P870HNU-51B

IPv6 version

802.11n Wireless VDSL2 4-port Gateway

User's Guide

Default Login Details

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

Firmware Version 1.12
Edition 1, 5/2011

www.zyxel.com

ZyXEL

About This User's Guide

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Intended Audience

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

Related Documentation

- Support Disc

  Refer to the included CD for support documents.

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.

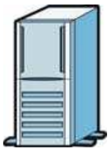
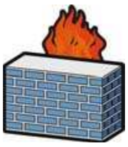
Syntax Conventions

- The P-870HNU-51b may be referred to as the “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 Device icon is not an exact representation of your device.

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

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

PART I

User’s Guide

1

Introducing the Device

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

1.1 Overview

The 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 IEEE 802.11n. The "N" models support IEEE 802.11n wireless connection mode.
- "U" denotes a USB port used to set up a 3G WAN connection via a 3G wireless card or share files via a USB memory stick or a USB hard drive. The Device can also function as a print server with an USB printer connected.

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

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

See Chapter 24 on page 255 for a full list of features.

1.2 Ways to Manage the Device

Use any of the following methods to manage the Device.

- Web Configurator. This is recommended for everyday management of the 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 Device

Do the following things regularly to make the Device more secure and to manage the 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 Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the Device. You could simply restore your last configuration.

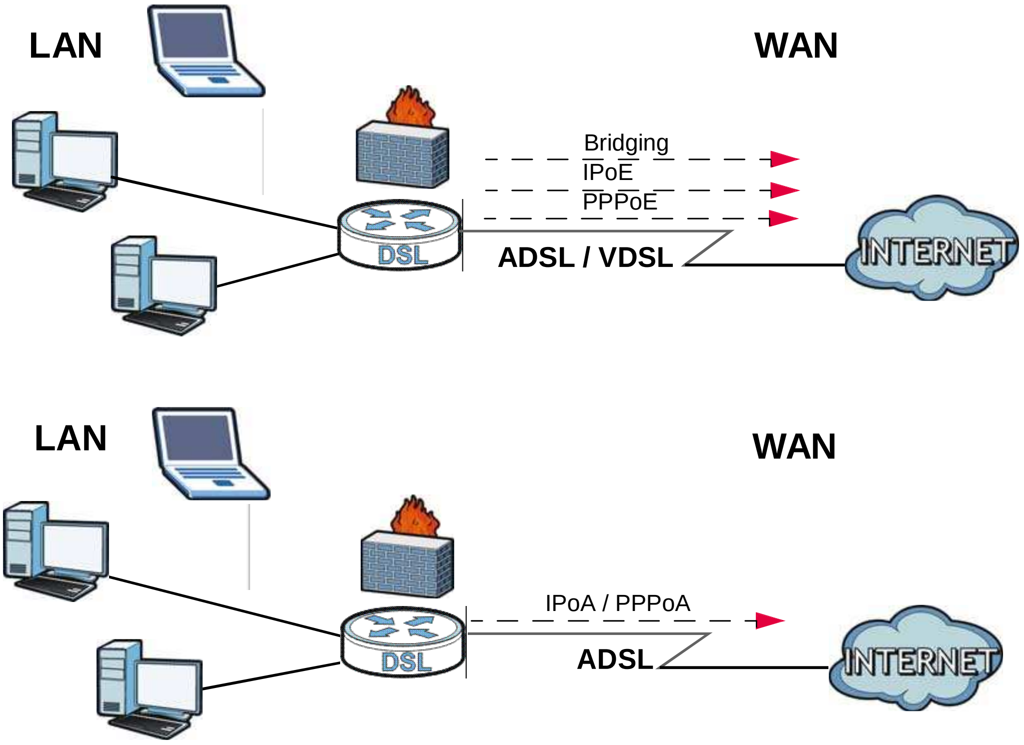
1.4 Applications for the Device

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

1.4.1 Internet Access

Your 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 Device’s LAN ports (or wirelessly). You can have multiple WAN services over one ADSL or VDSL line. The Device cannot work in ADSL and VDSL mode at the same time.

Figure 1 Device’s Internet Access Application



You can also configure IP filtering on the 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 The WLAN/WPS Button

You can use the WLAN/WPS button (((ı))) 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.

1.5.1 Turn the Wireless LAN Off or On

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

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

1.5.2 Activate WPS

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

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

Note: You must activate WPS in the Device and in another wireless device within two minutes of each other. See Section 7.8.4 on page 144 for more information.

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 the default.

1.6.1 Using the Reset Button

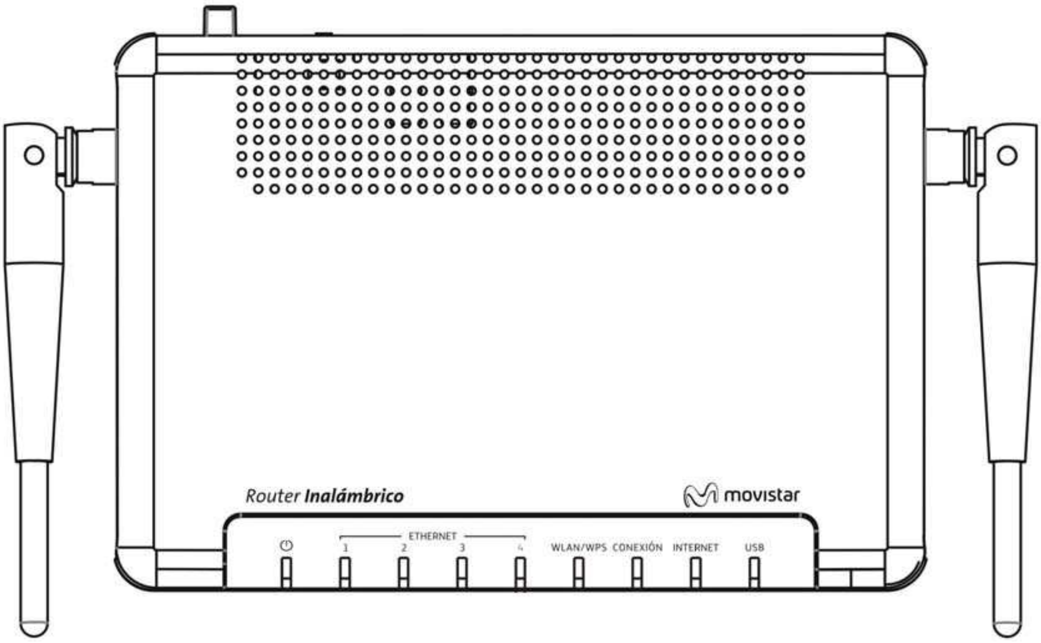
1 Make sure the **POWER** LED is on (not blinking).

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 LEDs (Lights)

The following graphic displays the labels of the LEDs.

Figure 2 The Top Panel of the Device:



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

Table 1 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The Device is receiving power and ready for use.
		Blinking	The Device is self-testing.
		Off	The Device is not receiving power.
ETHERNET1-4	Green	On	The Device has an Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The Device is sending/receiving data to /from the LAN.
		Off	The Device does not have an Ethernet connection with the LAN.
WLAN/WPS	Green	On	The wireless network is activated.
		Blinking	The Device is communicating with other wireless clients.
	Orange	Blinking	The Device is setting up a WPS connection.
		Off	WPS is disabled or the WLAN is not ready.
CONEXION	Green	On	The ADSL line is up.
		Blinking	The Device is initializing the ADSL line.
	Orange	On	The VDSL line is up.
		Blinking	The Device is initializing the VDSL line.
		Off	The DSL line is down.

Table 1 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
INTERNET	Green	On	The Device has received an IP address through a WAN interface and can connect to the Internet. Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used) and the DSL connection is up.
		Blinking	The Device is sending or receiving traffic through a WAN interface.
		Off	The Device has not received an IP address through a WAN interface and as such cannot connect to the Internet.
USB	Green	On	The Device has a 3G card installed and the 3G connection is up.
		Blinking (Fast)	The Device is sending and/or receiving data through the 3G connection.
		Blinking (Slow)	The Device is tring to bring the 3G connection up.
		Off	There is no 3G card installed or the 3G connection is down.

2

Tutorials

2.1 Overview

This chapter describes:

- How to Set up Your VDSL Connection for Internet Access on page 25.
- How to Set up a Secure Wireless Network on page 30
- How to Use File Sharing on the Device on page 38
- How to Share a USB Printer via Your Device on page 41
- How to Prioritize Traffic Using QoS Class and Queue on page 42
- How to Access the Device Using DDNS on page 46.
- How to Route Traffic to Another Network Using Static Route on page 48.
- How to Set Up NAT Port Forwarding on page 50.
- How to Use ATM QoS with Multiple PVCs on page 52.

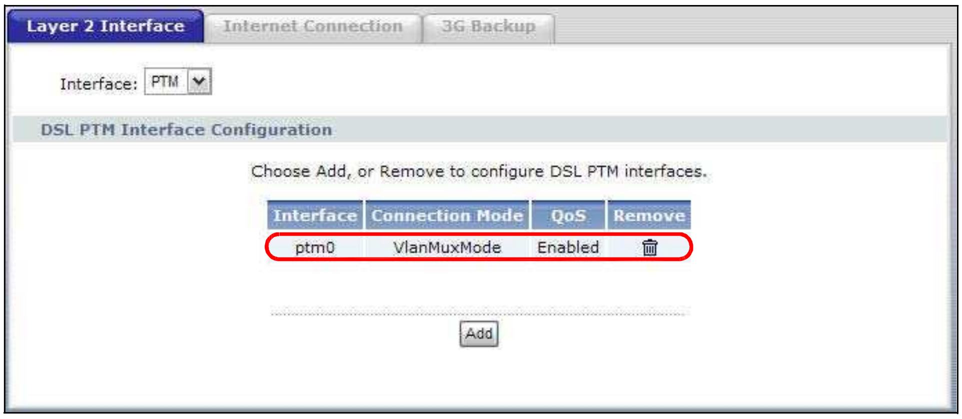
Note: The tutorials featured in this chapter require a basic understanding of connecting to and using the Web Configurator on your Device. For field descriptions of individual screens, see the related technical reference in this User's Guide.

2.2 How to Set up Your VDSL Connection for Internet Access

To access the Internet, you need to configure a layer-2 interface to allow users to use the DSL port on the Device. Then set up a WAN service (connection) for the interface.

This example shows you how to set up a VDSL connection using PPPoE. You need to create a WAN interface in the **Network > WAN > Layer 2 Interface** screen, then enter Internet access settings for the WAN interface in the **Network > WAN > Internet Connection** screen.

1 Go to **Network > WAN > Layer 2 Interface**. By default, you can only have one PTM interface on the Device and there is one PTM interface configured already.



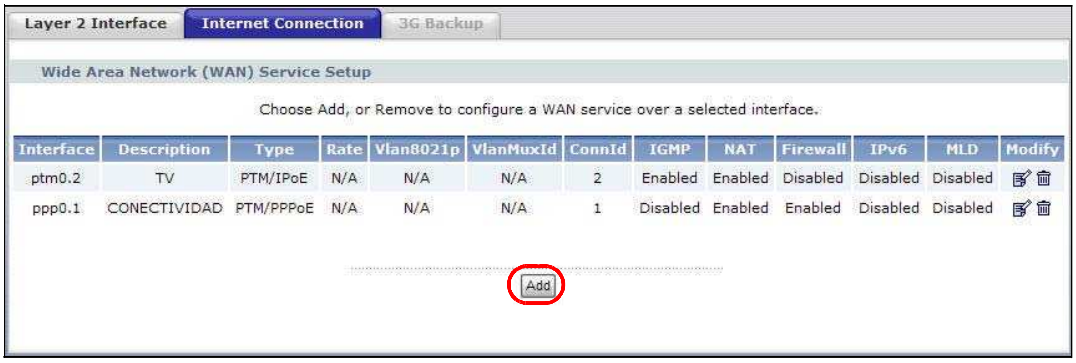
Interface: PTM

DSL PTM Interface Configuration

Choose Add, or Remove to configure DSL PTM interfaces.

Interface	Connection Mode	QoS	Remove
ptm0	VlanMuxMode	Enabled	🗑

2 Go to **Network > WAN > Internet Connection**, click **Add** to create a new WAN service using PPPoE through the existing PTM interface.

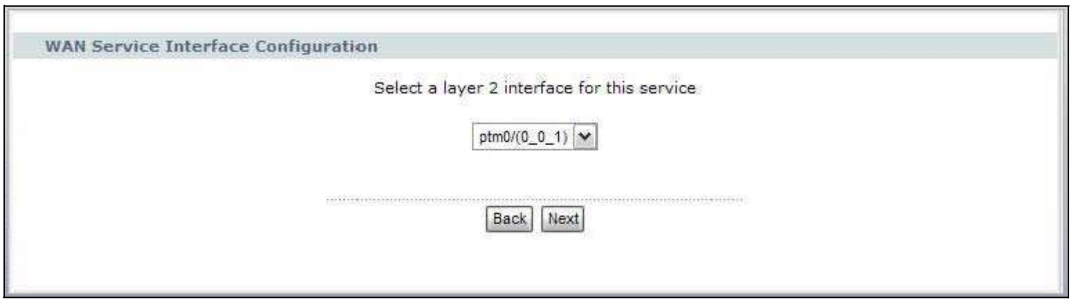


Wide Area Network (WAN) Service Setup

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

Interface	Description	Type	Rate	Vlan8021p	VlanMuxId	ConnId	IGMP	NAT	Firewall	IPv6	MLD	Modify
ptm0.2	TV	PTM/IPoE	N/A	N/A	N/A	2	Enabled	Enabled	Disabled	Disabled	Disabled	✎ 🗑
ppp0.1	CONECTIVIDAD	PTM/PPPoE	N/A	N/A	N/A	1	Disabled	Enabled	Enabled	Disabled	Disabled	✎ 🗑

3 Select the PTM layer-2 interface (**ptm0/(0_1_1)** in this example). Click **Next**.

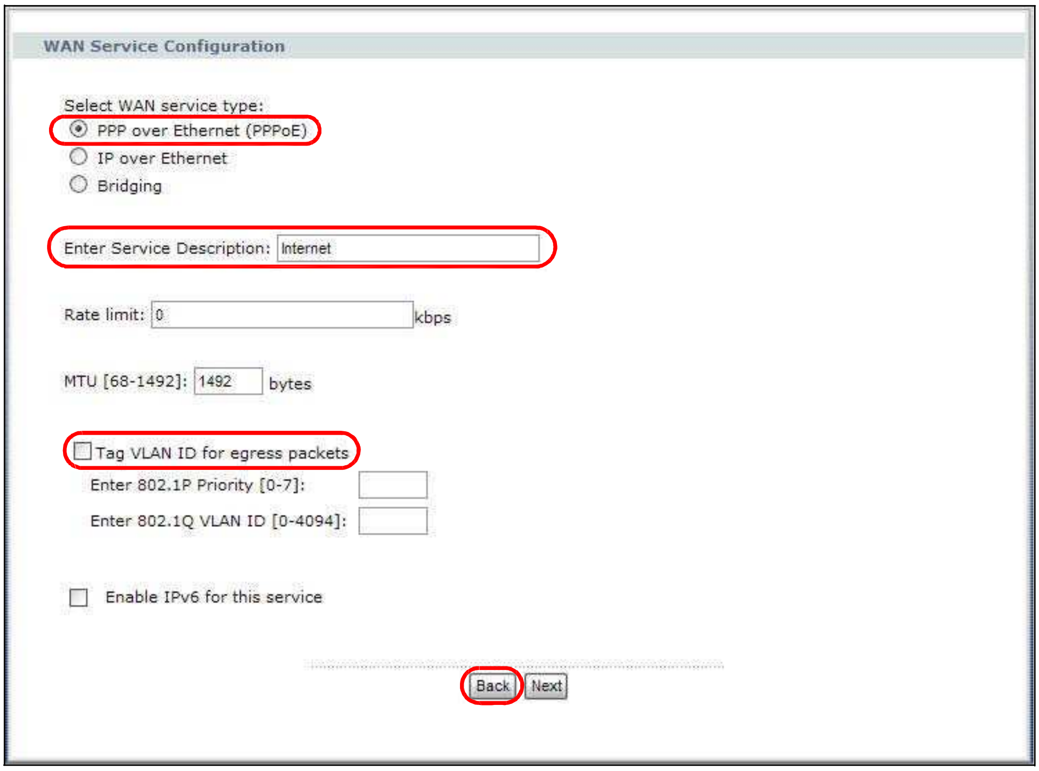


WAN Service Interface Configuration

Select a layer 2 interface for this service

ptm0/(0_0_1)

4 Select **PPP over Ethernet**, enter a descriptive name for this connection (**Internet** for example), clear the checkbox to not add a priority level and VLAN ID to traffic through this connection, and click **Next**.



WAN Service Configuration

Select WAN service type:

● PPP over Ethernet (PPPoE)

○ IP over Ethernet

○ Bridging

Enter Service Description: Internet

Rate limit: 0 kbps

MTU [68-1492]: 1492 bytes

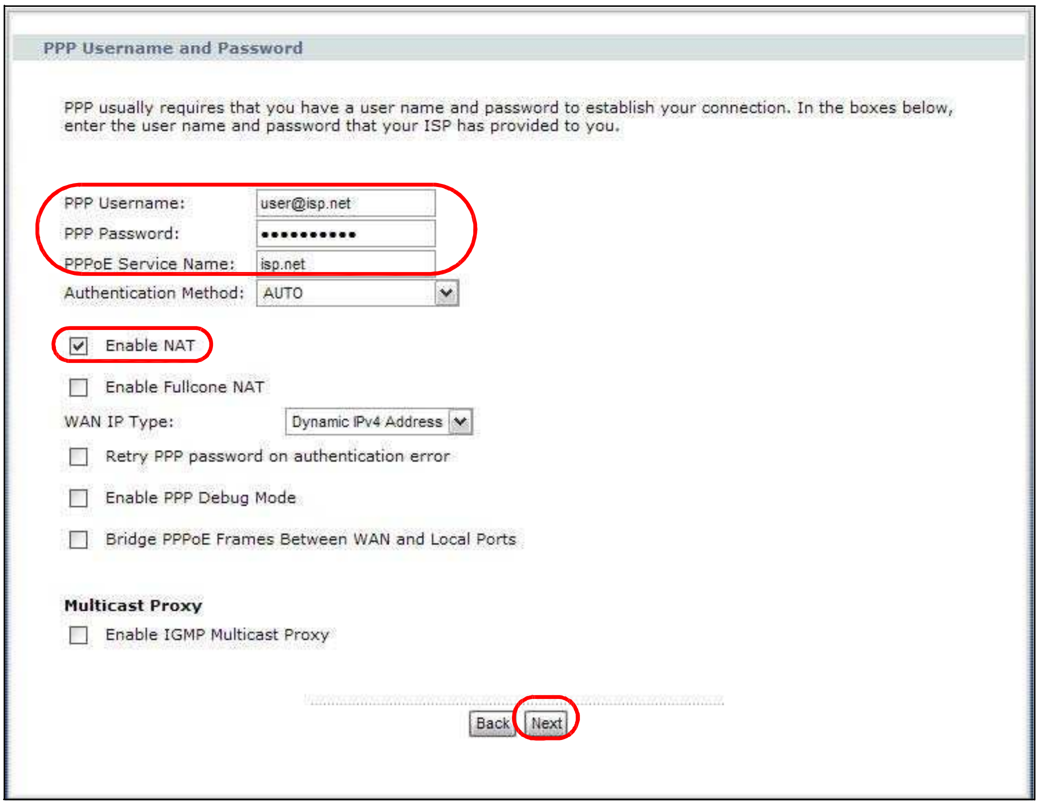
□ Tag VLAN ID for egress packets

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

□ Enable IPv6 for this service

5 Enter the user name (**user@isp.net** for example), password (**qwert12345** for example) and service name (**isp.net** for example) provided by your ISP for the PPPoE connection. Enable NAT on this connection. Click **Next**.



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: user@isp.net

PPP Password: ●●●●●●●●●●●

PPPoE Service Name: isp.net

Authentication Method: AUTO

☑ Enable NAT

□ Enable Fullcone NAT

WAN IP Type: Dynamic IPv4 Address

□ Retry PPP password on authentication error

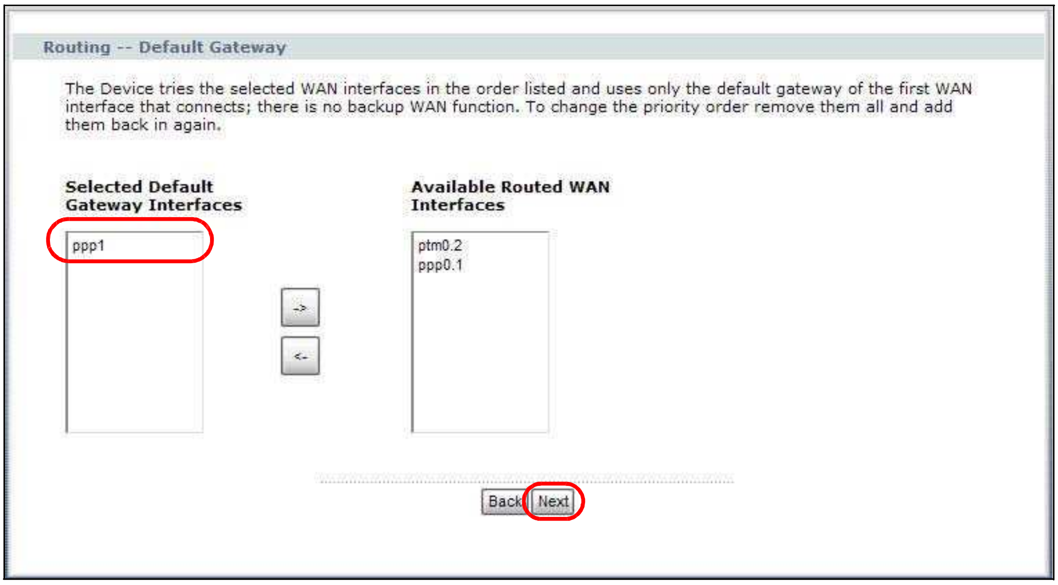
□ Enable PPP Debug Mode

□ Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

□ Enable IGMP Multicast Proxy

6 Remove the existing interfaces in the **Selected Default Gateway Interfaces** list. Select and move a WAN interface (**ppp1** in this example) to the **Selected Default Gateway Interfaces** list to use that interface as the default gateway. Click **Next**.

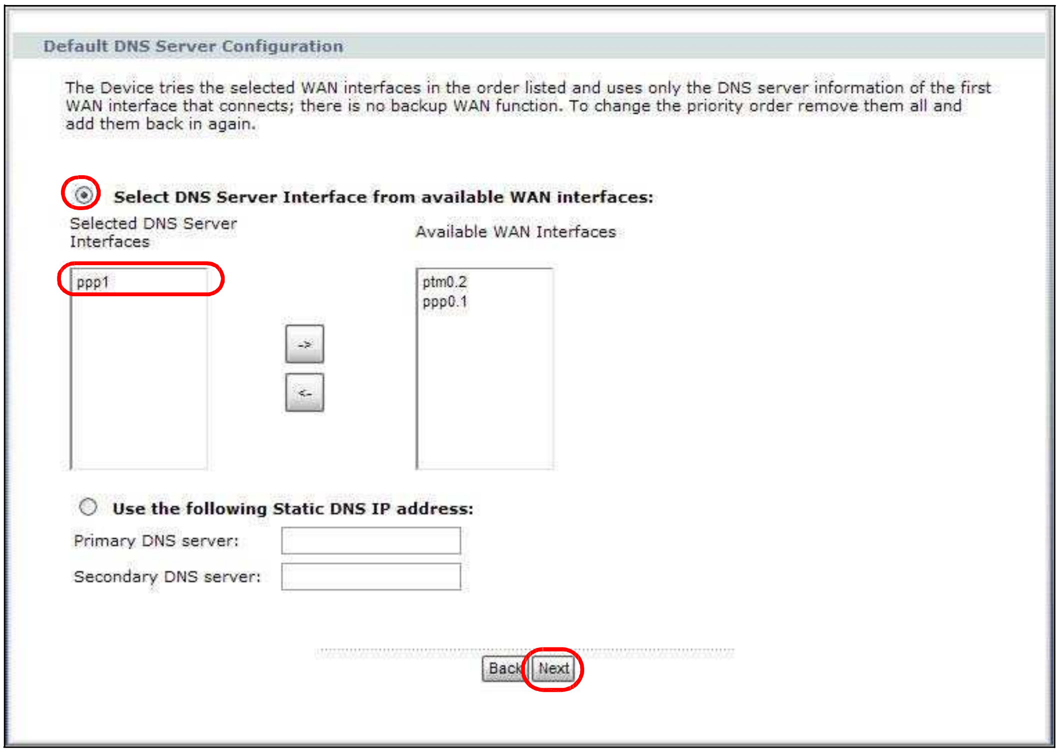


Routing -- Default Gateway

The Device tries the selected WAN interfaces in the order listed and uses only the default gateway of the first WAN interface that connects; there is no backup WAN function. To change the priority order remove them all and add them back in again.

