC Address	Select the check box and enter the source MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
IP Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
IP Subnet Mask	Enter the source subnet mask.
TCP/UDP Port Range	If you select **TCP** or **UDP** in the **IP Protocol** field, select the check box and enter the port number(s) of the source.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Destination	
MAC Address	Select the check box and enter the destination MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
IP Address	Select the check box and enter the destination IP address in dotted decimal notation. A blank source IP address means any source IP address.
IP Subnet Mask	Enter the destination subnet mask.
TCP/UDP Port Range	If you select **TCP** or **UDP** in the **IP Protocol** field, select the check box and enter the port number(s) of the source.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Others	

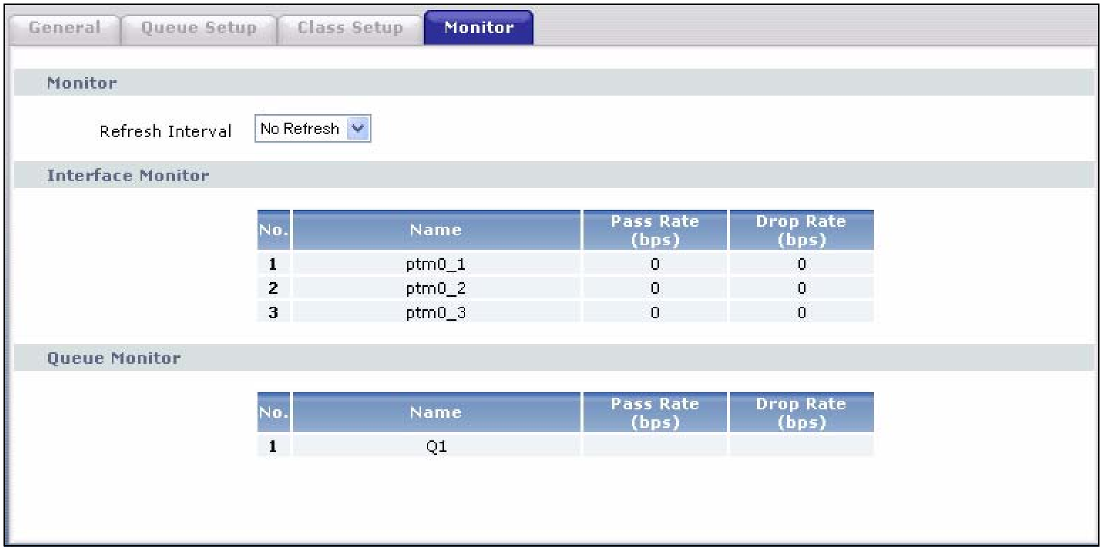
Table 64 QoS Class Configuration (continued)

LABEL	DESCRIPTION
802.1P	This field is available only when you select **802.1Q** in the **Ether Type** field. Select this option and select a priority level (between 0 and 7) from the drop down list box. "0" is the lowest priority level and "7" is the highest.
VLAN ID	This field is available only when you select **802.1Q** in the **Ether Type** field. Select this option and specify a VLAN ID number between 1 and 4095.
IP Protocol	This field is available only when you select **IP** in the **Ether Type** field. Select this option and select the protocol (service type) from **TCP**, **UDP**, **ICMP** or **IGMP**. If you select **User defined**, enter the protocol (service type) number.
IP Packet Length	This field is available only when you select **IP** in the **Ether Type** field. Select this option and enter the minimum and maximum packet length (from 28 to 1500) in the fields provided.
DSCP	This field is available only when you select **IP** in the **Ether Type** field. Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
TCP ACK	This field is available only when you select **IP** in the **Ether Type** field. If you select this option, the matched TCP packets must contain the ACK (Acknowledge) flag.
DHCP	This field is available only when you select **IP** in the **Ether Type** field. Select this option and select a DHCP option. If you select **Vendor Class ID (DHCP Option 60)**, enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware. If you select **User Class ID (DHCP Option 77)**, enter a string that identifies the user's category or application type in the matched DHCP packets.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Back	Click **Back** to return to the previous screen without saving.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

14.6 The QoS Monitor Screen

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

Figure 97 QoS > Monitor



Monitor

Refresh Interval: No Refresh

Interface Monitor

No.	Name	Pass Rate (bps)	Drop Rate (bps)
1	ptm0_1	0	0
2	ptm0_2	0	0
3	ptm0_3	0	0

Queue Monitor

No.	Name	Pass Rate (bps)	Drop Rate (bps)
1	Q1		

The following table describes the labels in this screen.