Selected Default Gateway Interfaces	Available Routed WAN Interfaces
ppp1	ptm0.2 ppp0.1

7 Select the first option. Remove the existing interfaces in the **Selected DNS Server Interfaces** list. Select and move a WAN interface (**ppp1** in this example) to the **Selected DNS Server Interfaces** list to use that interface as the system DNS server. Click **Next**.



Default DNS Server Configuration

The Device tries the selected WAN interfaces in the order listed and uses only the DNS server information of the first WAN interface that connects; there is no backup WAN function. To change the priority order remove them all and add them back in again.

● Select DNS Server Interface from available WAN interfaces:

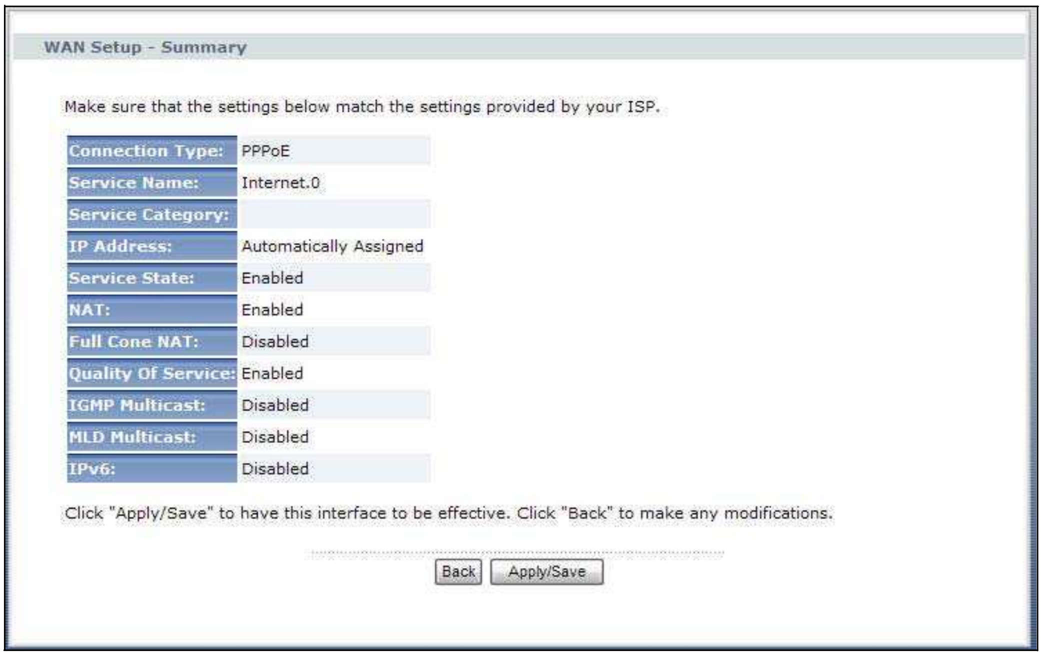
Selected DNS Server Interfaces	Available WAN Interfaces
ppp1	ptm0.2 ppp0.1

○ Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

8 The summary screen displays. Click **Apply/Save** to save your changes and go back to the **Internet Connection** screen.



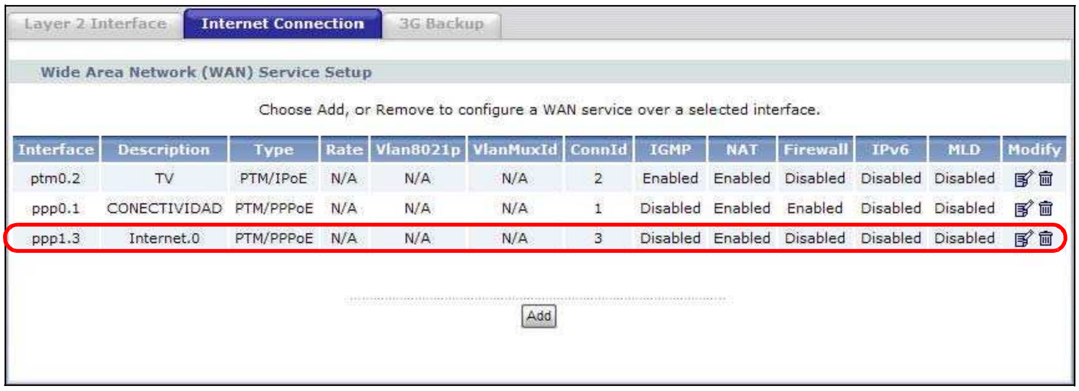
WAN Setup - Summary

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

Connection Type:	PPPoE
Service Name:	Internet.0
Service Category:	
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Full Cone NAT:	Disabled
Quality Of Service:	Enabled
IGMP Multicast:	Disabled
MLD Multicast:	Disabled
IPv6:	Disabled

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

9 You should see the WAN connection you just created in the **Internet Connection** screen. You are then able to access the Internet through this PPPoE connection when the Device's DSL port is connected properly.



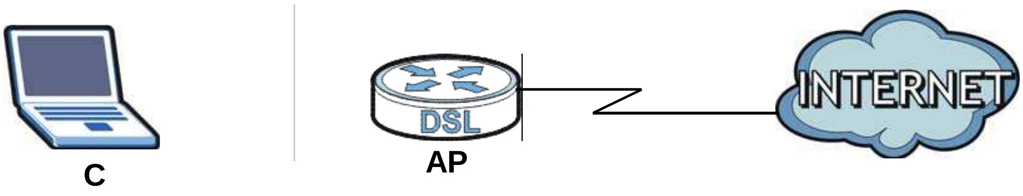
Wide Area Network (WAN) Service Setup

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

Interface	Description	Type	Rate	Vlan8021p	VlanMuxId	ConnId	IGMP	NAT	Firewall	IPv6	MLD	Modify
ptm0.2	TV	PTM/IPoE	N/A	N/A	N/A	2	Enabled	Enabled	Disabled	Disabled	Disabled	
ppp0.1	CONECTIVIDAD	PTM/PPPoE	N/A	N/A	N/A	1	Disabled	Enabled	Enabled	Disabled	Disabled	
ppp1.3	Internet.0	PTM/PPPoE	N/A	N/A	N/A	3	Disabled	Enabled	Disabled	Disabled	Disabled	

2.3 How to Set up a Secure Wireless Network

Thomas wants to set up a wireless network so that he can use his notebook to access the Internet. In this wireless network, the Device serves as an access point (**AP**), and the notebook with a wireless network card or USB/PCI adapter is the wireless client (**C**). The wireless client can access the Internet through the AP.



Thomas has to configure the wireless network settings on the Device. Then he can set up a wireless network using WPS (Section 2.3.2 on page 33) or manual configuration (Section 2.3.3 on page 37).

2.3.1 Configuring the Wireless Network Settings

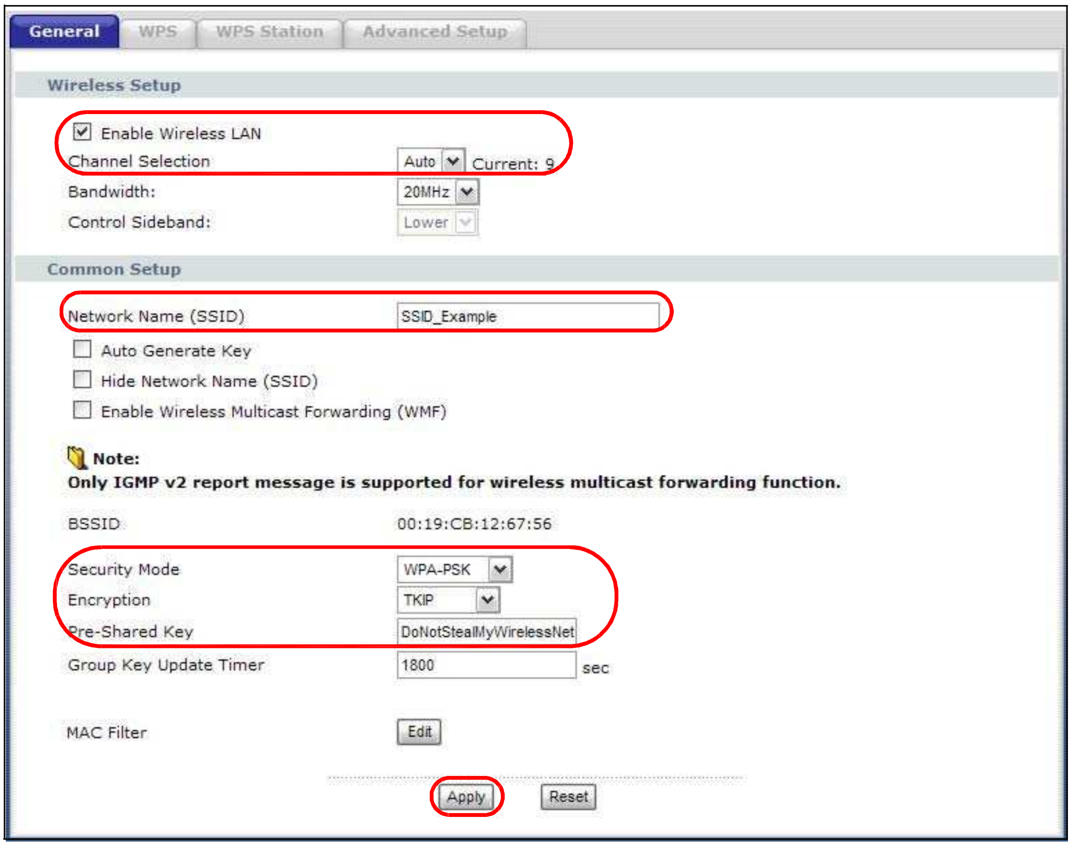
This example uses the following parameters to set up a wireless network.

SSID	SSID_Example
Security Mode	WPA-PSK
Pre-Shared Key	DoNotStealMyWirelessNetwork
802.11 Mode	IEEE 802.11b/g/n (Mixed)

Follow the steps below to configure the wireless settings on the Device.

Note: To see the default SSID, check the sticker on the rear panel of your Device. To see the current SSID, go to the **Status** screen.

1 Open the **Network > Wireless LAN > General** screen in the Device's web configurator. Configure the screen using the provided parameters (see page 30).



Wireless Setup

☑ Enable Wireless LAN

Channel Selection	Auto Current: 9
Bandwidth:	20MHz
Control Sideband:	Lower

Common Setup

Network Name (SSID)	SSID_Example

□ Auto Generate Key

□ Hide Network Name (SSID)

□ Enable Wireless Multicast Forwarding (WMF)

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

BSSID	00:19:CB:12:67:56
Security Mode	WPA-PSK
Encryption	TKIP
Pre-Shared Key	DoNotStealMyWirelessNet
Group Key Update Timer	1800 sec
MAC Filter	Edit

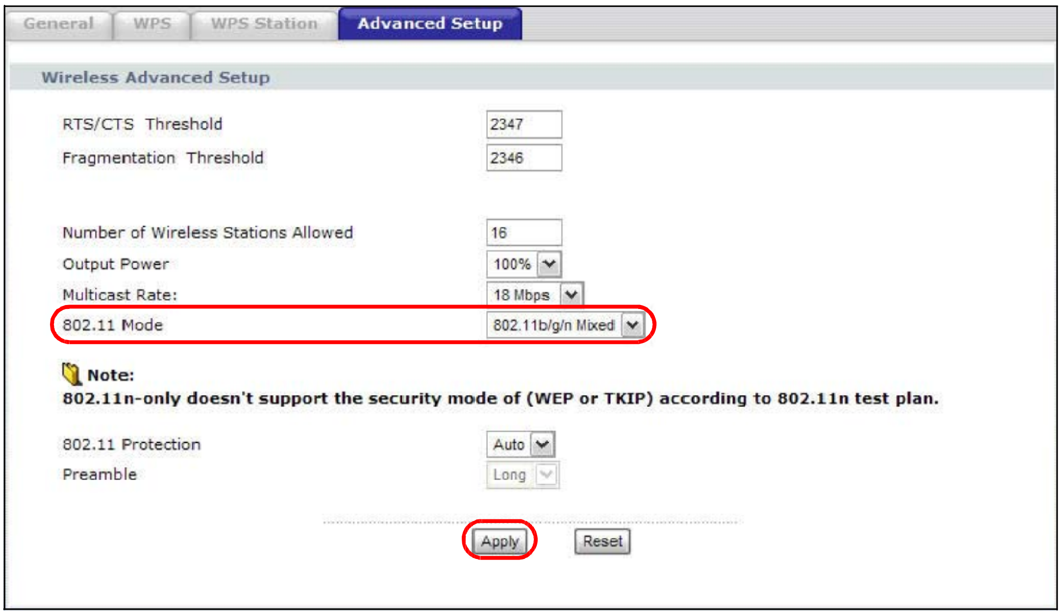
2 Make sure the **Enable Wireless LAN** check box is selected.

3 Select **Auto Channel Selection** to have the Device automatically determine a channel which is not used by another AP.

4 Enter "SSID_Example" as the SSID.

5 Set security mode to **WPA-PSK** and enter "DoNotStealMyWirelessNetwork" in the **Pre-Shared Key** field. Click **Apply**.

6 Click the **Advanced Setup** tab to display the advanced settings and select **802.11 b/g/n Mixed** in the **802.11 Mode** field. Click **Apply**.



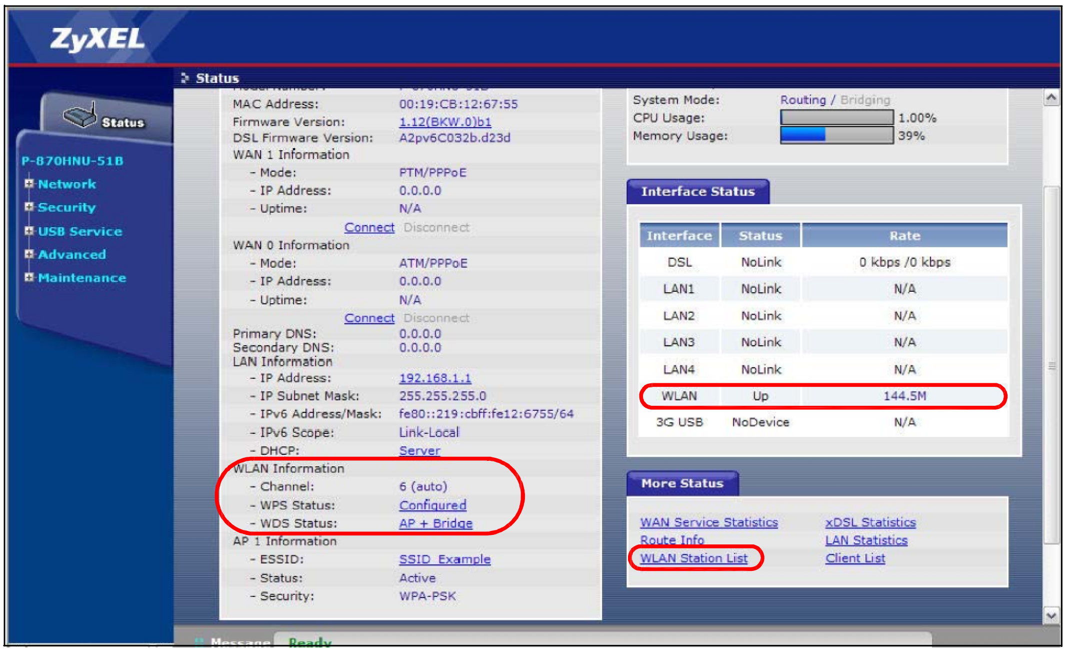
Wireless Advanced Setup

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/n Mixed

Note:
802.11n-only doesn't support the security mode of (WEP or TKIP) according to 802.11n test plan.

802.11 Protection	Auto
Preamble	Long

7 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**.



MAC Address:	00:19:CB:12:67:55
Firmware Version:	1.12(BKW.0)b1
DSL Firmware Version:	A2pv6C032b.d23d
WAN 1 Information	
- Mode:	PTM/PPPoE
- IP Address:	0.0.0.0
- Uptime:	N/A
WAN 0 Information	
- Mode:	ATM/PPPoE
- IP Address:	0.0.0.0
- Uptime:	N/A
Primary DNS:	0.0.0.0
Secondary DNS:	0.0.0.0
LAN Information	
- IP Address:	192.168.1.1
- IP Subnet Mask:	255.255.255.0
- IPv6 Address/Mask:	fe80::219:cbff:fe12:6755/64
- IPv6 Scope:	Link-Local
- DHCP:	Server
WLAN Information	
- Channel:	6 (auto)
- WPS Status:	Configured
- WDS Status:	AP + Bridge
AP 1 Information	
- ESSID:	SSID_Example
- Status:	Active
- Security:	WPA-PSK

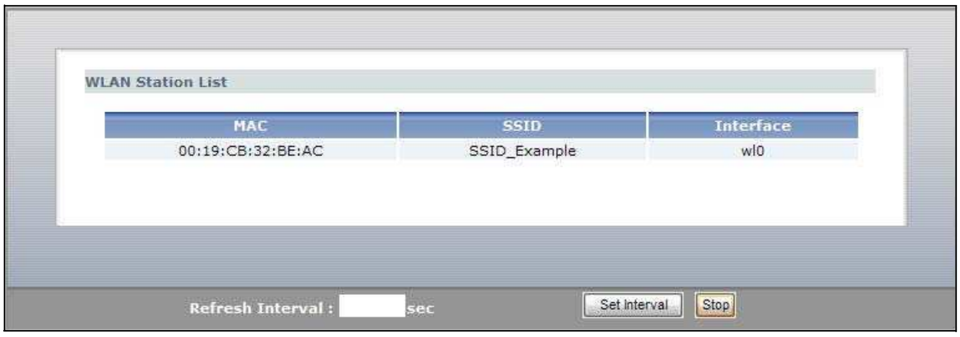
System Mode:	Routing / Bridging
CPU Usage:	1.00%
Memory Usage:	39%

Interface Status

Interface	Status	Rate
DSL	NoLink	0 kbps /0 kbps
LAN1	NoLink	N/A
LAN2	NoLink	N/A
LAN3	NoLink	N/A
LAN4	NoLink	N/A
WLAN	Up	144.5M
3G USB	NoDevice	N/A

8 Thomas can now use the WPS feature to establish a wireless connection between his notebook and the Device (see Section 2.3.2 on page 33). He can also use the notebook's wireless client to search for the Device (see Section 2.3.3 on page 37).

9 Click the **WLAN Station List** hyperlink in the **Status** screen. You can see if any wireless client has connected to the Device.



WLAN Station List

MAC	SSID	Interface
00:19:CB:32:BE:AC	SSID_Example	wl0

2.3.2 Using WPS

This section shows you how to set up a wireless network using WPS. It uses the Device as the AP and ZyXEL NWD210N as the wireless client which connects to the notebook.

Note: The wireless client must be a WPS-aware device (for example, a WPS USB adapter or PCMCIA card).

There are two WPS methods to set up the wireless client settings:

- **Push Button Configuration (PBC)** - simply press a button. This is the easier of the two methods.
- **PIN Configuration** - configure a Personal Identification Number (PIN) on the Device. A wireless client must also use the same PIN in order to download the wireless network settings from the Device.

Push Button Configuration (PBC)

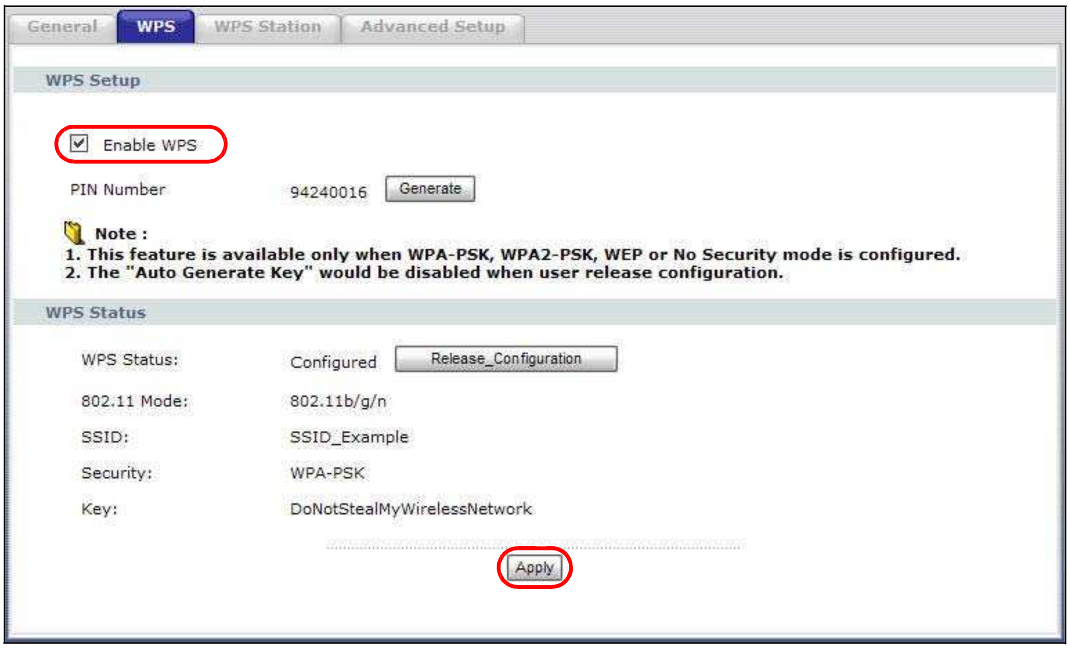
1 Make sure that your Device is turned on and your notebook is within the cover range of the wireless signal.

2 Make sure that you have installed the wireless client driver and utility in your notebook.

3 Press the WPS button on your notebook within range of the Device.

4 The wireless LAN of the Device is disabled by default. Press the WLAN/WPS button for three seconds and release it when the LED turns green. The wireless LAN is on. Then press the WLAN/WPS button for more than eight seconds and release it when the **WLAN/WPS** LED is blinking orange.

5 Alternatively, you may log into Device’s web configurator, make sure the **Enable WPS** checkbox is selected and click **Apply** in the **Network** > **Wireless LAN** > **WPS Station** screen.



☑ Enable WPS

PIN Number 94240016 Generate

Note :
1. This feature is available only when WPA-PSK, WPA2-PSK, WEP or No Security mode is configured.
2. The "Auto Generate Key" would be disabled when user release configuration.

WPS Status: Configured

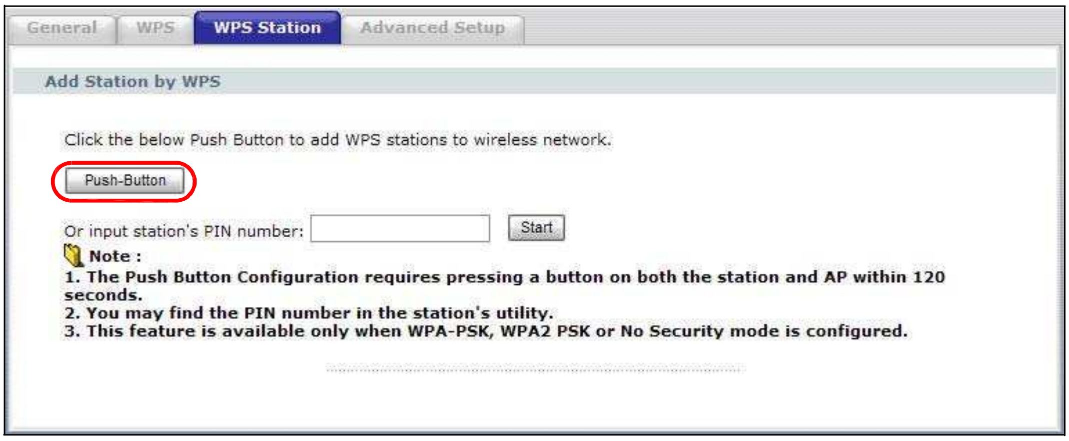
802.11 Mode: 802.11b/g/n

SSID: SSID_Example

Security: WPA-PSK

Key: DoNotStealMyWirelessNetwork

6 Click the **Push Button** in the **Network** > **Wireless LAN** > **WPS Station** screen.



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

Or input station's PIN number:

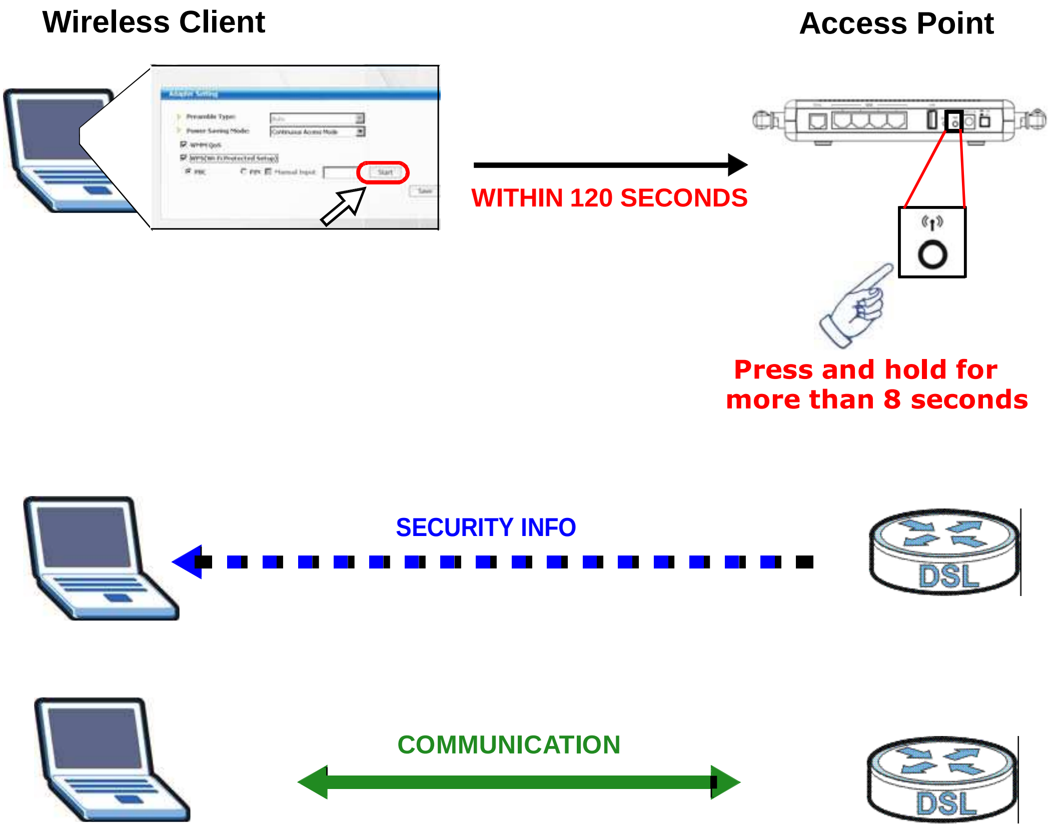
Note :
1. The Push Button Configuration requires pressing a button on both the station and AP within 120 seconds.
2. You may find the PIN number in the station's utility.
3. This feature is available only when WPA-PSK, WPA2 PSK or No Security mode is configured.

Note: Your Device has a WLAN/WPS button located on its rear panel as well as a WPS button in its configuration utility. Both buttons have exactly the same function: you can use one or the other.

Note: It doesn’t matter which button is pressed first. You must press the second button within 120 seconds of pressing the first one.

7 When the Device is sending the configuration settings to the wireless client, the **WLAN/WPS** LED blinks orange. This may take up to two minutes. Then the **WLAN/WPS** LED turns green when the wireless client is able to communicate with the Device securely.

The following figure shows you an example of how to set up a wireless network and its security by pressing a button on both Device and wireless client.

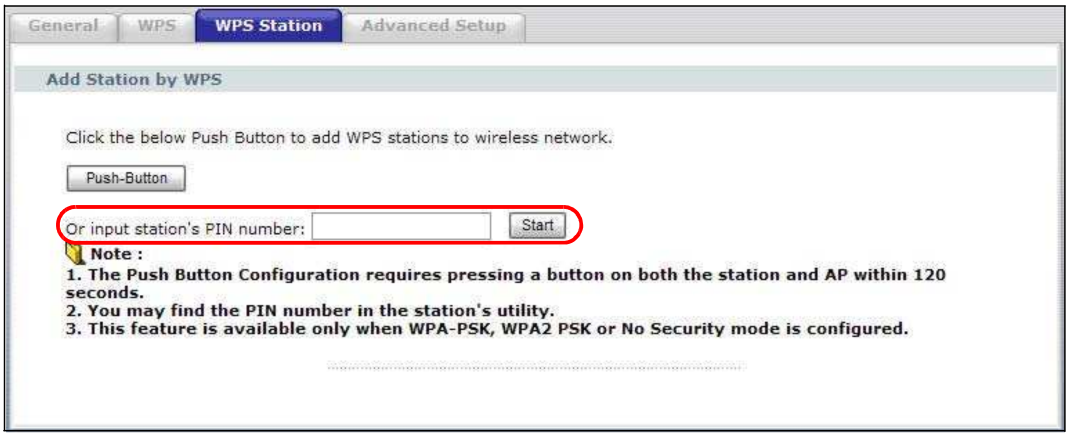


PIN Configuration

When you use the PIN configuration method, you need to use both the Device’s web configurator and the wireless client’s utility.

1 Launch your wireless client’s configuration utility. Go to the WPS settings and select the PIN method to get a PIN number.

2 Enter the PIN number in the **PIN** field in the **Network** > **Wireless LAN** > **WPS Station** screen on the Device.



Add Station by WPS

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

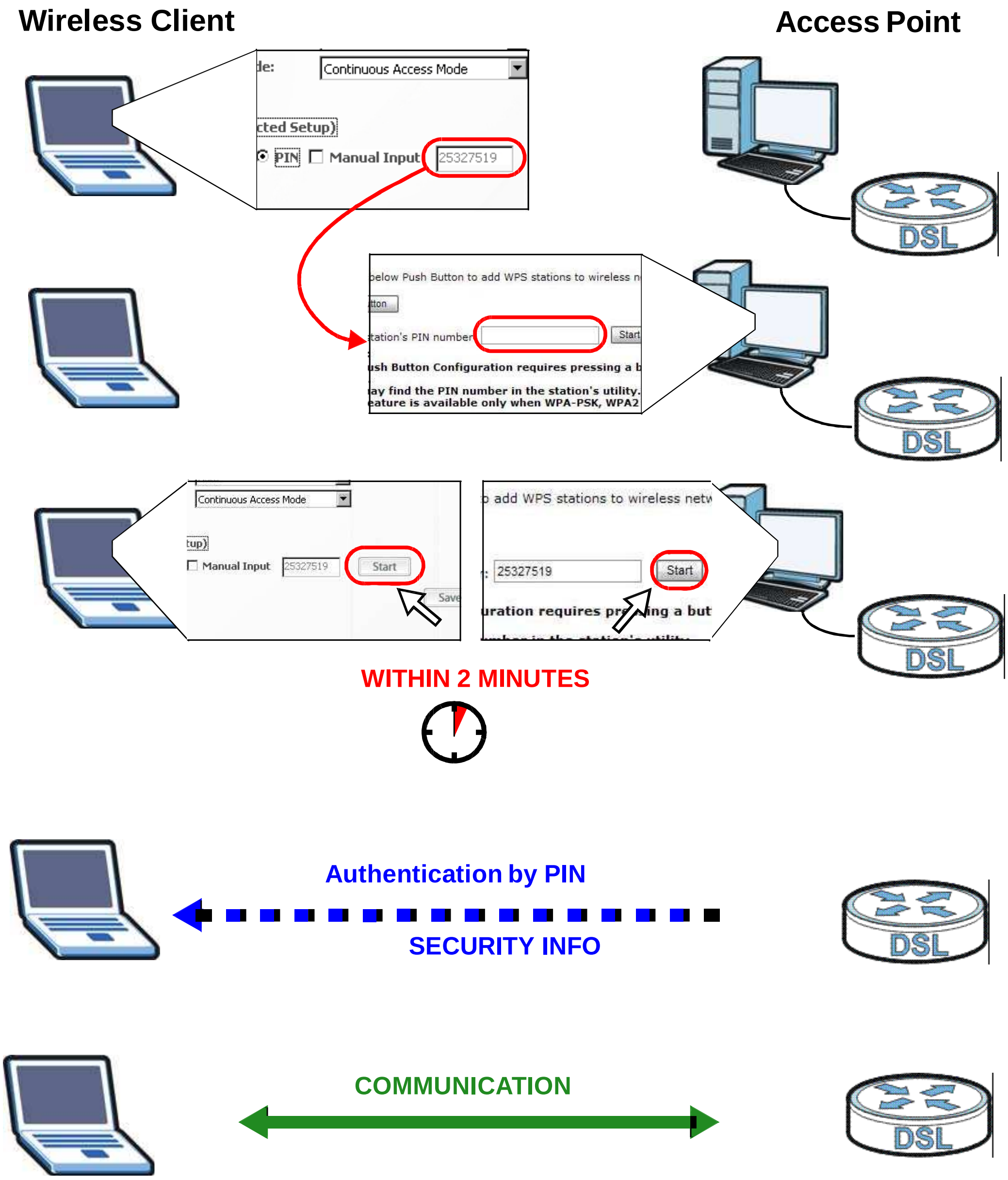
Or input station's PIN number:

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.

3 Click the **Start** buttons (or the button next to the PIN field) on both the wireless client utility screen and the Device’s **WPS Station** screen within two minutes.

The Device authenticates the wireless client and sends the proper configuration settings to the wireless client. This may take up to two minutes. The wireless client is then able to communicate with the Device securely.

The following figure shows you how to set up a wireless network and its security on a Device and a wireless client by using PIN method.


Wireless Client
Access Point
de: Continuous Access Mode
cted Setup)
PIN Manual Input 25327519
below Push Button to add WPS stations to wireless n
tton
tation's PIN number Start
ush Button Configuration requires pressing a b
ay find the PIN number in the station's utility.
eature is available only when WPA-PSK, WPA2
Continuous Access Mode
tup)
Manual Input 25327519 Start
Save
o add WPS stations to wireless netw
: 25327519 Start
uration requires pressing a but
DSL
WITHIN 2 MINUTES
Authentication by PIN
SECURITY INFO
COMMUNICATION

2.3.3 Without WPS

Use the wireless adapter’s utility installed on the notebook to search for the “Example” SSID. Then enter the “DoNotStealMyWirelessNetwork” pre-shared key to establish an wireless Internet connection.

Note: The Device supports IEEE 802.11b, IEEE 802.11g and IEEE 802.11n wireless clients. Make sure that your notebook or computer’s wireless adapter supports one of these standards.

2.4 How to Use File Sharing on the Device

In this tutorial you can:

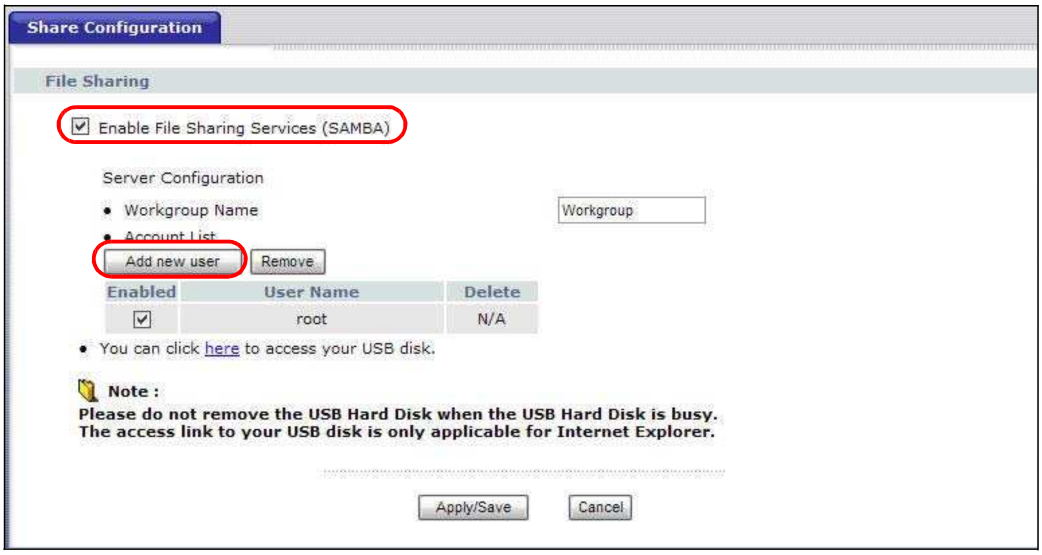
- Set up file sharing
- Access the shared files from a computer

2.4.1 Set up file sharing

To set up file sharing, you need to enable file sharing and have a user account on your Device. This shares the files in your USB device to other users in the local network.

1 Go to **USB Service > File Sharing** to enable file sharing and enter a workgroup name.

2 Before you can share files you need a user account. To set up a new file sharing user account, click **Add new user**.



File Sharing

☑ Enable File Sharing Services (SAMBA)

Server Configuration

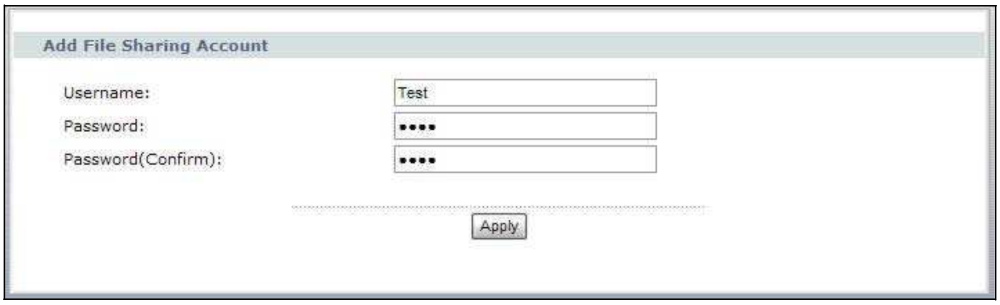
- Workgroup Name: Workgroup
- Account List

Enabled	User Name	Delete
☑	root	N/A

- You can click here to access your USB disk.

Note :
Please do not remove the USB Hard Disk when the USB Hard Disk is busy.
The access link to your USB disk is only applicable for Internet Explorer.

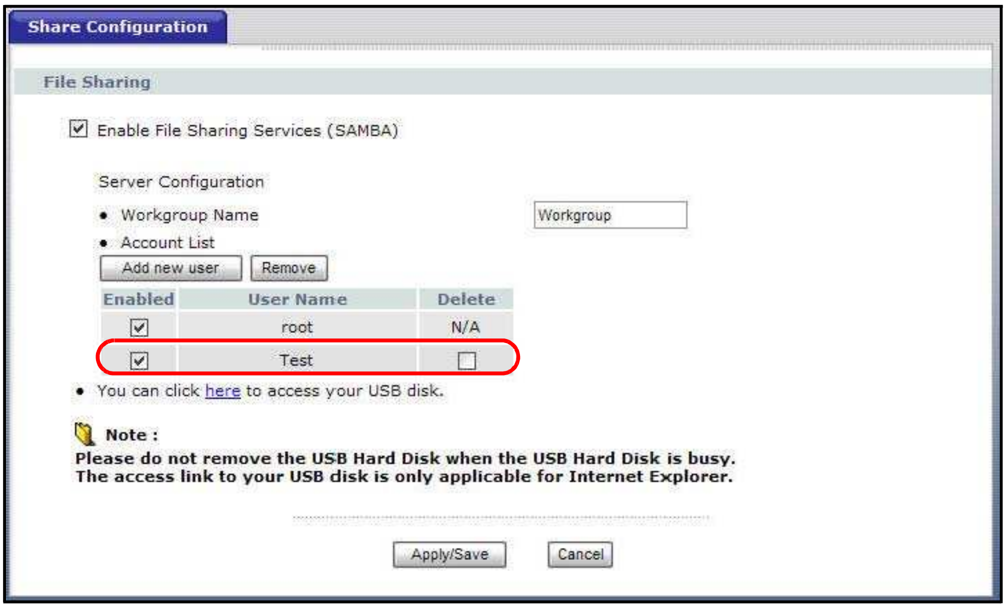
3 Enter a user name and password. Click **Apply** to save your changes go back to the previous screen.



Add File Sharing Account

Username:	Test
Password:	••••
Password(Confirm):	••••

4 Make sure the account is active.



☑ Enable File Sharing Services (SAMBA)

Server Configuration

- Workgroup Name: Workgroup
- Account List

Enabled	User Name	Delete
☑	root	N/A
☑	Test	□

- You can click here to access your USB disk.

Note :
Please do not remove the USB Hard Disk when the USB Hard Disk is busy.
The access link to your USB disk is only applicable for Internet Explorer.

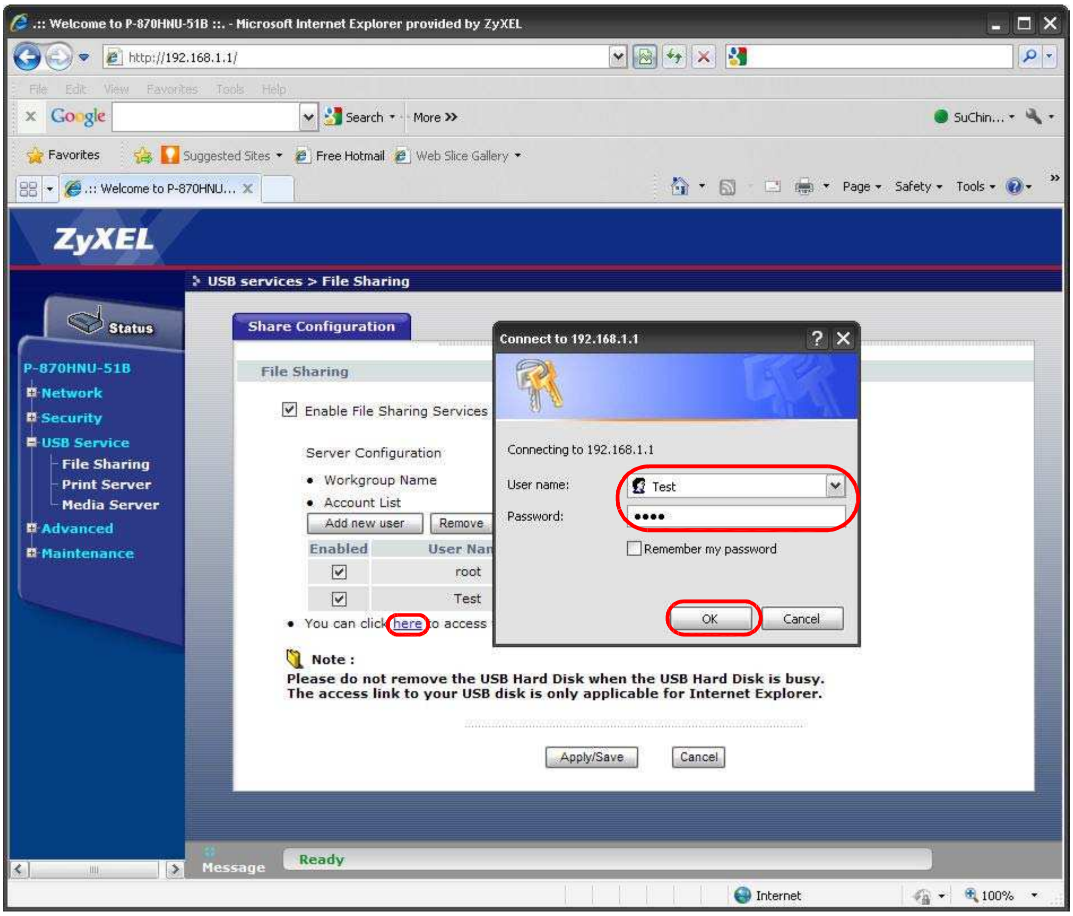
2.4.2 Access Your Shared Files From a Computer

You can use the Web Configurator or Windows Explorer to access the USB storage device connected to the Device.

2.4.2.1 Web Configurator

1 If you are using Internet Explorer, access the Device’s Web Configurator and click the link in the **File Sharing** screen.

2 A screen pops up asking for password authentication. Enter the pre-configured user account's user name and password. Click **OK**.



☑ Enable File Sharing Services

Server Configuration
- Workgroup Name
- Account List

Add new user | Remove

Enabled	User Nan
☑	root
☑	Test

- You can click here to access

Note :
Please do not remove the USB Hard Disk when the USB Hard Disk is busy.
The access link to your USB disk is only applicable for Internet Explorer.

Apply/Save | Cancel

Connect to 192.168.1.1

Connecting to 192.168.1.1

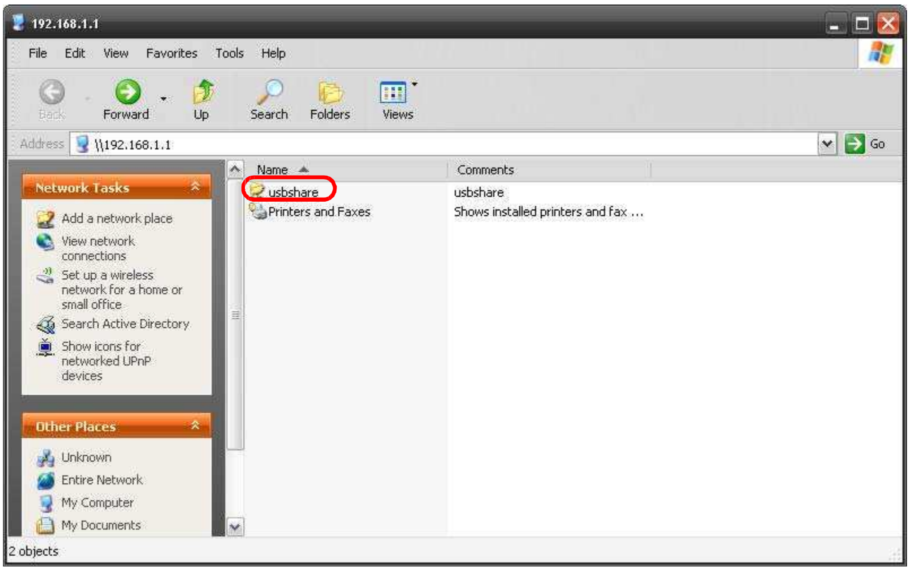
User name: Test

Password: ••••

□ Remember my password

OK | Cancel

3 A screen appears and shows you the folder for the USB device connected to your Device. Double-click the folder to display the contents in it.



Address \\192.168.1.1

Name	Comments
usbshare	usbshare
Printers and Faxes	Shows installed printers and fax ...