Table 65 QoS > Monitor

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

14.7 Technical Reference

The following section contains additional technical information about the ZyXEL Device features described in this chapter.

IEEE 802.1Q Tag

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

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

Table 66 IEEE 802.1p Priority Level and Traffic Type

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

DiffServ

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

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

DSCP and Per-Hop Behavior

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

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

DSCP (6 bits)	Unused (2 bits)

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

15

Dynamic DNS Setup

15.1 Overview

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

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

15.1.1 What You Can Do in this Chapter

Use the **Dynamic DNS** screen (Section 15.3 on page 192) to enable DDNS and configure the DDNS settings on the ZyXEL Device.

15.2 What You Need To Know

DYNDNS Wildcard

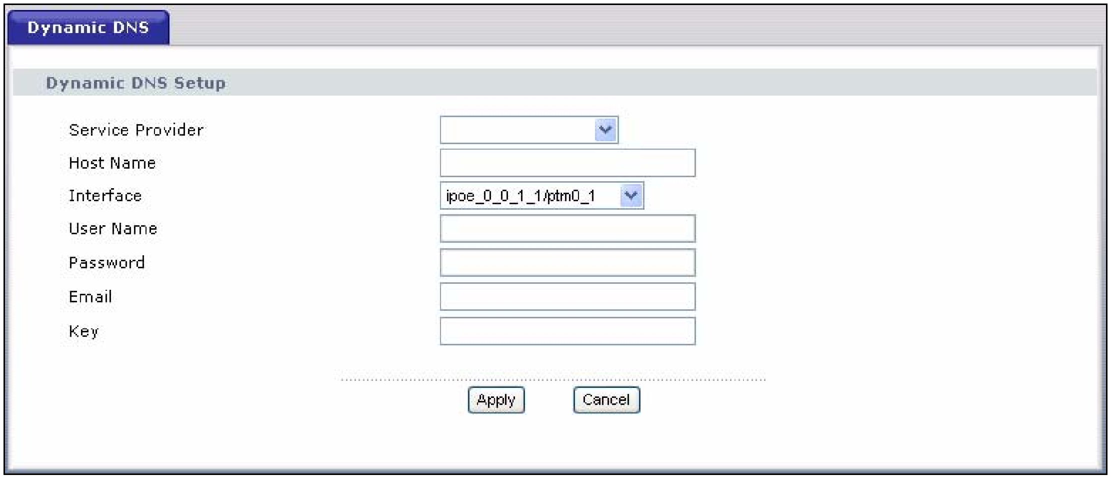
Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

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

15.3 The Dynamic DNS Screen

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

Figure 98 Advanced > Dynamic DNS



The following table describes the fields in this screen.

Table 67 Advanced > Dynamic DNS

LABEL	DESCRIPTION
Service Provider	Select the name of your Dynamic DNS service provider.
Host Name	Type the domain name assigned to your ZyXEL Device by your Dynamic DNS provider. You can specify up to two host names in the field separated by a comma (",").
Interface	Select the WAN interface to use for updating the IP address of the domain name.
User Name	Type your user name.
Password	Type the password assigned to you.
Email	If you select **TZO** in the **Service Provider** field, enter the user name you used to register for this service.
Key	If you select **TZO** in the **Service Provider** field, enter the password you used to register for this service.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

16

Remote Management

16.1 Overview

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

16.1.1 What You Can Do in this Chapter

- The **TR-069** screen lets you configure the ZyXEL Device's TR-069 auto-configuration settings (Section 16.3 on page 195).
- The **TR-064** screen lets you enable management via TR-064 on the ZyXEL Device (Section 16.3 on page 195)
- The **Service Control** screens let you configure through which interface(s) users can use which service(s) to manage the ZyXEL Device (Section 16.4 on page 196).
- The **IP Address** screens let you configure from which IP address(es) users can use a service to manage the ZyXEL Device (Section 16.5 on page 197).