2 objects

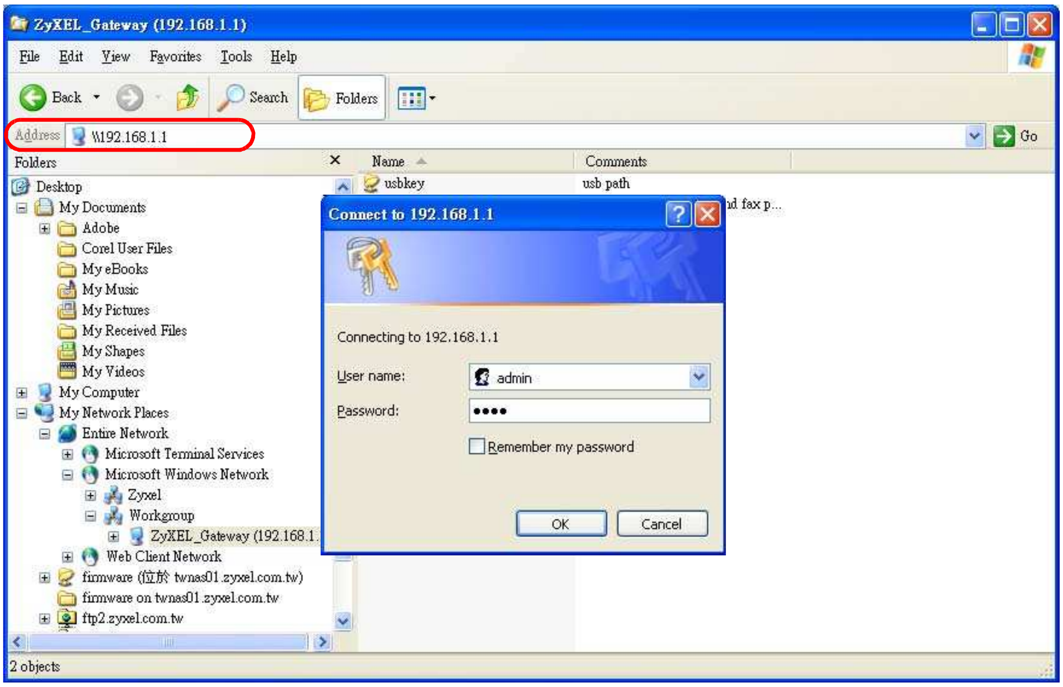
2.4.2.2 Windows Explorer

Note: The examples in this User's Guide show you how to use Microsoft's Windows XP to browse your shared files. Refer to your operating system's documentation for how to browse your file structure.

1 Open Windows Explorer to share files in the attached USB device using Windows Explorer browser.

2 In Windows Explorer's Address bar type a double backslash "\\" followed by the IP address of the Device (the default IP address of the Device is 192.168.1.1) and press [ENTER]. A screen asking for password authentication appears. Type the user name and password you set up for file sharing and click **OK**.

Figure 3 File Sharing via Windows Explorer



Address \\192.168.1.1

Connecting to 192.168.1.1

User name: admin

Password: ••••

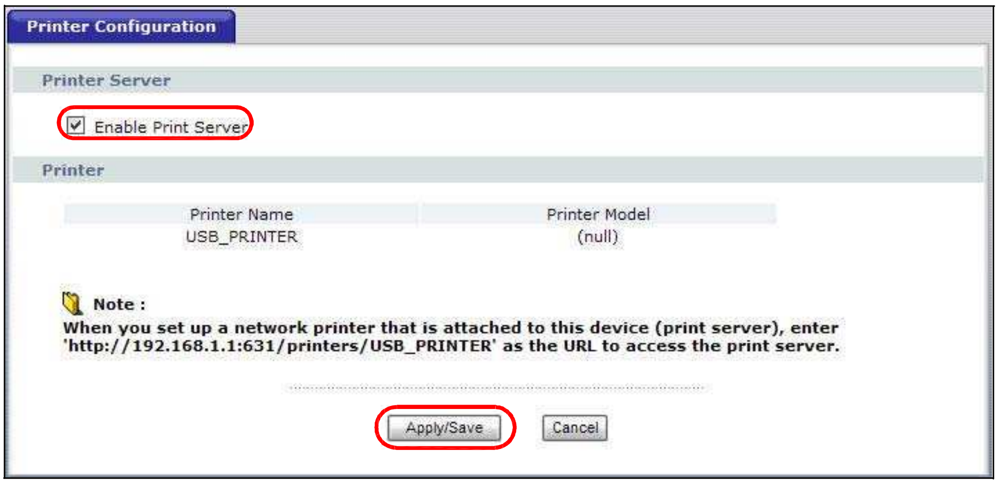
□ Remember my password

Note: Once you log in to the file share via your Device, you do not have to log in again unless you restart your computer.

2.5 How to Share a USB Printer via Your Device

Your Device can act as a print server and let the computers on your network use the USB printer that is connected to the Device's USB port.

1 Go to **USB Service > Print Server** to enable the print server function on the Device. Click **Apply/ Save** to save your settings.



Printer Name	Printer Model
USB_PRINTER	(null)

Note :
When you set up a network printer that is attached to this device (print server), enter 'http://192.168.1.1:631/printers/USB_PRINTER' as the URL to access the print server.

2 Make sure that a USB printer is connected to the Device.

3 See Section 11.5 on page 171 and/or Section 11.6 on page 175 for examples of how to set up a printer on your computer. The computers on your network must have the printer software already installed before they can use the printer.

2.6 How to Prioritize Traffic Using QoS Class and Queue

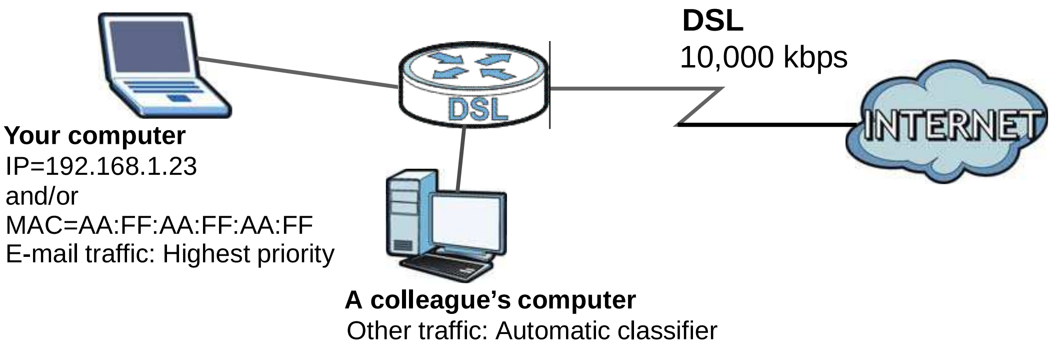
This tutorial shows you how to group traffic and give priorities using QoS. Let's say you are a team leader of a small sales branch office. You want to prioritize e-mail traffic because your task includes sending urgent updates to clients at least twice every hour. You also upload data files (such as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

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

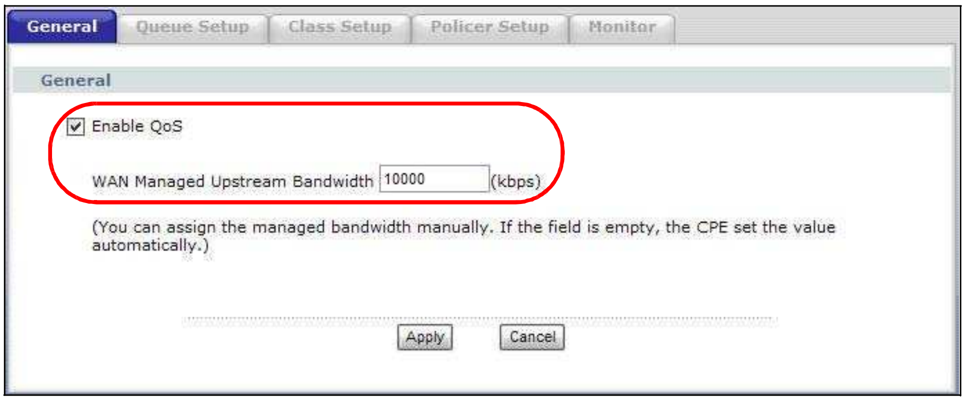
- Configure a queue to assign the highest priority queue (1) to e-mail traffic from the LAN1 interface, so that e-mail traffic would not get delayed when there is network congestion.
- Note the IP address (192.168.1.23 for example) and/or MAC address (AA:FF:AA:FF:AA:FF for example) of your computer and map it to the queue.

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

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



1 Click **Advanced > QoS > General** and enable QoS on the Device. Set your **WAN Managed Upstream Bandwidth** to 10,000 kbps (or leave this blank to have the Device automatically determine this figure). Click **Apply**.



☑ Enable QoS

WAN Managed Upstream Bandwidth 10000 (kbps)

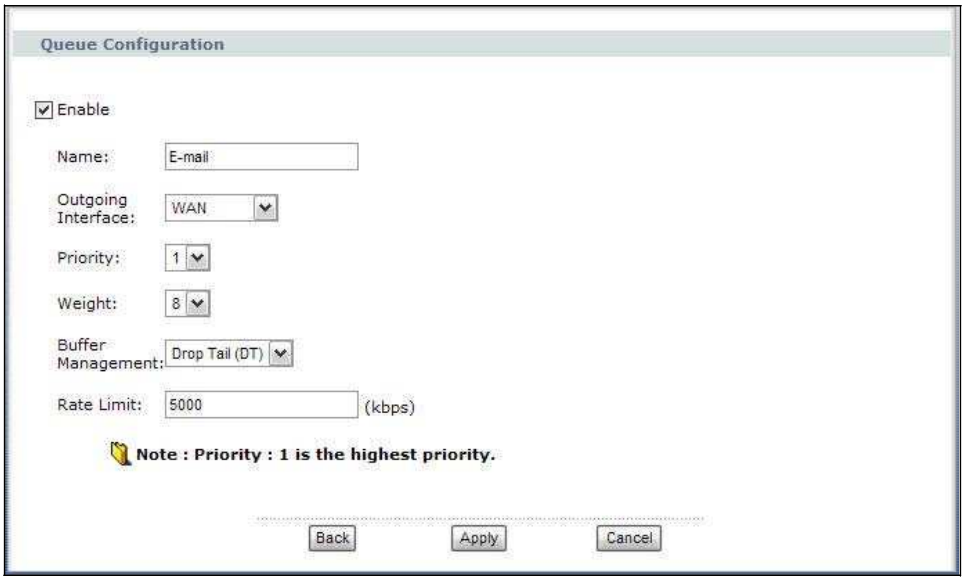
(You can assign the managed bandwidth manually. If the field is empty, the CPE set the value automatically.)

2 Go to **Advanced > QoS > Queue Setup**. Click **Add** to create a new queue. In the screen that opens, check **Enable** and enter or select the following values:

- **Name**: E-mail
- **Outgoing Interface**: WAN
- **Priority**: 1 (Highest)
- **Weight**: 8

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

Click **Apply** to save you changes.



Queue Configuration

☑ Enable

Name: E-mail

Outgoing Interface: WAN

Priority: 1

Weight: 8

Buffer Management: Drop Tail (DT)

Rate Limit: 5000 (kbps)

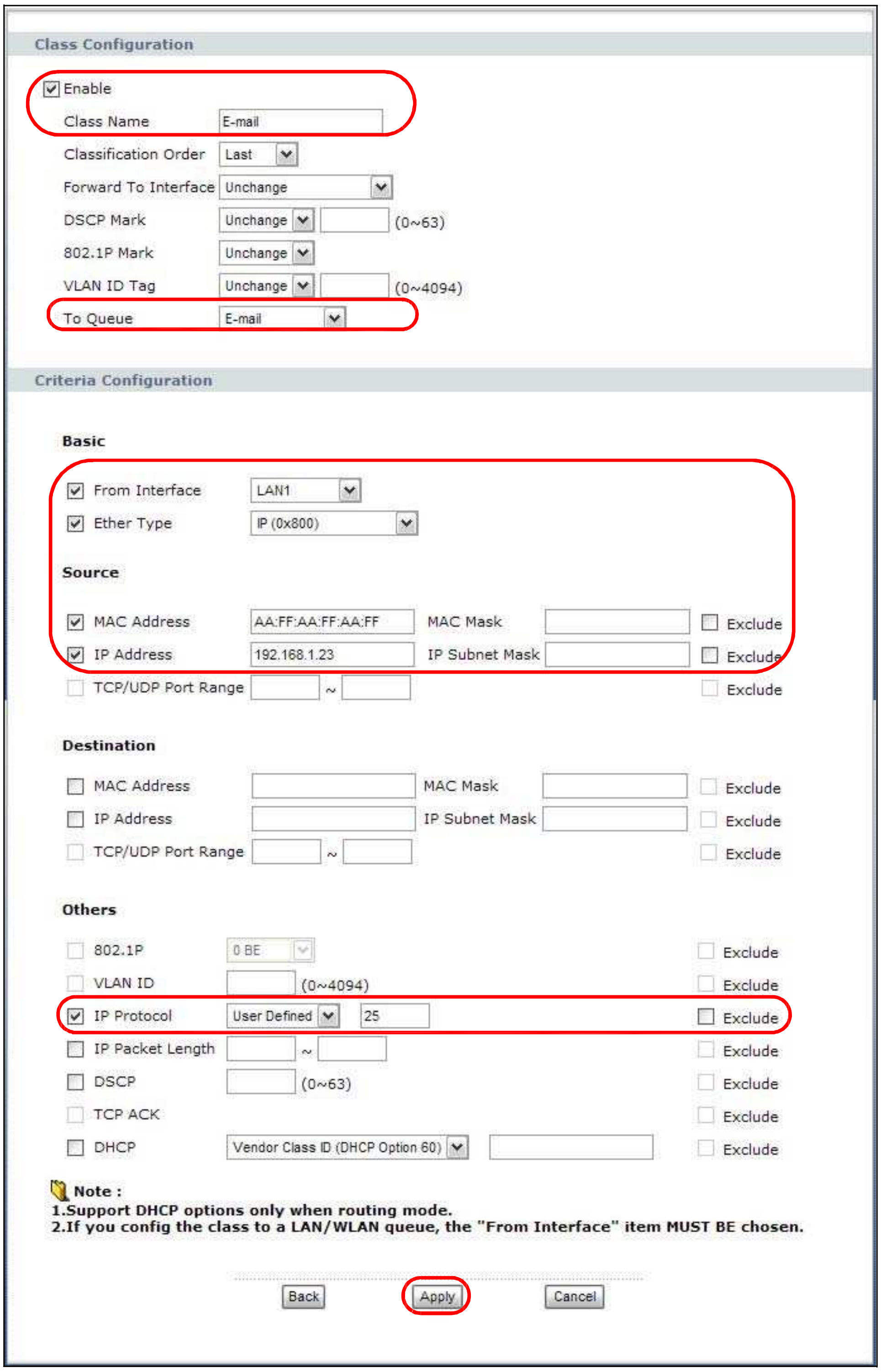
Note : Priority : 1 is the highest priority.

3 Go to **Advanced > QoS > Class Setup**. Click **Add** to create a new class. Select **Enable** and follow the settings as shown in the screen below.

- **Class Name**: E-mail
- **To Queue**: E-mail
- **From Interface**: LAN1 (the interface from which the traffic will be coming from)
- **Ether Type**: IP (to identify the traffic source by its IP address or MAC address)
- **MAC Address**: AA:FF:AA:FF:AA:FF (the MAC address of your computer)
- **IP Address**: 192.168.1.23 (the IP address of your computer)
- **IP Protocol**: user-defined port 25

Click **Apply** to save you changes.

This maps e-mail traffic coming from port 25 to the highest priority, which you have created in the previous screen. This also maps your computer’s IP address and MAC address to the **E-mail** queue.



Class Configuration

☑ Enable

Class Name: E-mail

Classification Order: Last

Forward To Interface: Unchange

DSCP Mark: Unchange (0~63)

802.1P Mark: Unchange

VLAN ID Tag: Unchange (0~4094)

To Queue: E-mail

Criteria Configuration

Basic

☑ From Interface: LAN1

☑ Ether Type: IP (0x800)

Source

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

☑ IP Address: 192.168.1.23 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: (0~4094) □ Exclude

☑ IP Protocol: User Defined 25 □ Exclude

□ IP Packet Length: ~ □ Exclude

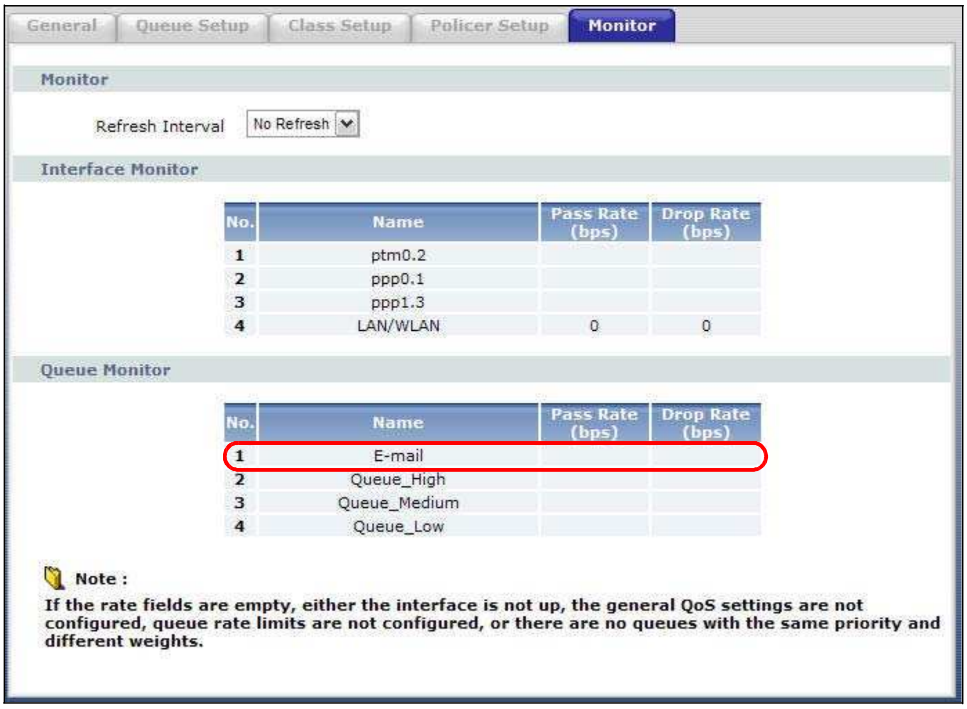
□ DSCP: (0~63) □ Exclude

□ TCP ACK □ Exclude

□ DHCP: Vendor Class ID (DHCP Option 60) □ Exclude

Note :
1.Support DHCP options only when routing mode.
2.If you config the class to a LAN/WLAN queue, the "From Interface" item MUST BE chosen.

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



Monitor

Refresh Interval: No Refresh

Interface Monitor

No.	Name	Pass Rate (bps)	Drop Rate (bps)
1	ptm0.2		
2	ppp0.1		
3	ppp1.3		
4	LAN/WLAN	0	0

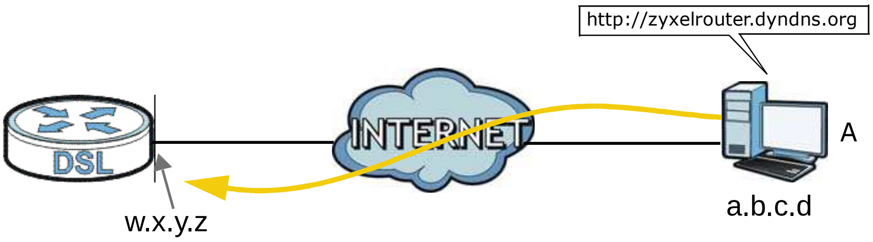
Queue Monitor

No.	Name	Pass Rate (bps)	Drop Rate (bps)
1	E-mail		
2	Queue_High		
3	Queue_Medium		
4	Queue_Low		

Note :
If the rate fields are empty, either the interface is not up, the general QoS settings are not configured, queue rate limits are not configured, or there are no queues with the same priority and different weights.

2.7 How to Access the Device Using DDNS

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



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

This tutorial shows you how to:

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

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

2.7.1 Registering a DDNS Account on www.dyndns.org

1. Open a browser and type **http://www.dyndns.org**.
2. Apply for a user account. This tutorial uses **UserName1** and **12345** as the username and password.
3. Log into www.dyndns.org using your account.
4. Add a new DDNS host name. This tutorial uses the following settings as an example.
   - Hostname: **zyxelrouter.dyndns.org**
   - Service Type: **Host with IP address**
   - IP Address: Enter the WAN IP address that your Device is currently using. You can find the IP address on the Device’s Web Configurator **Status** page.

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

2.7.2 Configuring DDNS on Your Device

1. Log into the Device's advanced mode.
2. Configure the following settings in the **Advanced** > **Dynamic DNS** screen.

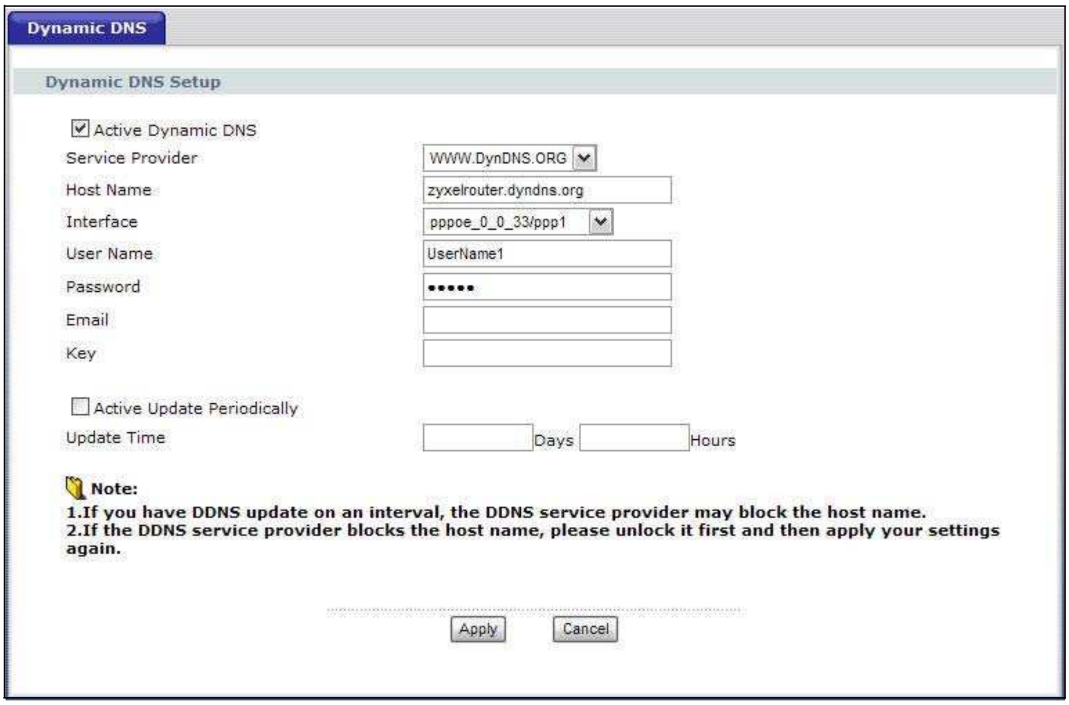
   2a Select **Active Dynamic DNS**.

   2b Select **WWW.DynDNS.ORG** as the **Service Provider**.

   2c Type **zyxelrouter.dyndns.org** in the **Host Name** field.

   2d Select a WAN interface to use for updating the IP address of the domain name.

2e Enter the user name (**UserName1** for example) and password (**12345** for example).



Dynamic DNS Setup

☑ Active Dynamic DNS

Service Provider	WWW.DynDNS.ORG
Host Name	zyxelrouter.dyndns.org
Interface	pppoe_0_0_33/ppp1
User Name	UserName1
Password	•••••
Email	
Key	

□ Active Update Periodically

Update Time Days Hours

Note:
1.If you have DDNS update on an interval, the DDNS service provider may block the host name.
2.If the DDNS service provider blocks the host name, please unlock it first and then apply your settings again.

2f Click **Apply**.