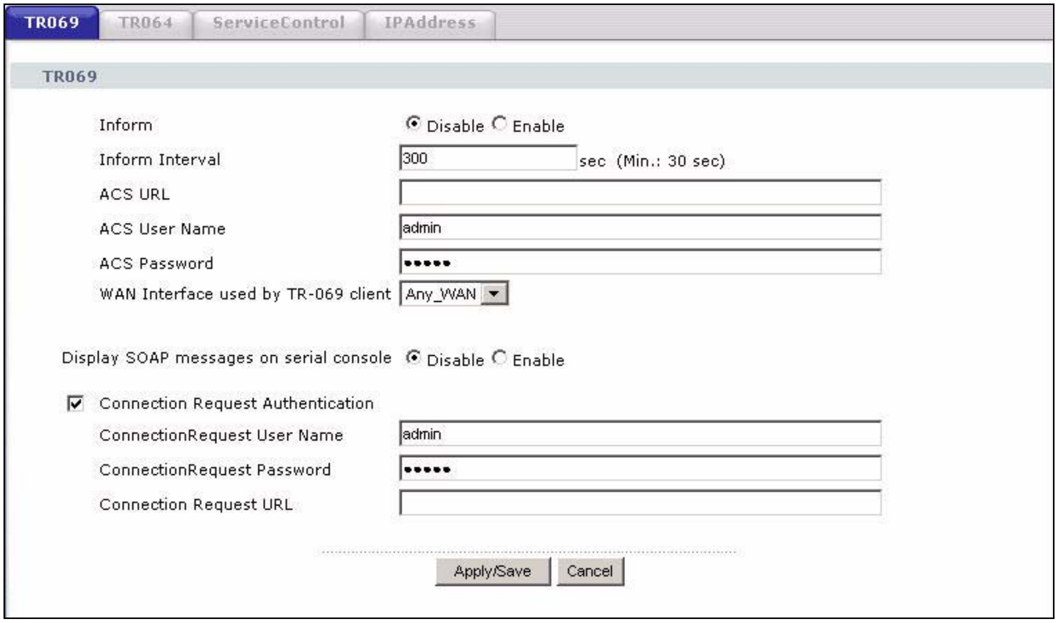
16.2 The TR-069 Screen

TR-069 defines how Customer Premise Equipment (CPE), for example your ZyXEL Device, can be managed over the WAN by an Auto Configuration Server (ACS). TR-069 is based on sending Remote Procedure Calls (RPCs) between an ACS and a client device. RPCs are sent in Extensible Markup Language (XML) format over HTTP or HTTPS.

An administrator can use an ACS to remotely set up the ZyXEL Device, modify settings, perform firmware upgrades as well as monitor and diagnose the ZyXEL Device. You have enable the device to be managed by the ACS and specify the ACS IP address or domain name and username and password.

Click **Advanced > Remote MGMT** to open the following screen. Use this screen to configure your P-870HN to be managed by an ACS.

Figure 99 TR-069



TR069

Inform ● Disable ○ Enable

Inform Interval 300 sec (Min.: 30 sec)

ACS URL

ACS User Name admin

ACS Password •••••

WAN Interface used by TR-069 client Any_WAN

Display SOAP messages on serial console ● Disable ○ Enable

☑ Connection Request Authentication

ConnectionRequest User Name admin

ConnectionRequest Password •••••

Connection Request URL

The following table describes the fields in this screen.

Table 68 TR-069

LABEL	DESCRIPTION
Inform	Select **Enable** to activate remote management via TR-069 on the WAN. Otherwise, select **Disable**.
Inform Interval	Enter the time interval (in seconds) at which the ZyXEL Device sends information to the auto-configuration server.
ACS URL	Enter the URL or IP address of the auto-configuration server.
ACS User Name	Enter the TR-069 user name for authentication with the auto-configuration server.
ACS Password	Enter the TR-069 password for authentication with the auto-configuration server.
WAN Interface used by TR-069 client	Select a WAN interface through which the TR-069 traffic passes.
Display SOAP messages on serial console	Select **Enable** to show the SOAP messages on the console.
Connection Request Authentication	Select this option to enable authentication when there is a connection request from the ACS.
Connection Request User Name	Enter the connection request user name. When the ACS makes a connection request to the ZyXEL Device, this user name is used to authenticate the ACS.

Table 68 TR-069 (continued)

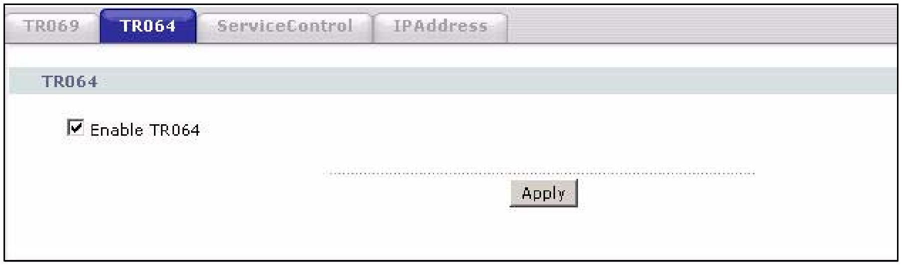
LABEL	DESCRIPTION
Connection Request Password	Enter the connection request password. When the ACS makes a connection request to the ZyXEL Device, this password is used to authenticate the ACS.
Connection Request URL	This shows the connection request URL. The ACS can use this URL to make a connection request to the ZyXEL Device.
Apply/Save	Click this button to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

16.3 The TR-064 Screen

TR-064 is a LAN-Side DSL CPE Configuration protocol defined by the DSL Forum. TR-064 is built on top of UPnP. It allows the users to use a TR-064 compliant CPE management application on the their computers from the LAN to discover the CPE and configure user-specific parameters, such as the username and password.

Click **Advanced > Remote MGMT** > **TR064** to open the following screen.

Figure 100 TR-064



☑ Enable TR064

The following table describes the fields in this screen.

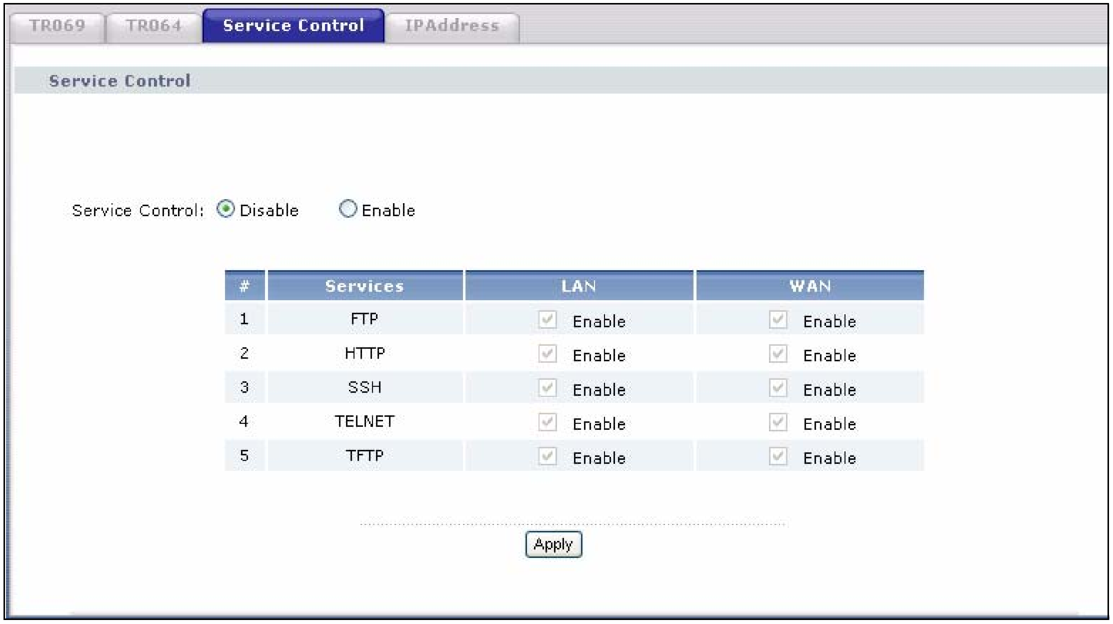
Table 69 TR-064

LABEL	DESCRIPTION
Enanble TR064	Select the check box to activate management via TR-064 on the LAN.
Apply	Click this button to save your changes back to the ZyXEL Device.