2.7.3 Testing the DDNS Setting

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

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

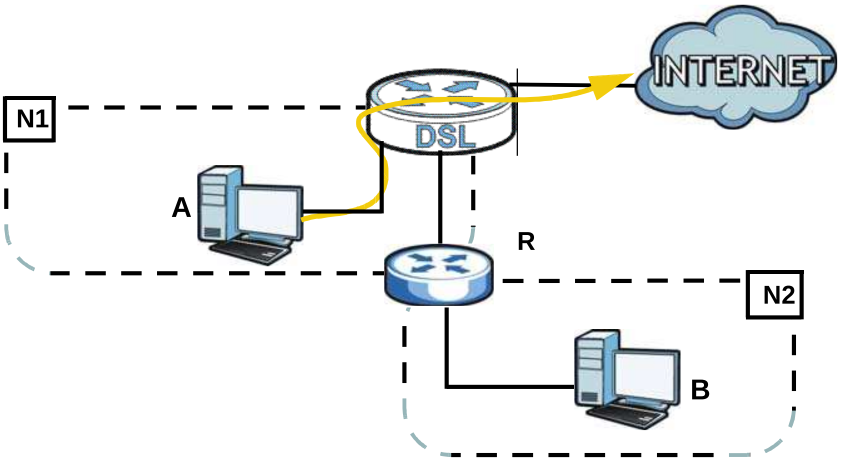
2 Type **http://zyxelrouter.dyndns.org** and press [Enter].

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

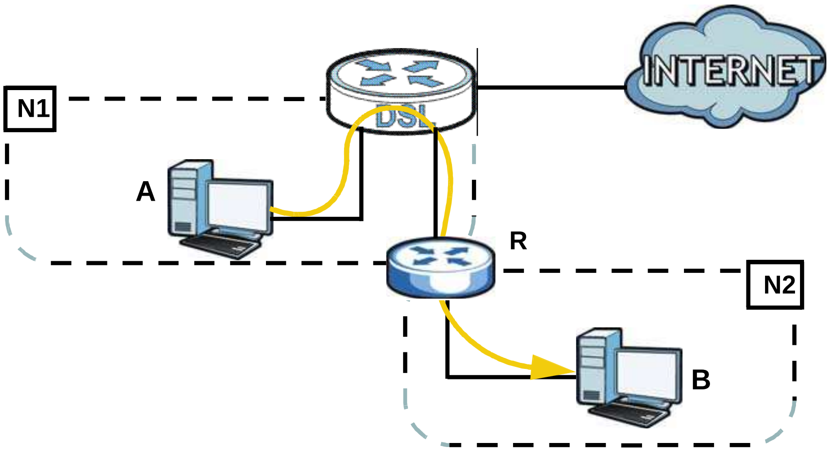
2.8 How to Route Traffic to Another Network Using Static Route

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

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



You need to specify a static routing rule on the Device to specify **R** as the router in charge of forwarding traffic to **N2**. In this case, the Device routes traffic from **A** to **R** and then **R** routes the traffic to **B**.



This tutorial uses the following example IP settings:

Table 2 IP Settings in this Tutorial

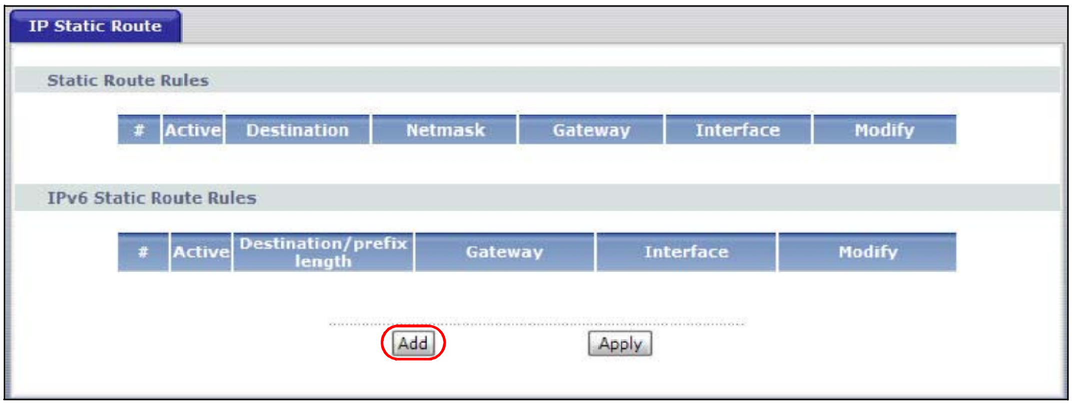
DEVICE / COMPUTER	IP ADDRESS
The Device's WAN	172.16.1.1
The Device's LAN	192.168.1.1
A	192.168.1.34
R's N1	192.168.1.253
R's N2	192.168.10.2
B	192.168.10.33

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

1 Log into the Device’s Web Configurator in advanced mode.

2 Click **Advanced** > **Static Route**.

3 Click **Add** in the **Static Route** screen.



IP Static Route

Static Route Rules

#	Active	Destination	Netmask	Gateway	Interface	Modify

IPv6 Static Route Rules

#	Active	Destination/prefix length	Gateway	Interface	Modify

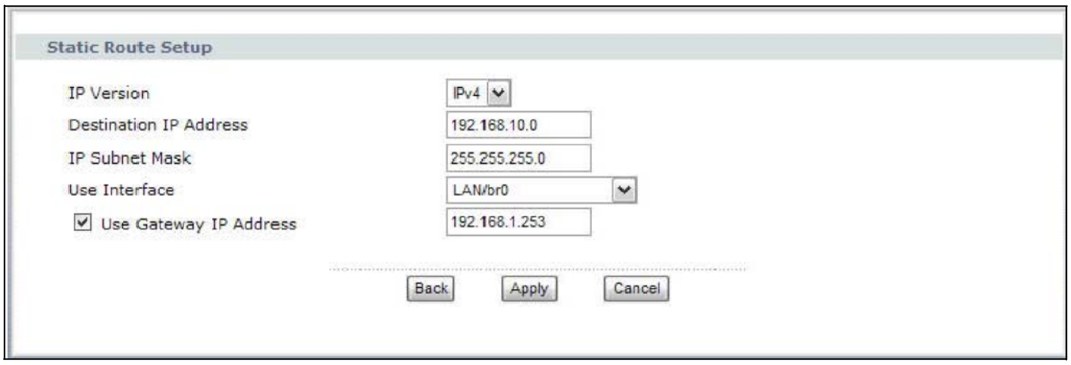
4 Configure the **Static Route Setup** screen using the following settings:

4a Select **IPv4** in the **IP Version** field.

4b Type **192.168.10.0** and subnet mask **255.255.255.0** for the destination, **N2**.

4c Select the LAN interface through which the traffic is sent.

4d Select the **Use Gateway IP Address** checkbox and type **192.168.1.253** (**R**’s N1 address).



Static Route Setup

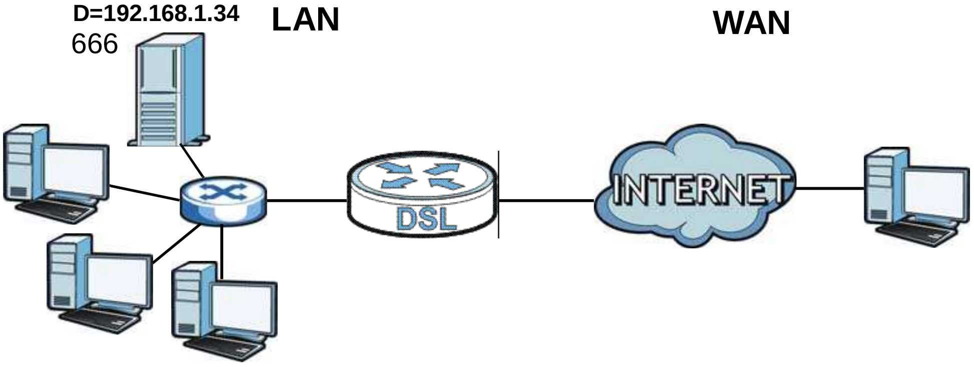
IP Version	IPv4
Destination IP Address	192.168.10.0
IP Subnet Mask	255.255.255.0
Use Interface	LAN/br0
☑ Use Gateway IP Address	192.168.1.253

4a Click **Apply**.

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

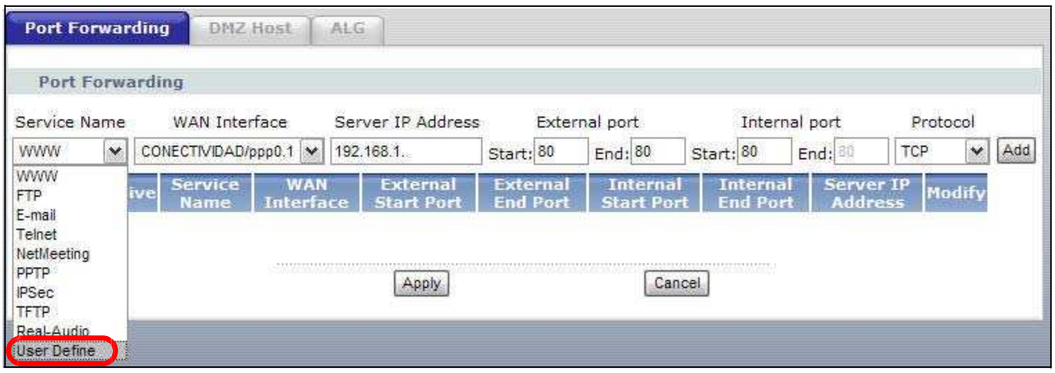
2.9 How to Set Up NAT Port Forwarding

Thomas manages the Doom server on a computer behind the Device. In order for players on the Internet to communicate with the Doom server, Thomas needs to configure the port settings and IP address on the Device. Traffic should be forwarded to the port 666 of the Doom server computer which has an IP address of 192.168.1.34.



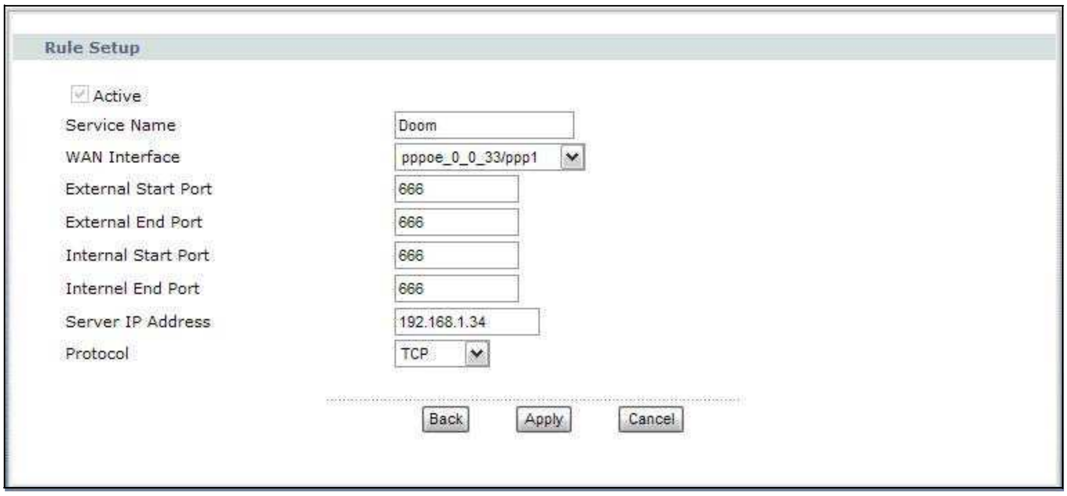
1 Make sure you enable NAT on a WAN connection through which port traffic is transmitted.

2 Click **Network** > **NAT** > **Port Forwarding** to open the following screen. Select **User Define** from the **Service Name** field.



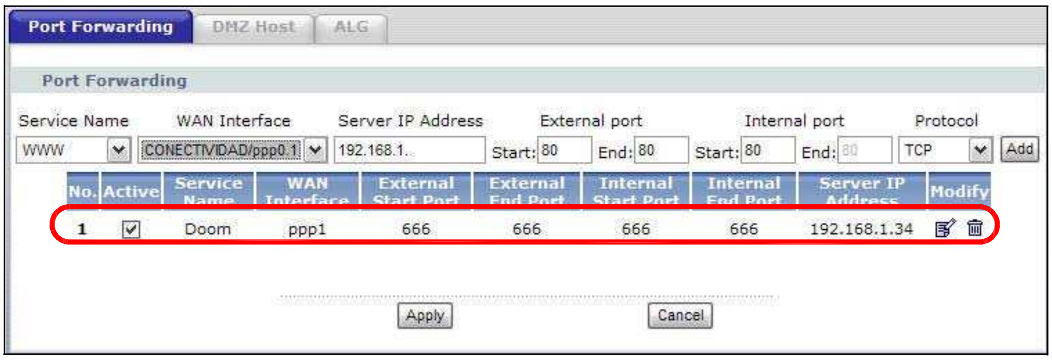
Service Name	WAN Interface	Server IP Address	External port		Internal port		Protocol
WWW	CONECTIVIDAD/ppp0.1	192.168.1.	Start: 80	End: 80	Start: 80	End: 80	TCP

3 Configure the screen as follows to forward port 666 traffic to the computer with IP address 192.168.1.34. In this example, port 666 traffic is forwarded through the pppoe_0_0_33/ppp1 WAN interface. Click **Apply**.



☑ Active	
Service Name	Doom
WAN Interface	pppoe_0_0_33/ppp1
External Start Port	666
External End Port	666
Internal Start Port	666
Internel End Port	666
Server IP Address	192.168.1.34
Protocol	TCP

4 The port forwarding settings you configured are listed in the **Port Forwarding** screen.



Port Forwarding | DMZ Host | ALG

Port Forwarding

Service Name: WWW
WAN Interface: CONECTIVIDAD/ppp0.1
Server IP Address: 192.168.1.
External port Start: 80 End: 80
Internal port Start: 80 End: 80
Protocol: 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	☑	Doom	ppp1	666	666	666	666	192.168.1.34	

Apply Cancel

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

2.10 How to Use ATM QoS with Multiple PVCs

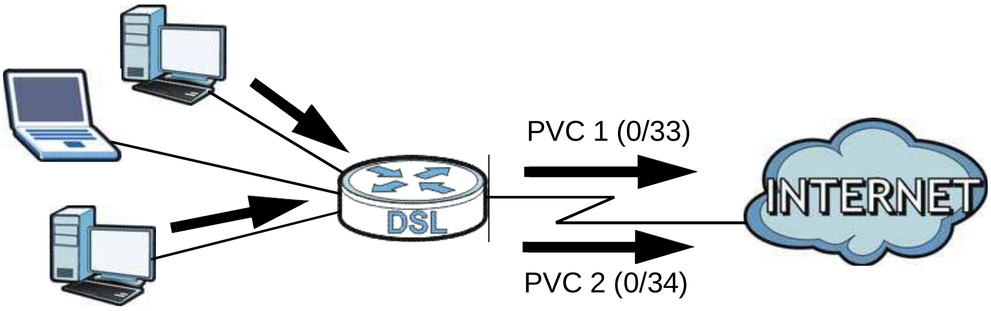
Note: Voice traffic will not be affected by the user-defined QoS settings on the Device. It always gets the highest priority.

The Device allows you to have more than one PVC using the ATM layer-2 interface. You can apply different ATM QoS settings to traffic through different PVCs. In this example, real-time or video service, such as using a webcam to send photos or uploading media content to share videos and images on a blog, is forwarded out through PVC 1 (0/33). Non-time sensitive data transfers, such as e-mail or FTP, are forwarded out through PVC 2 (0/34). The maximum upstream transmission speed of your ADSL port is 1 Mbps. You want to give the real-time traffic fixed bandwidth 400 Kbps and higher priority over the general data transmission which shares the bandwidth 600 Kbps.

Table 3 ATM QoS and PVC Settings

TRAFFIC TYPE	PVC	ATM QOS	BANDWIDTH
Real-time or video service	atm1 (0/33)	CBR	400 Kbps
Non-time sensitive data	atm2 (0/34)	Non Realtime VBR	600 Kbps

Note: To apply different QoS priorities to different applications over a PVC, use the **Advanced > QoS** screens. The packet-level QoS feature is not applicable to a PVC with CBR or Realtime VBR enabled.



2.10.1 Configuring PVCs

Follows the steps below to set up two PVCs on the Device.

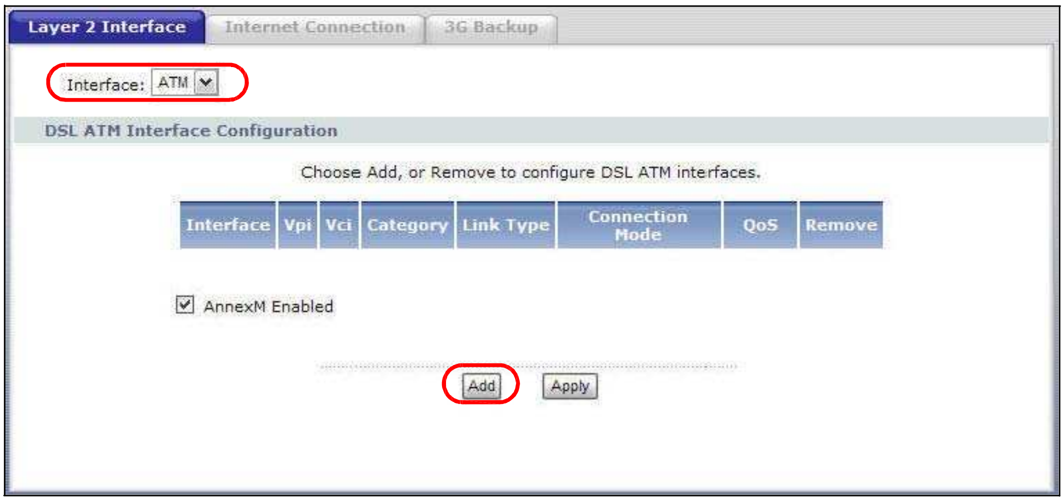
Table 4 Multiple PVC Settings

PVC	LAYER-2 INTERFACE	WAN SERVICE
0/33	atm0	PPPoE (pppoe_0_0_33)
0/34	atm1	IPoE (ipoe_0_0_34)

Note: Make sure you set the **DSL/WAN** switch (on the back of the Device) to the **DSL** side.

1 Click **Network > WAN** > **Layer 2 Interface**.

2 Select **ATM** from the **Interface** drop-down list and click **Add**.

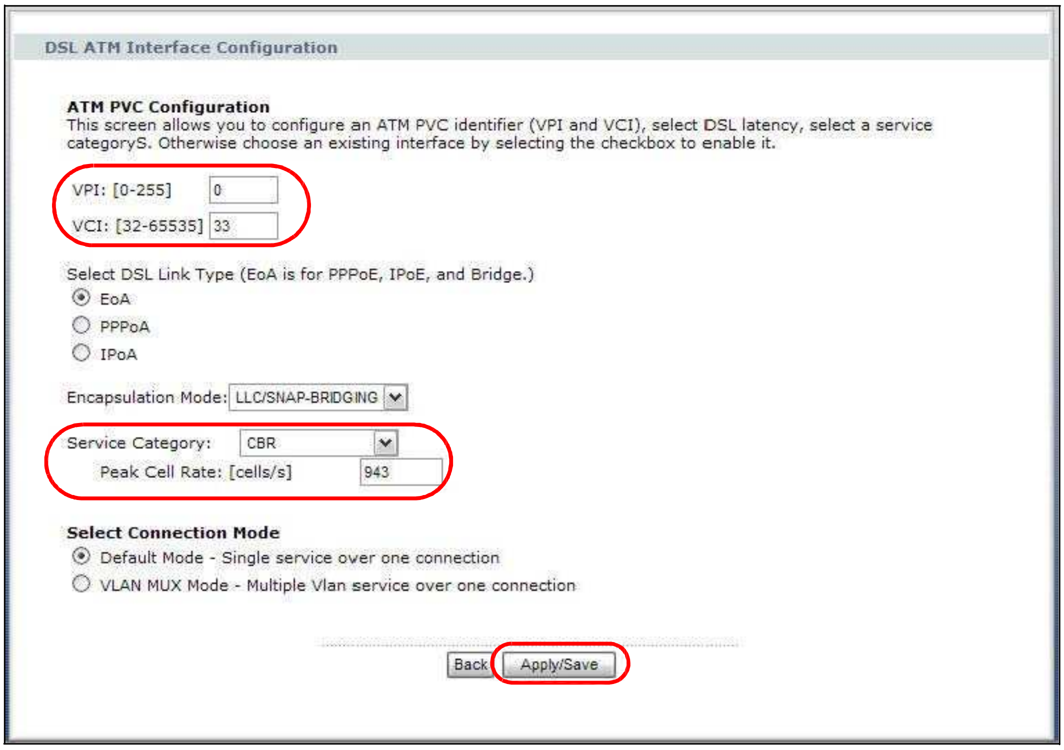


Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	Category	Link Type	Connection Mode	QoS	Remove

☑ AnnexM Enabled

3 Enter the VPI and VCI values (**0** and **33** in this example) for PVC 1.
Select **CBR** in the **Service Category** field and set the **Peak Cell Rate** as **943** (divide the bandwidth 400000 bps by 424). Click **Apply/Save** to save the changes and go back to the **Layer 2 Interface** screen.



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] 33

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

Encapsulation Mode: LLC/SNAP-BRIDGING

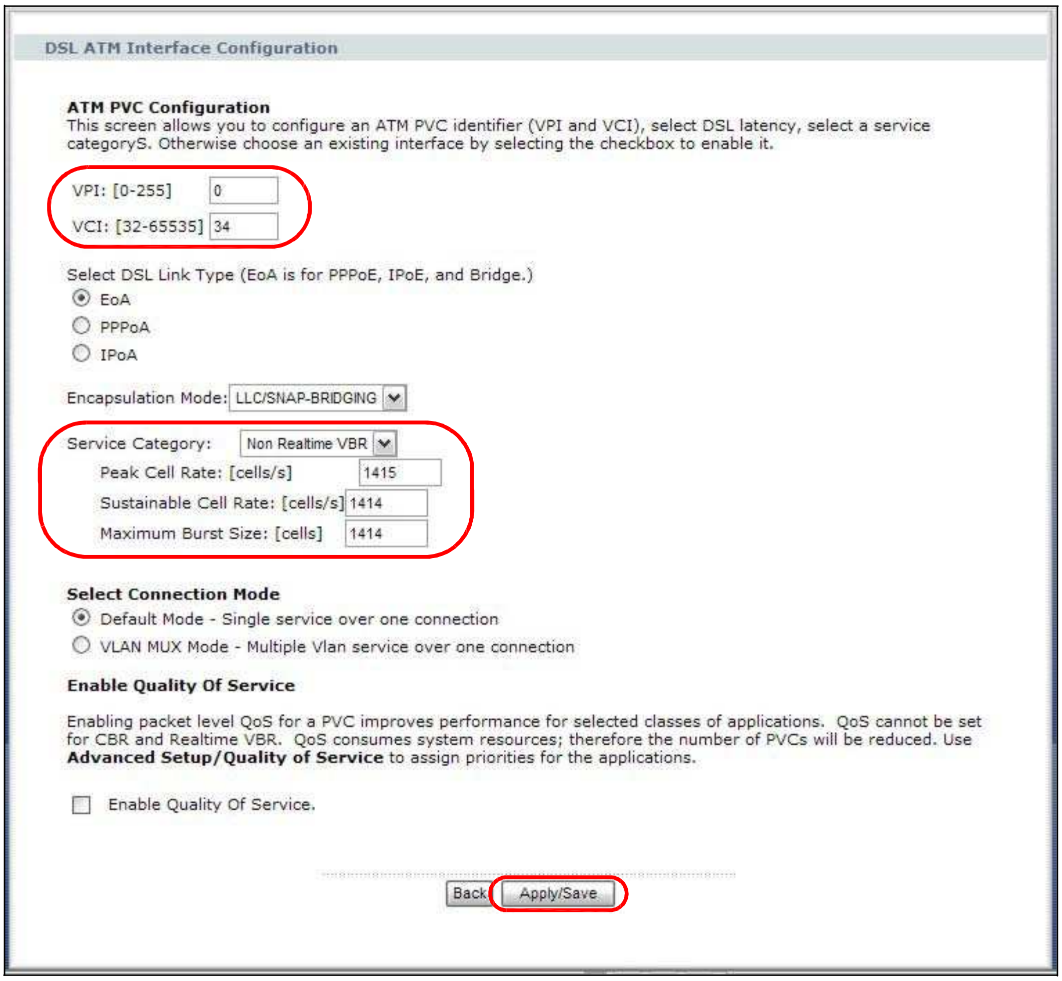
Service Category: CBR
Peak Cell Rate: [cells/s] 943

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

4 Click **Add** to configure another PVC.

5 Enter the VPI and VCI values (**0** and **34** in this example) for PVC 2.
Select **Non Realtime VBR** in the **Service Category** field. Set the **Peak Cell Rate** as **1415** (divide the bandwidth 600000 bps by 424) and set both the **Sustainable Cell Rate** and **Maximum Burst Size** as **1414** (which is less than the peak cell rate).

6 Click **Apply/Save** to save the changes and go back to the **Layer 2 Interface** screen.



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] 34

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

● EoA

○ PPPoA

○ IPoA

Encapsulation Mode: LLC/SNAP-BRIDGING

Service Category: Non Realtime VBR

Peak Cell Rate: [cells/s] 1415

Sustainable Cell Rate: [cells/s] 1414

Maximum Burst Size: [cells] 1414

Select Connection Mode

● Default Mode - Single service over one connection

○ VLAN MUX Mode - Multiple Vlan service over one connection

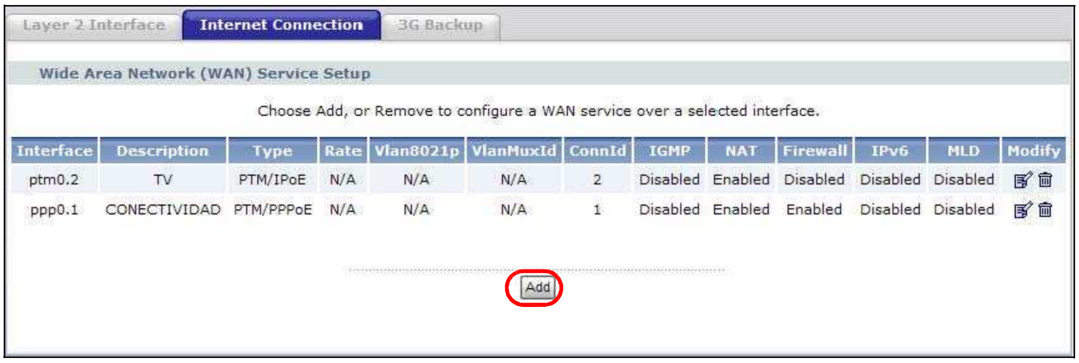
Enable Quality Of Service

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.

2.10.1.1 Internet Connection Settings for PVC 1

1 Click **Network > WAN** > **Internet Connection** to configure WAN connection settings for PVC 1. Click **Add**.

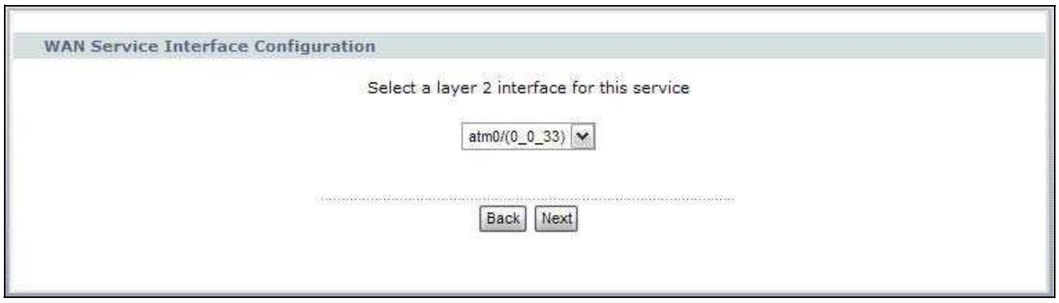


Wide Area Network (WAN) Service Setup

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

Interface	Description	Type	Rate	Vlan8021p	VlanMuxId	ConnId	IGMP	NAT	Firewall	IPv6	MLD	Modify
ptm0.2	TV	PTM/IPoE	N/A	N/A	N/A	2	Disabled	Enabled	Disabled	Disabled	Disabled	
ppp0.1	CONECTIVIDAD	PTM/PPPoE	N/A	N/A	N/A	1	Disabled	Enabled	Enabled	Disabled	Disabled	

2 Select PVC 1 (**atm0/0_0_33**) as the layer-2 interface. Click **Next**.

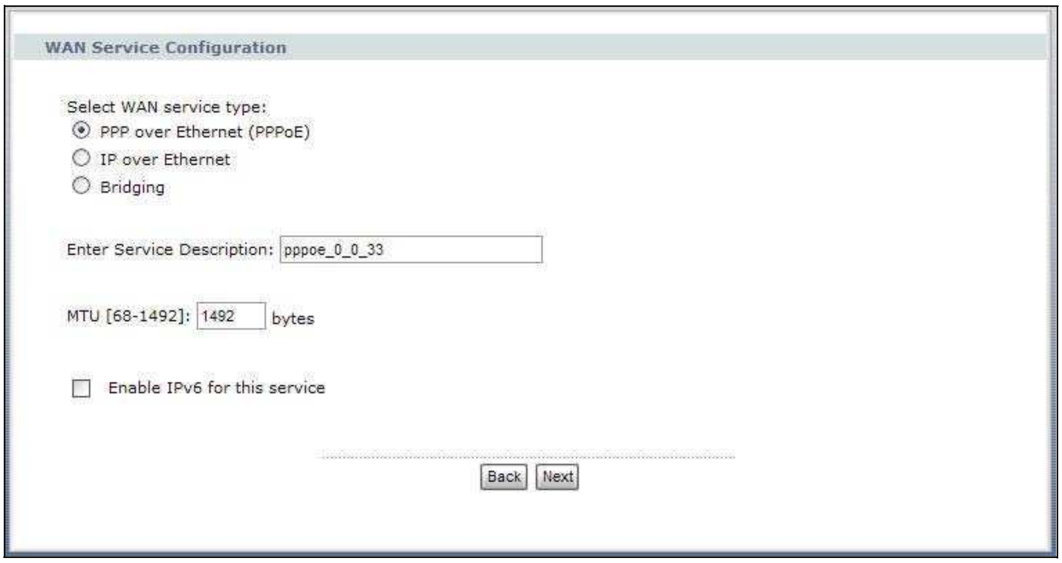


WAN Service Interface Configuration

Select a layer 2 interface for this service

atm0/(0_0_33)

3 Select **PPP over Ethernet** and click **Next**.



WAN Service Configuration

Select WAN service type:

● PPP over Ethernet (PPPoE)

○ IP over Ethernet

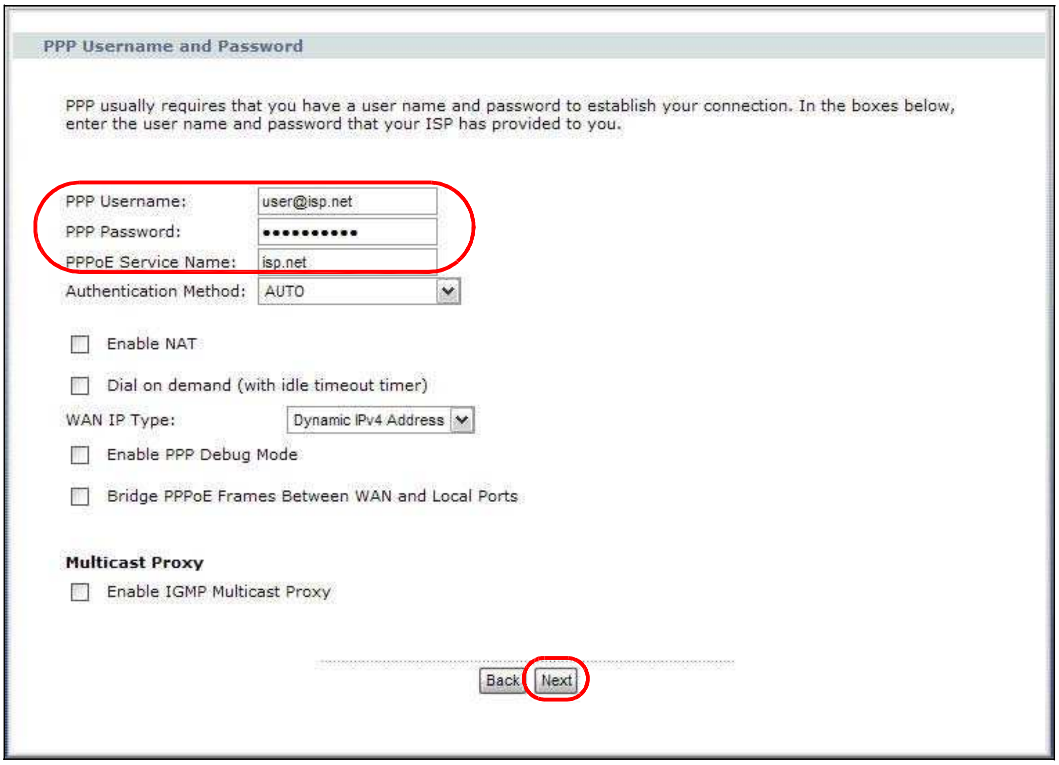
○ Bridging

Enter Service Description: pppoe_0_0_33

MTU [68-1492]: 1492 bytes

□ Enable IPv6 for this service

4 Enter the user name (**user@isp.net** for example), password (**qwert12345** for example) and service name (**isp.net** for example) for the PPP connection. Click **Next**.



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: user@isp.net
PPP Password: ●●●●●●●●●●●
PPPoE Service Name: isp.net
Authentication Method: AUTO

□ Enable NAT

□ Dial on demand (with idle timeout timer)

WAN IP Type: Dynamic IPv4 Address

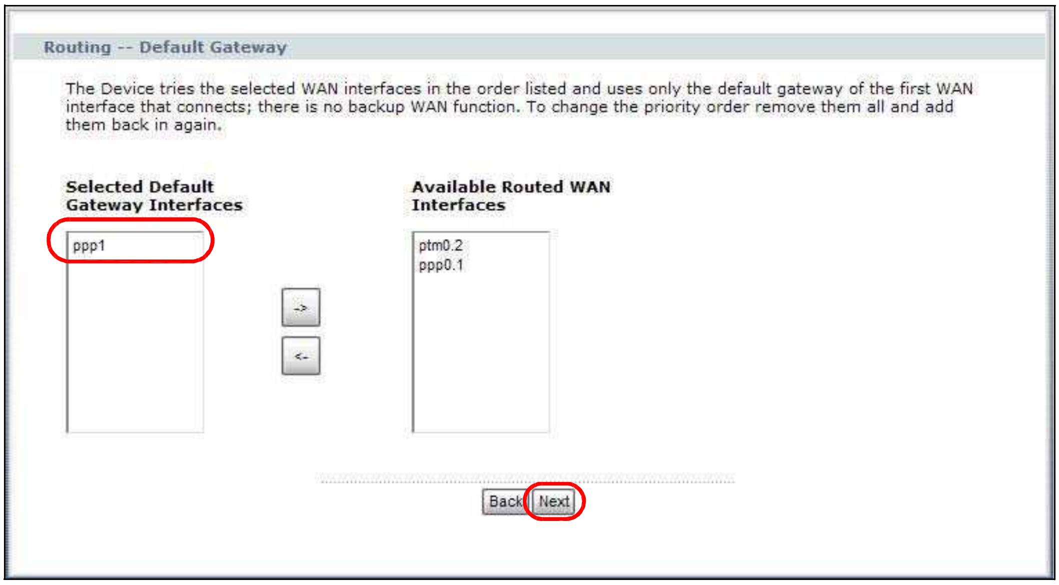
□ Enable PPP Debug Mode

□ Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

□ Enable IGMP Multicast Proxy

5 Remove the existing interfaces in the **Selected Default Gateway Interfaces** list. Select and move a WAN interface (**ppp1** in this example) to the **Selected Default Gateway Interfaces** list to use that interface as the default gateway. Click **Next**.



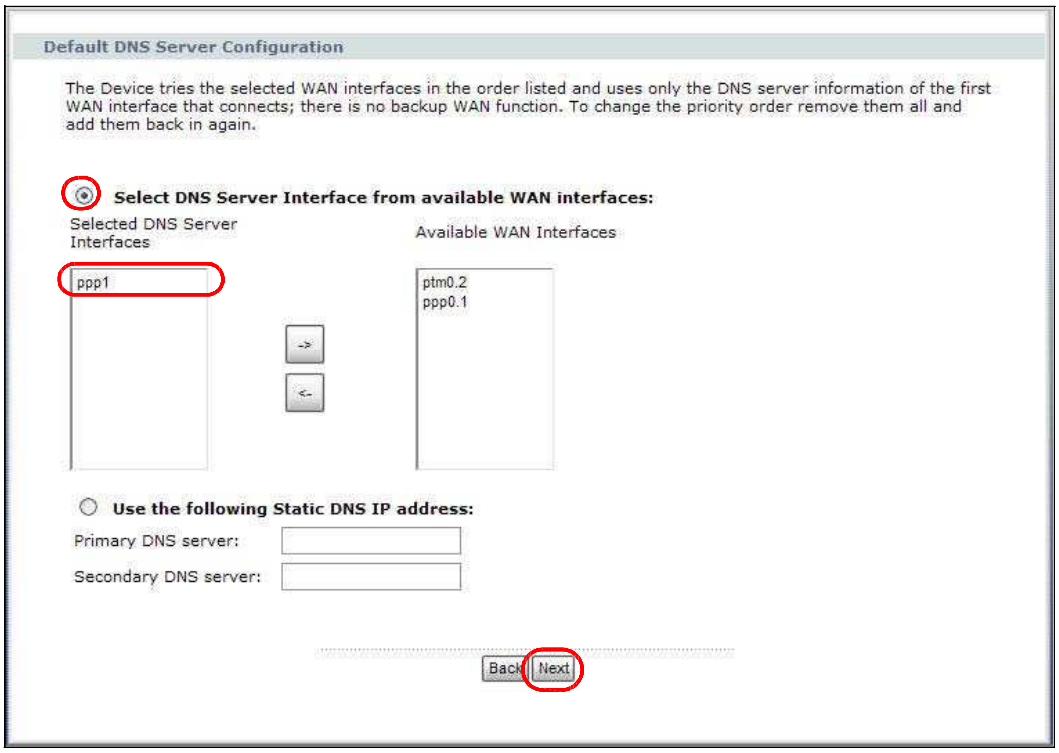
Routing -- Default Gateway

The Device tries the selected WAN interfaces in the order listed and uses only the default gateway of the first WAN interface that connects; there is no backup WAN function. To change the priority order remove them all and add them back in again.

Selected Default Gateway Interfaces: ppp1

Available Routed WAN Interfaces: ptm0.2, ppp0.1

6 Select the first option. Remove the existing interfaces in the **Selected DNS Server Interfaces** list. Select and move a WAN interface (**ppp1** in this example) to the **Selected DNS Server Interfaces** list to use that interface as the system DNS server. Click **Next**.



Default DNS Server Configuration

The Device tries the selected WAN interfaces in the order listed and uses only the DNS server information of the first WAN interface that connects; there is no backup WAN function. To change the priority order remove them all and add them back in again.

● Select DNS Server Interface from available WAN interfaces:

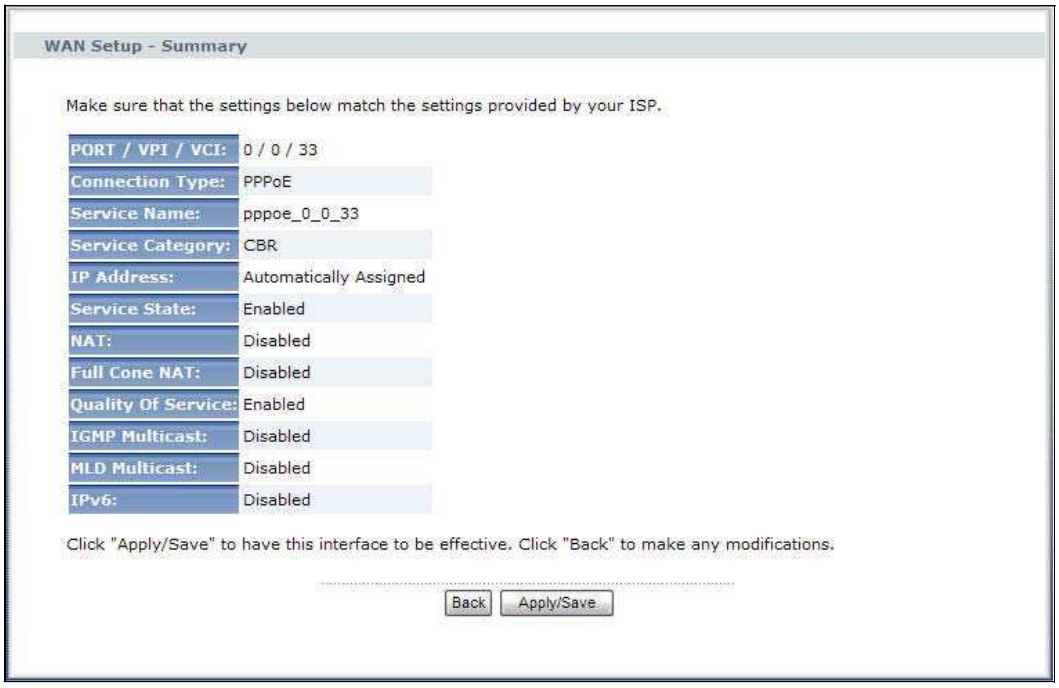
Selected DNS Server Interfaces	Available WAN Interfaces
ppp1	ptm0.2 ppp0.1

○ Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

7 The summary screen displays. Click **Apply/Save** to save your changes and go back to the **Internet Connection** screen.



WAN Setup - Summary

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

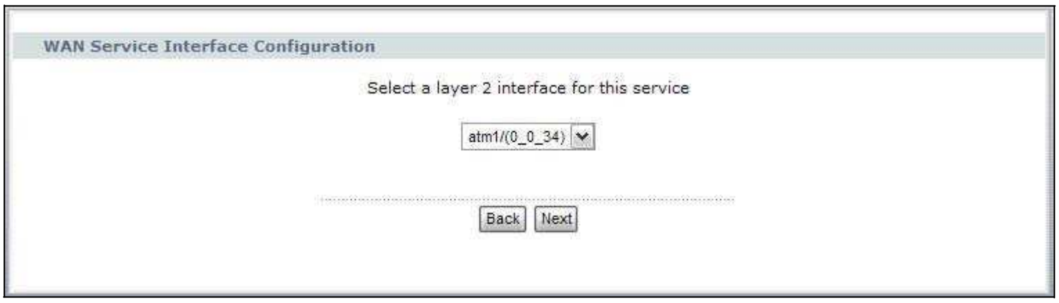
PORT / VPI / VCI:	0 / 0 / 33
Connection Type:	PPPoE
Service Name:	pppoe_0_0_33
Service Category:	CBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Disabled
Full Cone NAT:	Disabled
Quality Of Service:	Enabled
IGMP Multicast:	Disabled
MLD Multicast:	Disabled
IPv6:	Disabled

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

2.10.1.2 Internet Connection Settings for PVC 2

1 Click **Add** in the **WAN > Internet Connection** screen to configure WAN connection settings for PVC 2.

2 Select PVC 2 (**atm1/0_0_34**) as the layer-2 interface. Click **Next**.

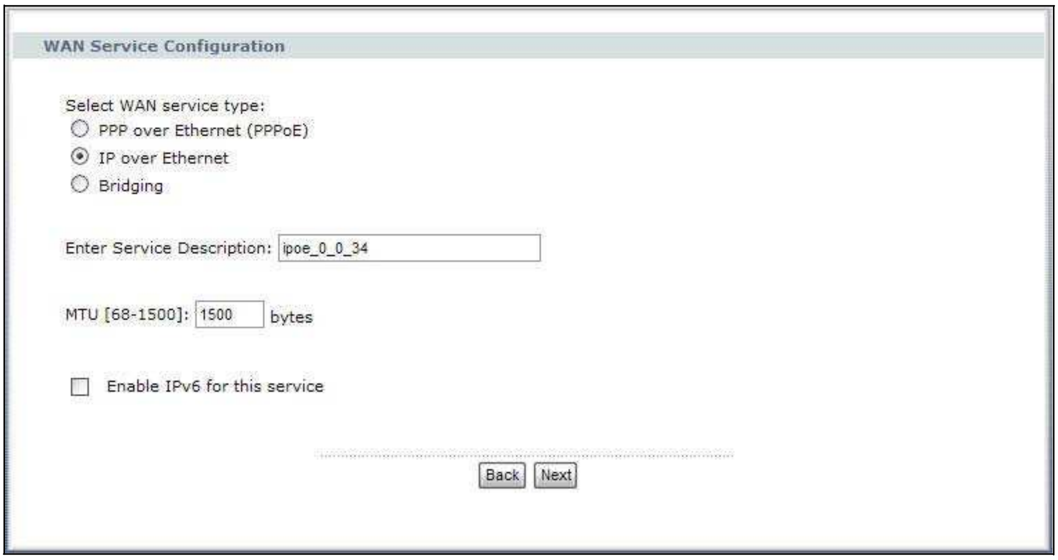


WAN Service Interface Configuration

Select a layer 2 interface for this service

atm1/(0_0_34)

3 Select **IP over Ethernet** and click **Next**.



WAN Service Configuration

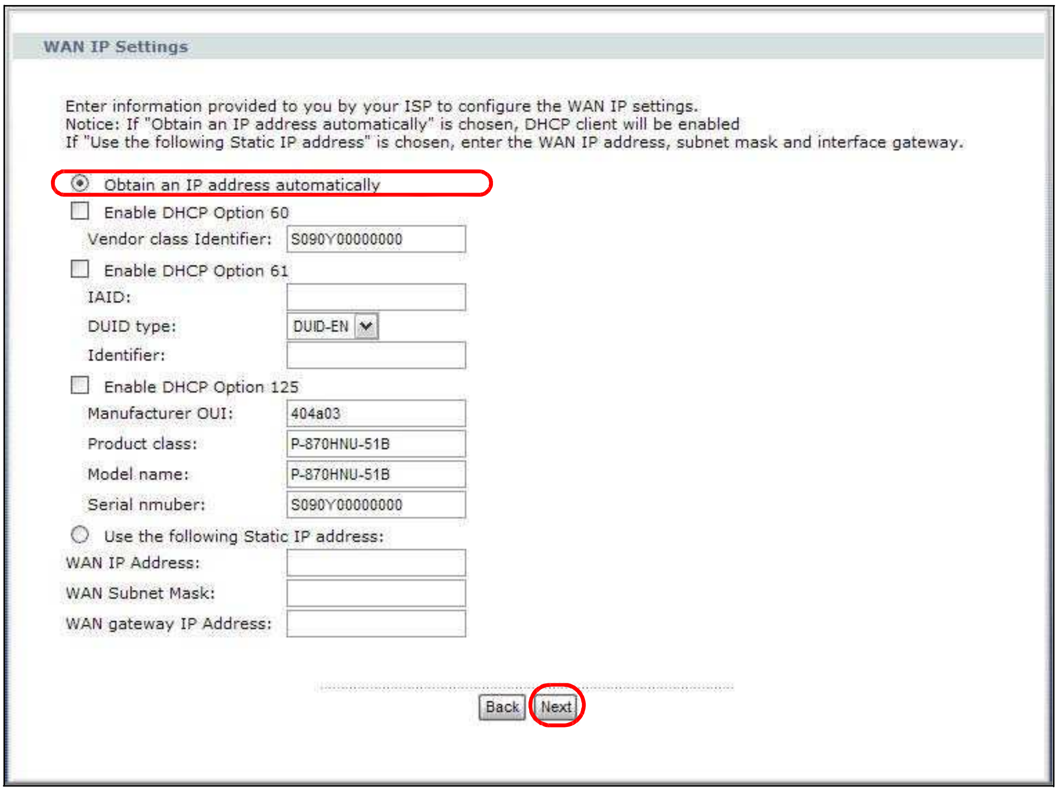
Select WAN service type:
○ PPP over Ethernet (PPPoE)
● IP over Ethernet
○ Bridging

Enter Service Description: ipoe_0_0_34

MTU [68-1500]: 1500 bytes

□ Enable IPv6 for this service

4 Select **Obtain an IP address automatically** and click **Next**.



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: S090Y00000000

□ Enable DHCP Option 61

IAID:

DUID type: DUID-EN

Identifier:

□ Enable DHCP Option 125

Manufacturer OUI: 404a03

Product class: P-870HNU-51B

Model name: P-870HNU-51B

Serial nmuber: S090Y00000000

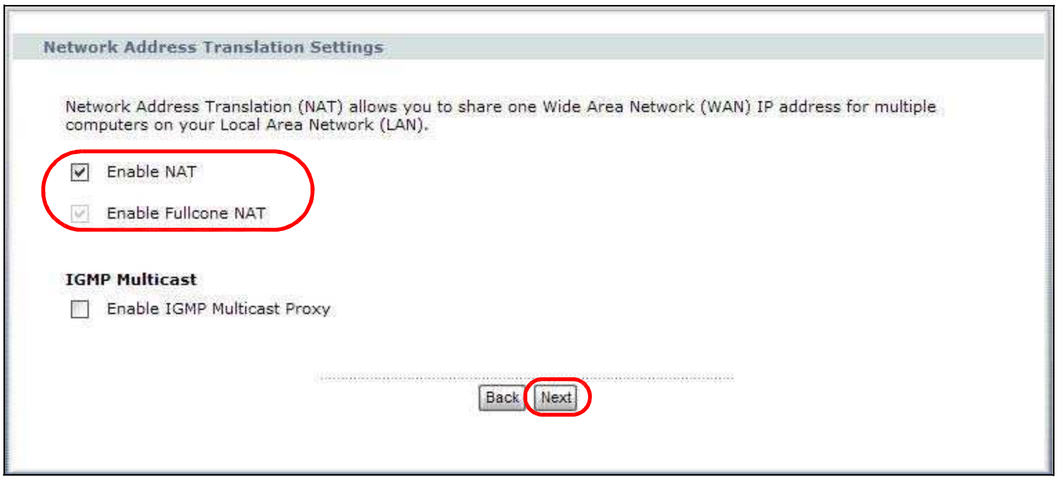
○ Use the following Static IP address:

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

5 Select **Enable NAT**, then click **Next**.



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).