16.4 The Service Control Screen

Click **Advanced > Remote MGMT > Service Control** to open the following screen. Use this screen to decide what services you may use to access which ZyXEL Device interface.

Figure 101 Service Control



Service Control: ● Disable ○ Enable

#	Services	LAN	WAN
1	FTP	☑ Enable	☑ Enable
2	HTTP	☑ Enable	☑ Enable
3	SSH	☑ Enable	☑ Enable
4	TELNET	☑ Enable	☑ Enable
5	TFTP	☑ Enable	☑ Enable

The following table describes the fields in this screen.

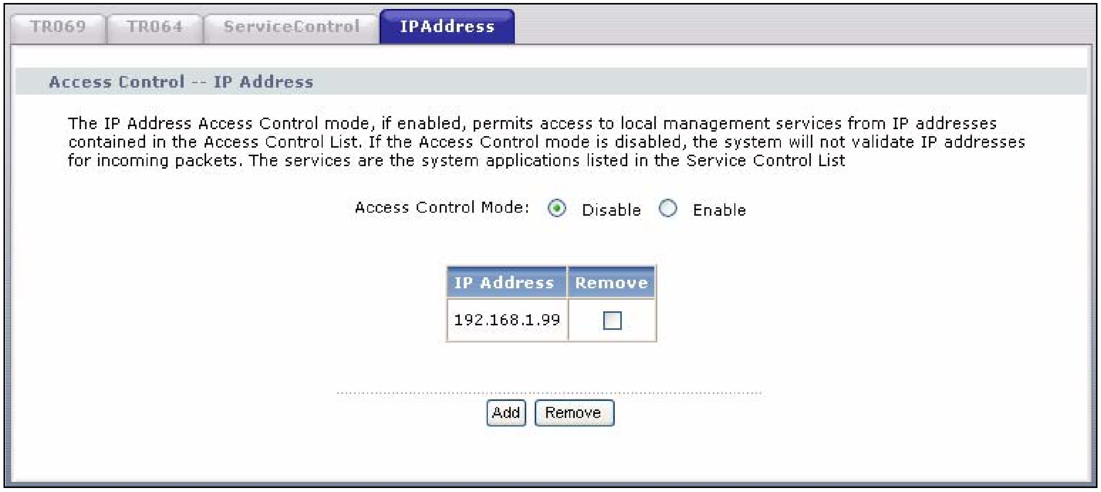
Table 70 Access Control: Services

LABEL	DESCRIPTION
Service Control	Select **Enable** to turn on service control. Otherwise, select **Disable**.
#	This is the index number of the entry.
Services	This is the service you may use to access the ZyXEL Device.
LAN	Select the **Enable** check box for the corresponding services that you want to allow access to the ZyXEL Device from the LAN.
WAN	Select the **Enable** check box for the corresponding services that you want to allow access to the ZyXEL Device from the WAN.
Apply	Click this button to save your changes back to the ZyXEL Device.

16.5 The IP Address Screen

Click **Advanced > Remote MGMT > IP Address** to open the following screen. Use this screen to specify the “trusted” computers from which an administrator may use a service to manage the ZyXEL Device.

Figure 102 IP Address



Access Control -- IP Address

The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List

Access Control Mode: ● Disable ○ Enable

IP Address	Remove
192.168.1.99	□

The following table describes the fields in this screen.