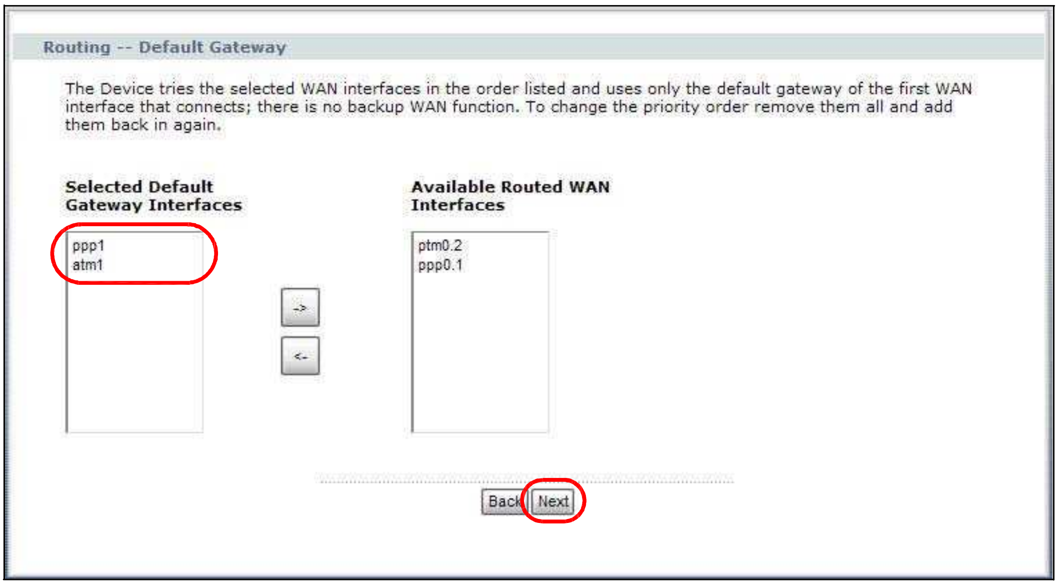
☑ Enable NAT

☑ Enable Fullcone NAT

IGMP Multicast

□ Enable IGMP Multicast Proxy

6 Select and move the WAN interface (**atm1** in this example) to the **Selected Default Gateway Interfaces** list to use that interface as the default gateway. Click **Next**.

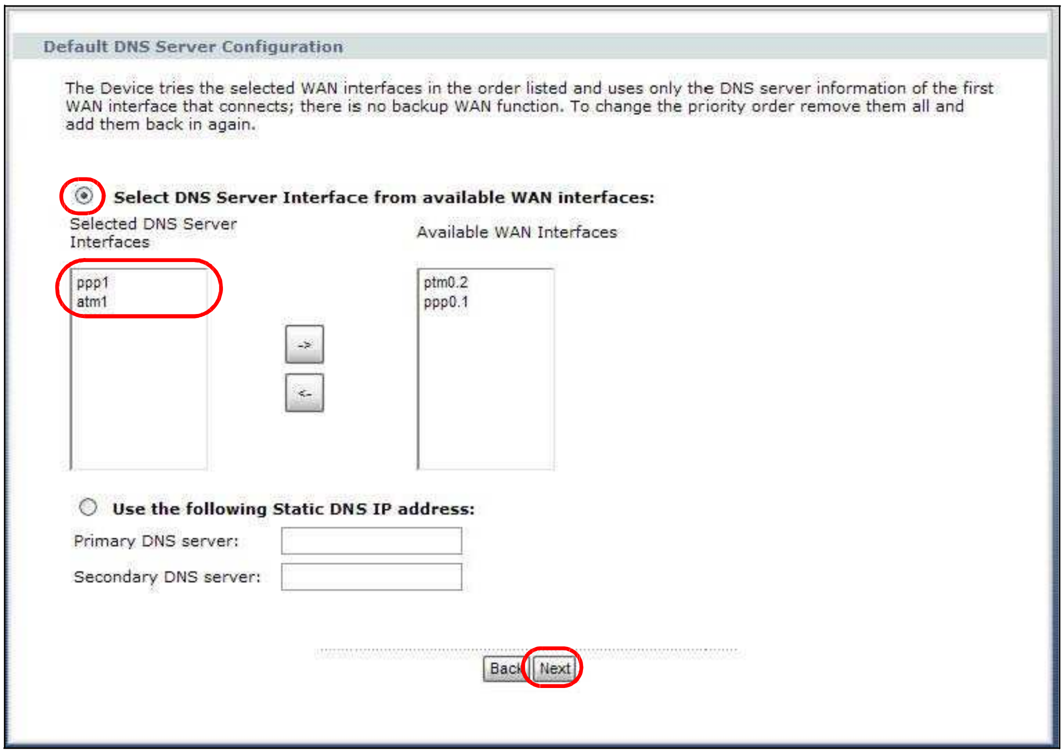


Routing -- Default Gateway

The Device tries the selected WAN interfaces in the order listed and uses only the default gateway of the first WAN interface that connects; there is no backup WAN function. To change the priority order remove them all and add them back in again.

Selected Default Gateway Interfaces		Available Routed WAN Interfaces
ppp1 atm1	-> <-	ptm0.2 ppp0.1

7 Select the first option. Select and move the WAN interface (**atm1** in this example) to the **Selected DNS Server Interfaces** list to use that interface as the system DNS server. Click **Next**.



Default DNS Server Configuration

The Device tries the selected WAN interfaces in the order listed and uses only the DNS server information of the first WAN interface that connects; there is no backup WAN function. To change the priority order remove them all and add them back in again.

● Select DNS Server Interface from available WAN interfaces:

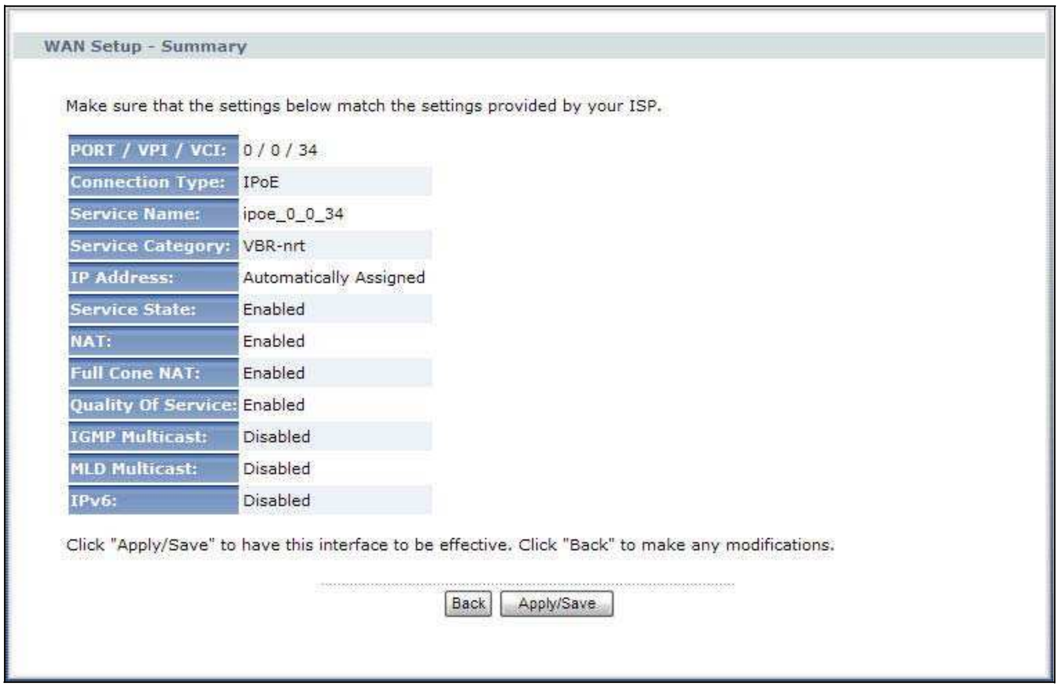
Selected DNS Server Interfaces		Available WAN Interfaces
ppp1 atm1	-> <-	ptm0.2 ppp0.1

○ Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

8 The summary screen displays. Click **Apply/Save** to save your changes and go back to the **Internet Connection** screen.



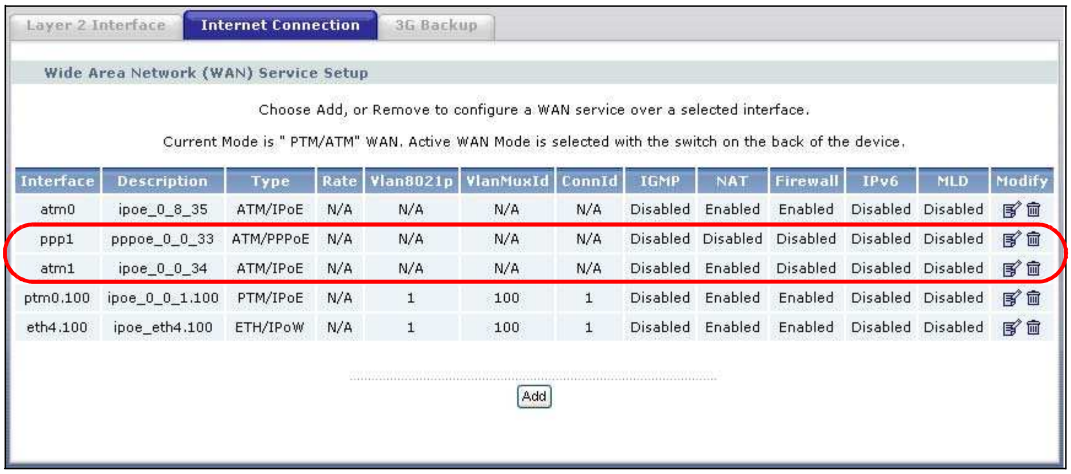
WAN Setup - Summary

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

PORT / VPI / VCI:	0 / 0 / 34
Connection Type:	IPoE
Service Name:	ipoe_0_0_34
Service Category:	VBR-nrt
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Full Cone NAT:	Enabled
Quality Of Service:	Enabled
IGMP Multicast:	Disabled
MLD Multicast:	Disabled
IPv6:	Disabled

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

9 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.

Current Mode is " PTM/ATM" WAN. Active WAN Mode is selected with the switch on the back of the device.

Interface	Description	Type	Rate	Vlan8021p	VlanMuxId	ConnId	IGMP	NAT	Firewall	IPv6	MLD	Modify
atm0	ipoe_0_8_35	ATM/IPoE	N/A	N/A	N/A	N/A	Disabled	Enabled	Enabled	Disabled	Disabled	✎ 🗑
ppp1	pppoe_0_0_33	ATM/PPPoE	N/A	N/A	N/A	N/A	Disabled	Disabled	Disabled	Disabled	Disabled	✎ 🗑
atm1	ipoe_0_0_34	ATM/IPoE	N/A	N/A	N/A	N/A	Disabled	Enabled	Disabled	Disabled	Disabled	✎ 🗑
ptm0.100	ipoe_0_0_1.100	PTM/IPoE	N/A	1	100	1	Disabled	Enabled	Enabled	Disabled	Disabled	✎ 🗑
eth4.100	ipoe_eth4.100	ETH/IPoW	N/A	1	100	1	Disabled	Enabled	Enabled	Disabled	Disabled	✎ 🗑

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 Firefox 2.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

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

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

See Appendix A on page 261 if you need to make sure these functions are allowed in Internet Explorer.

3.1.1 Accessing the Web Configurator

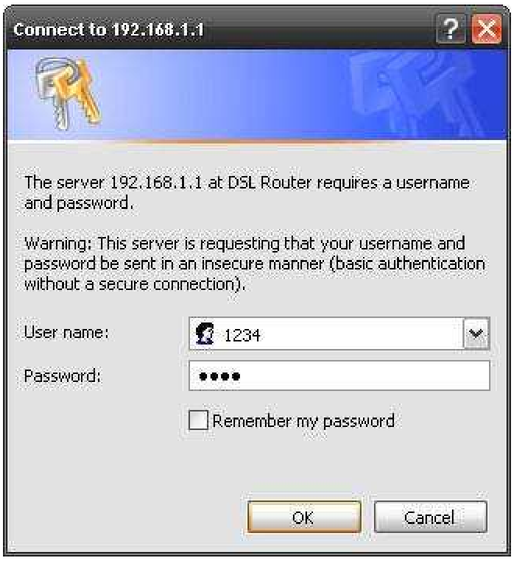
1 Make sure your Device hardware is properly connected (refer to the Quick Start Guide).

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 **1234** and default admin password **1234**. 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 4 Password Screen



The server 192.168.1.1 at DSL Router requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name: 1234

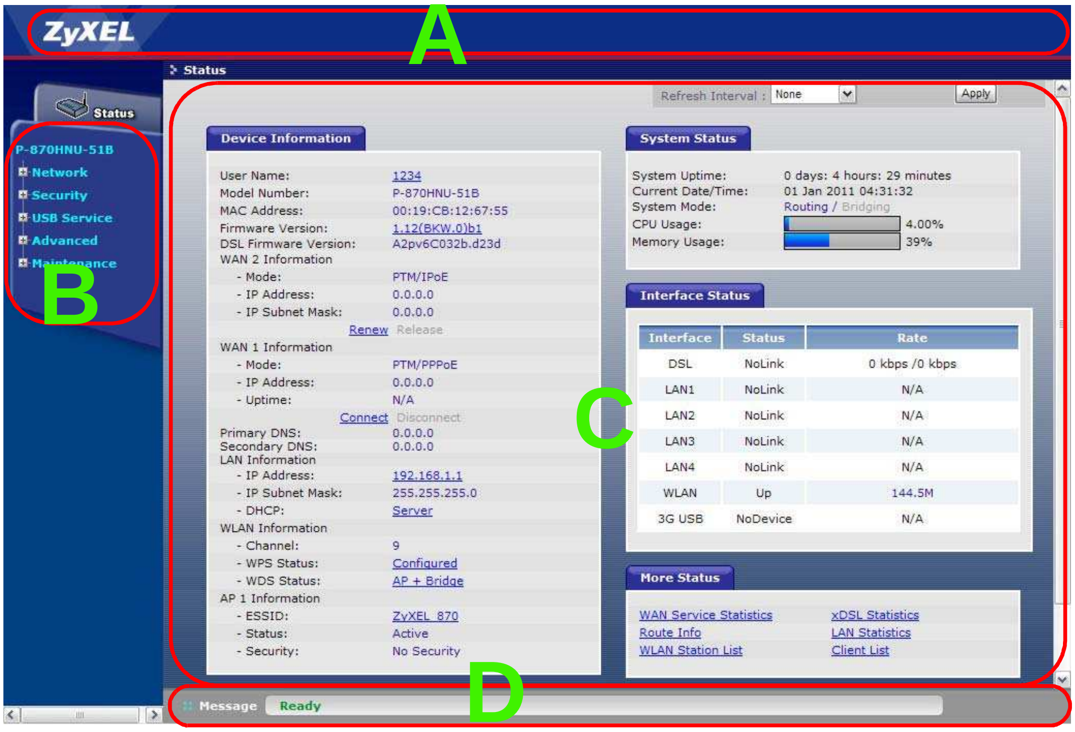
Password: ••••

□ 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 Device models.

Figure 5 Main Screen



User Name: 1234
Model Number: P-870HNU-51B
MAC Address: 00:19:CB:12:67:55
Firmware Version: 1.12(BKW.0)b1
DSL Firmware Version: A2pv6C032b.d23d
WAN 2 Information
- Mode: PTM/IPoE
- IP Address: 0.0.0.0
- IP Subnet Mask: 0.0.0.0
WAN 1 Information
- Mode: PTM/PPPoE
- IP Address: 0.0.0.0
- Uptime: N/A
Primary DNS: 0.0.0.0
Secondary DNS: 0.0.0.0
LAN Information
- IP Address: 192.168.1.1
- IP Subnet Mask: 255.255.255.0
- DHCP: Server
WLAN Information
- Channel: 9
- WPS Status: Configured
- WDS Status: AP + Bridge
AP 1 Information
- ESSID: ZyXEL_870
- Status: Active
- Security: No Security

System Uptime: 0 days: 4 hours: 29 minutes
Current Date/Time: 01 Jan 2011 04:31:32
System Mode: Routing / Bridging
CPU Usage: 4.00%
Memory Usage: 39%

Interface	Status	Rate
DSL	NoLink	0 kbps /0 kbps
LAN1	NoLink	N/A
LAN2	NoLink	N/A
LAN3	NoLink	N/A
LAN4	NoLink	N/A
WLAN	Up	144.5M
3G USB	NoDevice	N/A

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 Device features. The following tables describe each menu item.

Table 5 Navigation Panel Summary

LINK	TAB	FUNCTION
Status		This screen shows the 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 ATM or PTM (Packet Transfer Mode) interface.

Table 5 Navigation Panel Summary

LINK	TAB	FUNCTION
	Internet Connection	Use this screen to configure ISP parameters, WAN IP address assignment, and other advanced properties.
	3G Backup	Use this screen to configure the 3G WAN connection.
LAN	IP	Use this screen to configure LAN TCP/IP, DHCP and IP alias settings.
	DHCP Client List	Use this screen to look at the IP addresses currently assigned to DHCP clients and the IP addresses reserved for specific MAC addresses.
	IPv6	Use this screen to specify LAN IPv6 settings.
Wireless LAN	General	Use this screen to configure the wireless LAN settings, WLAN authentication/security settings and MAC filtering rules.
	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.
	Advanced Setup	Use this screen to configure the advanced wireless LAN settings.
NAT	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	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 Device.
Security		
Firewall	General	Use this screen to enable the firewall and configure the default policies.
	Rules	This screen shows a summary of the firewall rules, and allows you to add or remove a firewall rule.
USB Services		
File Sharing	Share Configuration	Use this screen to enable file sharing via the Device.
Print Server	Printer Configuration	Use this screen to enable the print server on the Device and get the model name of the associated printer.
Media Server	Media Server Configuration	Use this screen to use the Device as a media server.
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.
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.
	Policer Setup	Use this screen to configure QoS policers to limit the transmission rate of incoming traffic.
	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 Device to be managed by an ACS (Auto Configuration Server).
	IP Address	Use this screen to configure from which IP address(es) users can manage the Device.
UPnP	General	Use this screen to turn UPnP on or off.
Maintenance		

Table 5 Navigation Panel Summary

LINK	TAB	FUNCTION
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 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 Device's log settings.
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 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.
	OAM Ping Test	This screen displays information to help you identify problems with the DSL connection.

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 71 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.

PART II
Technical Reference

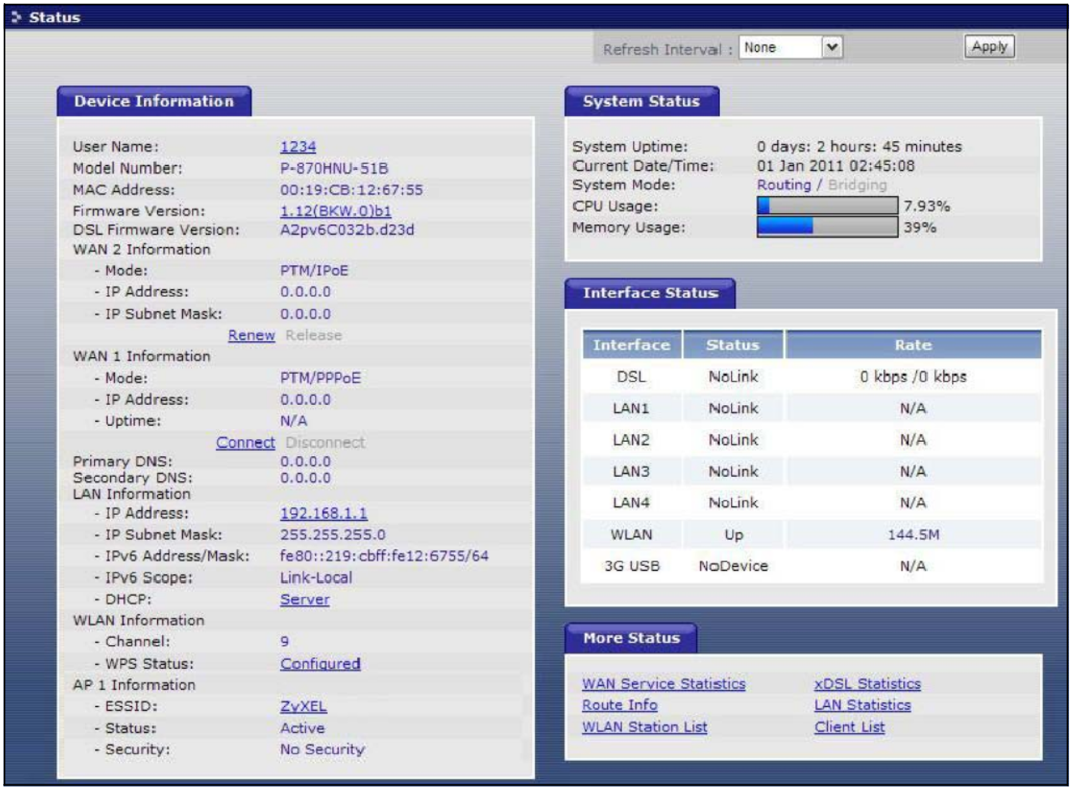
Status Screens

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 6 Status Screen



Device Information

User Name: 1234
Model Number: P-870HNU-51B
MAC Address: 00:19:CB:12:67:55
Firmware Version: 1.12(BKW.0)b1
DSL Firmware Version: A2pv6C032b.d23d
WAN 2 Information
- Mode: PTM/IPoE
- IP Address: 0.0.0.0
- IP Subnet Mask: 0.0.0.0
Renew Release
WAN 1 Information
- Mode: PTM/PPPoE
- IP Address: 0.0.0.0
- Uptime: N/A
Connect Disconnect
Primary DNS: 0.0.0.0
Secondary DNS: 0.0.0.0
LAN Information
- IP Address: 192.168.1.1
- IP Subnet Mask: 255.255.255.0
- IPv6 Address/Mask: fe80::219:cbff:fe12:6755/64
- IPv6 Scope: Link-Local
- DHCP: Server
WLAN Information
- Channel: 9
- WPS Status: Configured
AP 1 Information
- ESSID: ZyXEL
- Status: Active
- Security: No Security

System Status

System Uptime: 0 days: 2 hours: 45 minutes
Current Date/Time: 01 Jan 2011 02:45:08
System Mode: Routing / Bridging
CPU Usage: 7.93%
Memory Usage: 39%

Interface Status

Interface	Status	Rate
DSL	NoLink	0 kbps /0 kbps
LAN1	NoLink	N/A
LAN2	NoLink	N/A
LAN3	NoLink	N/A
LAN4	NoLink	N/A
WLAN	Up	144.5M
3G USB	NoDevice	N/A

More Status

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

Each field is described in the following table.