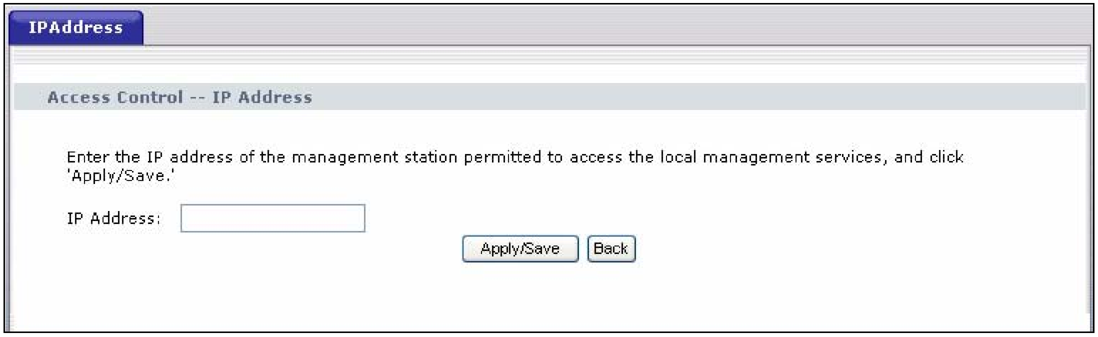
Table 71 IP Address

LABEL	DESCRIPTION
Access Control Mode	Select **Enable** to activate the secured client list. Select **Disable** to disable the list without deleting it.
IP Address	This is the IP address of the trusted computer from which you can manage the ZyXEL Device.
Remove	Select this check box and click the **Remove** button to delete this entry from the ZyXEL Device.
Add	Click this button to create a new entry.
Remove	Click this button to delete the selected entry.

16.5.1 Adding an IP Address

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

Figure 103 IP Address: Add



Access Control -- IP Address

Enter the IP address of the management station permitted to access the local management services, and click 'Apply/Save.'

IP Address:

The following table describes the fields in this screen.

Table 72 IP Address: Add

LABEL	DESCRIPTION
IP Address	Enter the IP address of the trusted computer from which you can manage the ZyXEL Device.
Apply/Save	Click this button to save your changes back to the ZyXEL Device.
Back	Click this button to return to the previous screen without saving.

Universal Plug-and-Play (UPnP)

17.1 Overview

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

17.1.1 What You Can Do in this Chapter

The **UPnP** screen lets you enable UPnP on the ZyXEL Device (Section 17.3 on page 200).

17.2 What You Need to Know

How do I know if I'm using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

NAT Traversal

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

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

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

See the NAT chapter for more information on NAT.

Cautions with UPnP

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

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

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

UPnP and ZyXEL

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

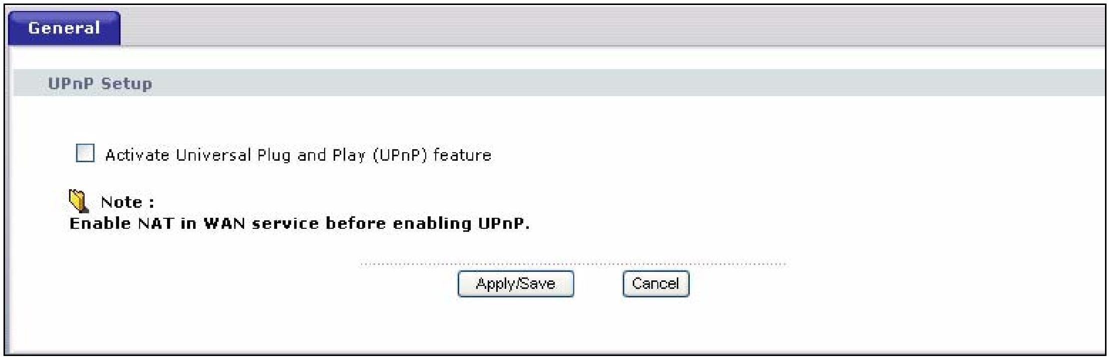
See the following sections for examples of installing and using UPnP.

17.3 The UPnP Screen

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

See Section 17.1 on page 199 for more information.

Figure 104 Advanced > UPnP



UPnP Setup

□ Activate Universal Plug and Play (UPnP) feature

Note :
Enable NAT in WAN service before enabling UPnP.