Table 6 Status Screen

LABEL	DESCRIPTION
Refresh Interval	Enter how often you want the Device to update this screen.
Apply	Click this to update this screen immediately.

Table 6 Status Screen

LABEL	DESCRIPTION
Device Information	
User Name	This field displays the 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 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 x Information	
Mode	This is the method of encapsulation used by your ISP.
IP Address	This field displays the current IP address of the Device in the WAN.
IP Subnet Mask	This field displays the current subnet mask in the WAN.
Primary DNS	This field displays the primary DNS server for the WAN.
Secondary DNS	This field displays the secondary DNS server for the WAN.
LAN Information	
IP Address	This field displays the current IP address of the 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.
IPv6 Address/ Mask	This field displays the current IPv6 address and prefix length for the Device's LAN interface. This field is available only when you enable IPv6 for the LAN connection.
IPv6 Scope	This field displays whether the IPv6 address is a link-local or global address. This field is available only when you enable IPv6 for the LAN connection.
DHCP	This field displays what DHCP services the Device is providing to the LAN. Choices are: **Server** - The Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. **Relay** - The Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. **None** - The 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 Device now.
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.
AP 1 Information	
ESSID	This is the descriptive name used to identify the 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.

Table 6 Status Screen

LABEL	DESCRIPTION
Security	This shows the level of wireless security the Device is using in this wireless network.
System Status	
System Uptime	This field displays how long the Device has been running since it last started up. The 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 22).
Current Date/ Time	This field displays the current date and time in the Device. You can change this in **Maintenance > System > Time Setting**.
System Mode	This displays whether the Device is functioning as a router or a bridge.
CPU Usage	This field displays what percentage of the Device’s processing ability is currently used. When this percentage is close to 100%, the 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 15 on page 191).
Memory Usage	This field displays what percentage of the Device’s memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100%, the Device is probably becoming unstable, and you should restart the device. See Section 21.4 on page 241, or turn off the device (unplug the power) for a few seconds.
Interface Status	
Interface	This column displays each interface the Device has.
Status	This field indicates whether or not the Device is using the interface. For the DSL interface, this field displays **LinkDown** (line is down), **NoLink** (line is disconnected) or **Up** (line is up or connected). For the LAN interface, this field displays **Up** when the 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. For the 3G WAN interface, it displays: • **NoDevice** when no 3G card is inserted, • **Disabled** when the 3G WAN is not activated, • **Up** when the 3G connection is up, • **Down** when the 3G connection is down, • **NoResponse** when there is no response from the inserted 3G card, • **InvalidPIN** if the PIN code you entered in the **WAN > 3G Backup** screen is not the right one for the 3G card you inserted, • **NeedPUK** if you enter the PIN (Personal Identification Number) code incorrectly for three times and the SIM card is blocked by your ISP, • **DialFail** when the Device fails to dial up a 3G connection. • or **InvalidSIM** when the SIM card is damaged or not inserted. If a link displays in this field, click the link to view more status information or enter the correct PIN or PUK (Personal Unblocking Key) code.
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. For the 3G WAN interface, it displays the downstream and upstream transmission rate.
More Status	

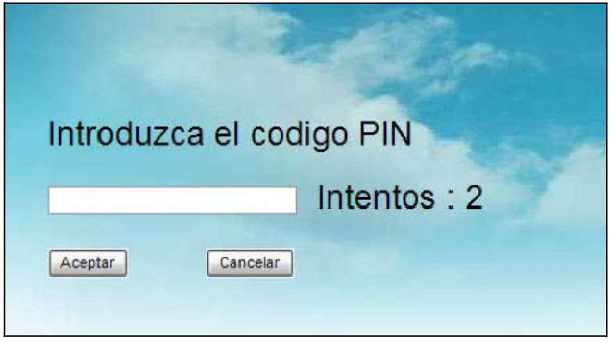
Table 6 Status Screen

LABEL	DESCRIPTION
WAN Service Statistics	Click this link to view packet specific statistics of the WAN connection(s). See Section 4.1.3 on page 76.
Route Info	Click this link to view the internal routing table on the Device. See Section 4.1.4 on page 77.
WLAN Station List	Click this link to display the MAC address(es) of the wireless stations that are currently associating with the Device. See Section 4.1.5 on page 78.
xDSL Statistics	Click this link to view detailed DSL statistics. See Section 4.1.6 on page 80.
LAN Statistics	Click this link to view packet specific statistics on the LAN and WLAN interfaces. See Section 4.1.7 on page 82.
Client List	Click this link to view current DHCP client information. See Section 4.1.8 on page 83.

4.1.1 3G Status: InvalidPIN

Click the **InvalidPIN** link under **Interface Status** of the **Status** screen to access this screen. Use this screen to enter the right PIN code for your 3G card.

Figure 7 Status > InvalidPIN



Introduzca el codigo PIN

Intentos : 2

The following table describes the labels in this screen.

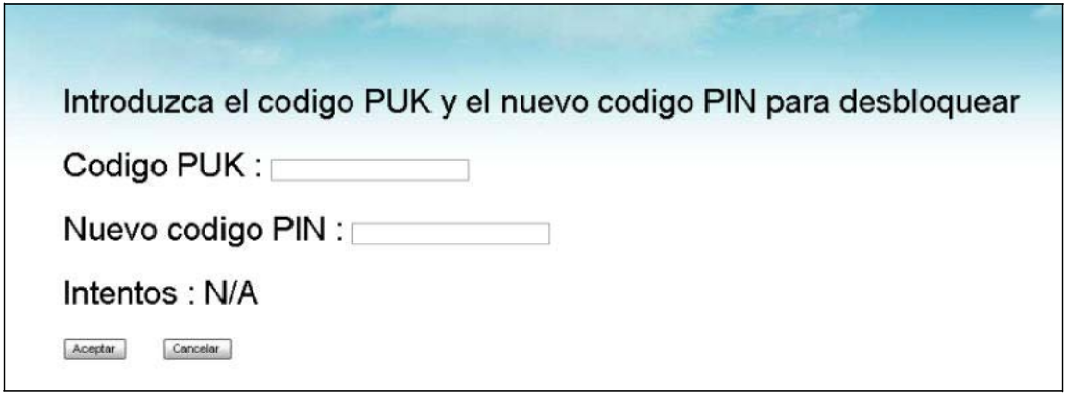
Table 7 Status > Need PIN

LABEL	DESCRIPTION
(Introduzca el código PIN) Enter PIN code again	Enter the correct PIN code (four to eight digits) for the inserted 3G card.
Intentos (Attempts)	This field displays how many times you can still enter a wrong PIN code before your ISP blocks your SIM card.
Aceptar (Accept)	Click **Aceptar** to save the correct PIN code.
Cancelar (Cancel)	Click **Cancelar** to return to the previous configuration.

4.1.2 3G Status: NeedPUK

Click the **NeedPUK** link under **Interface Status** of the **Status** screen to access this screen. Use this screen to enter the PUK code to enable the 3G SIM card again.

Figure 8 Status > NeedPUK



Introduzca el codigo PUK y el nuevo codigo PIN para desbloquear

Codigo PUK :

Nuevo codigo PIN :

Intentos : N/A

The following table describes the labels in this screen.

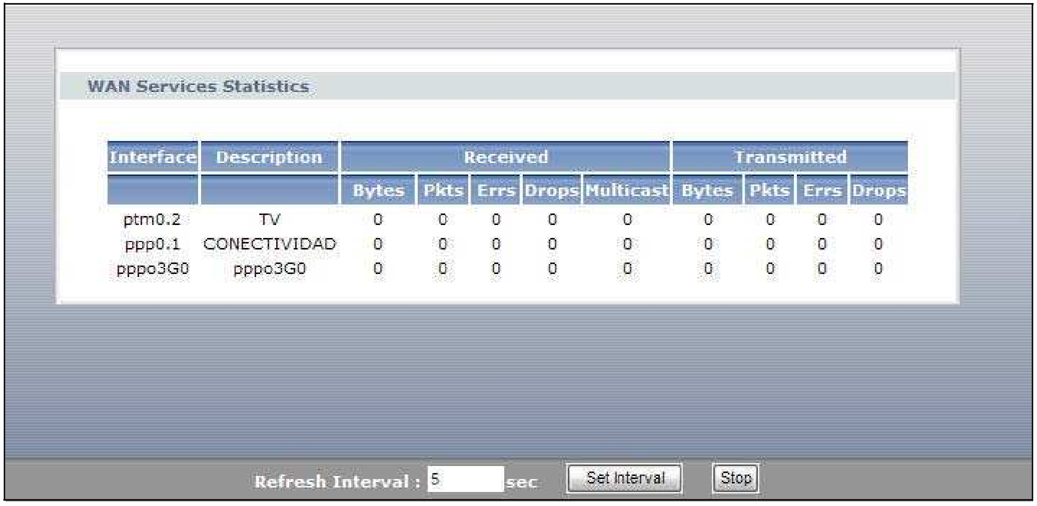
Table 8 Status > NeedPUK

LABEL	DESCRIPTION
(Codigo PUK) PUK code	If you enter the PIN code incorrectly three times, the SIM card will be blocked by your ISP and you cannot use the account to access the Internet. You should get the PUK (Personal Unblocking Key) code (four to eight digits) from your ISP. Enter the PUK code to enable the SIM card. If an incorrect PUK code is entered 10 times, the SIM card will be disabled permanently. You then need to contact your ISP for a new SIM card.
(Nuevo codigo PUK) New PIN code	Configure a PIN code for the SIM card. You can specify any four to eight digits to have a new PIN code or enter the previous PIN code.
Intentos (Attempts)	This field displays how many times you can still enter a wrong PUK code before your ISP disables your SIM card permanently.
Aceptar (Accept)	Click **Aceptar** to save your changes to the Device.
Cancelar (Cancel)	Click **Cancelar** to return to the previous configuration.

4.1.3 WAN Service Statistics

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

Figure 9 Status > WAN Service Statistics



WAN Services Statistics

Interface	Description	Received					Transmitted			
		Bytes	Pkts	Errs	Drops	Multicast	Bytes	Pkts	Errs	Drops
ptm0.2	TV	0	0	0	0	0	0	0	0	0
ppp0.1	CONECTIVIDAD	0	0	0	0	0	0	0	0	0
pppo3G0	pppo3G0	0	0	0	0	0	0	0	0	0

Refresh Interval : 5 sec

The following table describes the labels in this screen.

Table 9 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. **ppp*** 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.
Pkts	This indicates the number of packets received 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.
Multicast	This indicates the number of multicast packets received 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.

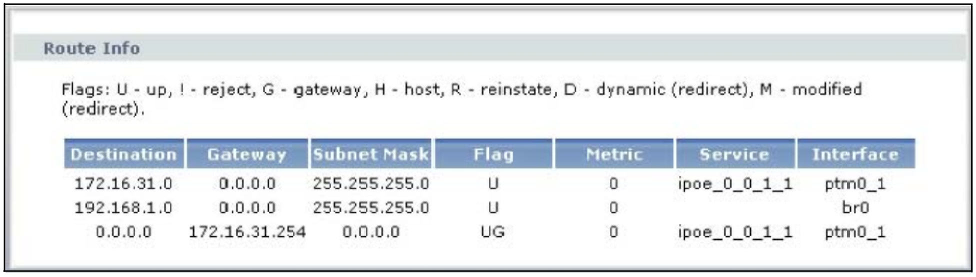
Table 9 Status > WAN Service Statistics (continued)

LABEL	DESCRIPTION
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.

4.1.4 Route Info

Routing is based on the destination address only and the 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 Device.

Figure 10 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 10 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.
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".

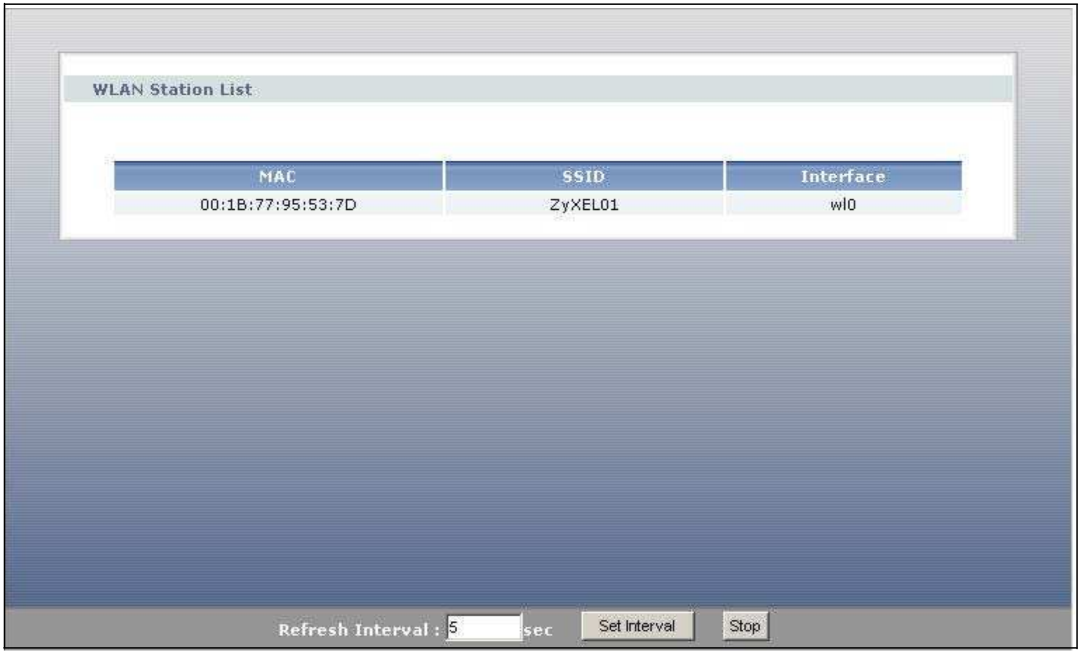
Table 10 Status > Route Info (continued)

LABEL	DESCRIPTION
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. • **ppp*** indicates the WAN interface using PPPoE. • **3G** indicates the 3G WAN interface.

4.1.5 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 Device.

Figure 11 Status > WLAN Station List



WLAN Station List

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

Refresh Interval : 5 sec

The following table describes the labels in this screen.

Table 11 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.

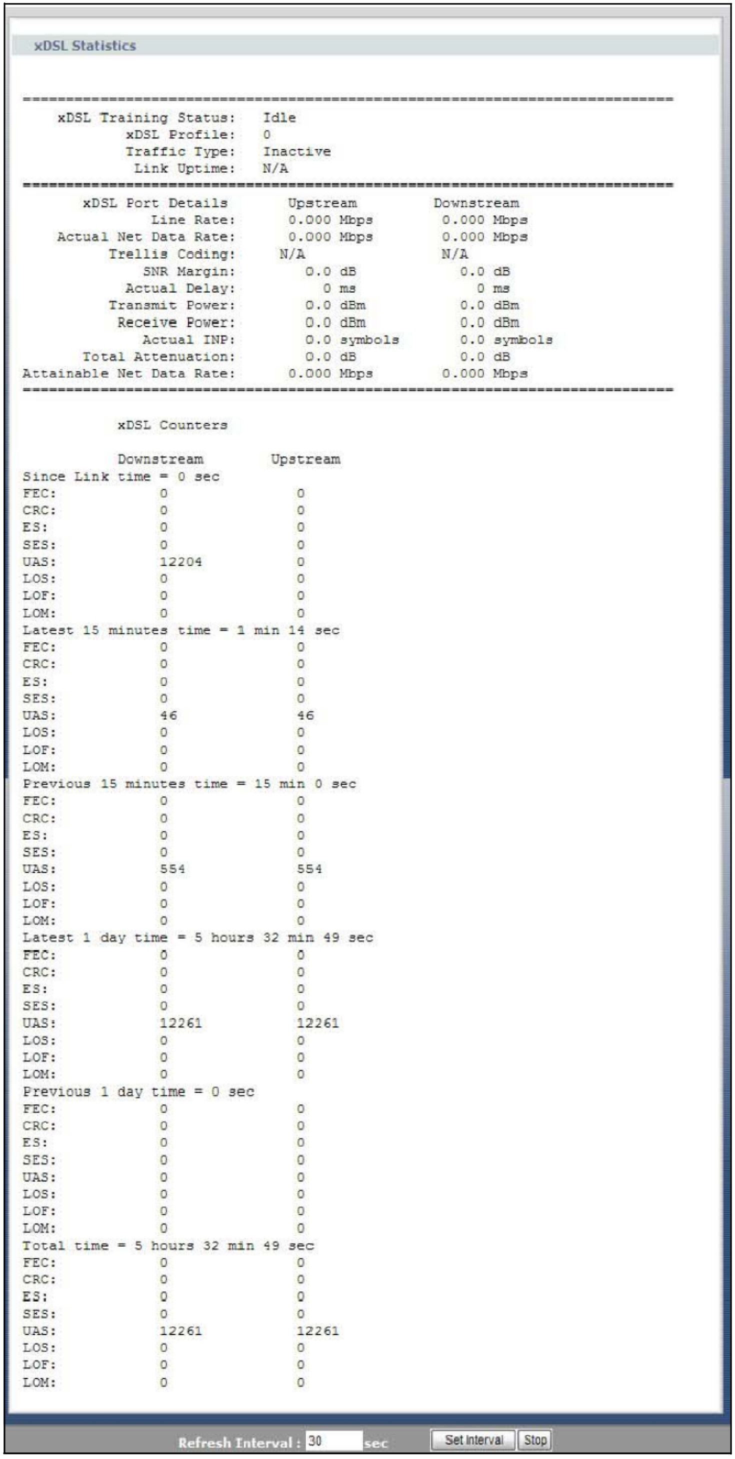
Table 11 Status > WLAN Station List (continued)

LABEL	DESCRIPTION
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.

4.1.6 xDSL Statistics

Click **Status > xDSL Statistics** to access this screen. Use this screen to view detailed DSL statistics.

Figure 12 Status > xDSL Statistics



xDSL Statistics

```
=============================================================================
    xDSL Training Status:   Idle
            xDSL Profile:   0
            Traffic Type:   Inactive
             Link Uptime:   N/A
=============================================================================
       xDSL Port Details       Upstream         Downstream
               Line Rate:      0.000 Mbps        0.000 Mbps
    Actual Net Data Rate:      0.000 Mbps        0.000 Mbps
          Trellis Coding:     N/A               N/A
              SNR Margin:        0.0 dB            0.0 dB
            Actual Delay:          0 ms              0 ms
          Transmit Power:        0.0 dBm           0.0 dBm
           Receive Power:        0.0 dBm           0.0 dBm
              Actual INP:        0.0 symbols       0.0 symbols
       Total Attenuation:        0.0 dB            0.0 dB
Attainable Net Data Rate:      0.000 Mbps        0.000 Mbps
=============================================================================

           xDSL Counters

           Downstream        Upstream
Since Link time = 0 sec
FEC:            0               0
CRC:            0               0
ES:             0               0
SES:            0               0
UAS:            12204           0
LOS:            0               0
LOF:            0               0
LOM:            0               0
Latest 15 minutes time = 1 min 14 sec
FEC:            0               0
CRC:            0               0
ES:             0               0
SES:            0               0
UAS:            46              46
LOS:            0               0
LOF:            0               0
LOM:            0               0
Previous 15 minutes time = 15 min 0 sec
FEC:            0               0
CRC:            0               0
ES:             0               0
SES:            0               0
UAS:            554             554
LOS:            0               0
LOF:            0               0
LOM:            0               0
Latest 1 day time = 5 hours 32 min 49 sec
FEC:            0               0
CRC:            0               0
ES:             0               0
SES:            0               0
UAS:            12261           12261
LOS:            0               0
LOF:            0               0
LOM:            0               0
Previous 1 day time = 0 sec
FEC:            0               0
CRC:            0               0
ES:             0               0
SES:            0               0
UAS:            0               0
LOS:            0               0
LOF:            0               0
LOM:            0               0
Total time = 5 hours 32 min 49 sec
FEC:            0               0
CRC:            0               0
ES:             0               0
SES:            0               0
UAS:            12261           12261
LOS:            0               0
LOF:            0               0
LOM:            0               0
```

The following table describes the labels in this screen.

Table 12 Status > xDSL Statistics

LABEL	DESCRIPTION
xDSL Training Status	This displays the current state of setting up the DSL connection.
xDSL Profile	This displays the group of DSL settings the DSL port is currently using. **0** displays if the DSL port is not currently using any group of DSL settings.
Traffic Type	This displays the type of traffic the DSL port is sending and receiving. **Inactive** displays if the DSL port is not currently sending or receiving traffic.
Link Uptime	This displays how long the port has been running (or connected) since the last time it was started.
xDSL Port Details	
Upstream	These are the statistics for the traffic direction going out from the port to the service provider.
Downstream	These are the statistics for the traffic direction coming into the port from the service provider.
Line Rate	These are the data transfer rates at which the port is sending and receiving data.
Actual Net Data Rate	These are the rates at which the port is sending and receiving the payload data without transport layer protocol headers and traffic.
Trellis Coding	This displays whether or not the port is using Trellis coding for traffic it is sending and receiving. Trellis coding helps to reduce the noise in ADSL transmissions. Trellis may reduce throughput but it makes the connection more stable.
SNR Margin	This is the upstream and downstream Signal-to-Noise Ratio margin (in dB). A DMT sub-carrier's SNR is the ratio between the received signal power and the received noise power. The signal-to-noise ratio margin is the maximum that the received noise power could increase with the system still being able to meet its transmission targets.
Actual Delay	This is the upstream and downstream interleave delay. It is the wait (in milliseconds) that determines the size of a single block of data to be interleaved (assembled) and then transmitted. Interleave delay is used when transmission error correction (Reed- Solomon) is necessary due to a less than ideal telephone line. The bigger the delay, the bigger the data block size, allowing better error correction to be performed.
Transmit Power	This is the upstream and downstream far end actual aggregate transmit power (in dBm). Upstream is how much power the port is using to transmit to the service provider. Downstream is how much port the service provider is using to transmit to the port.
Receive Power	Upstream is how much power the service provider is receiving from the port. Downstream is how much power the port is receiving from the service provider.
Actual INP	Sudden spikes in the line's level of external noise (impulse noise) can cause errors and result in lost packets. This could especially impact the quality of multimedia traffic such as voice or video. Impulse noise protection (INP) provides a buffer to allow for correction of errors caused by error correction to deal with this. The number of DMT (Discrete Multi-Tone) symbols shows the level of impulse noise protection for the upstream and downstream traffic. A higher symbol value provides higher error correction capability, but it causes overhead and higher delay which may increase error rates in received multimedia data.
Total Attenuation	This is the upstream and downstream line attenuation, measured in decibels (dB). This attenuation is the difference between the power transmitted at the near-end and the power received at the far-end. Attenuation is affected by the channel characteristics (wire gauge, quality, condition and length of the physical line).

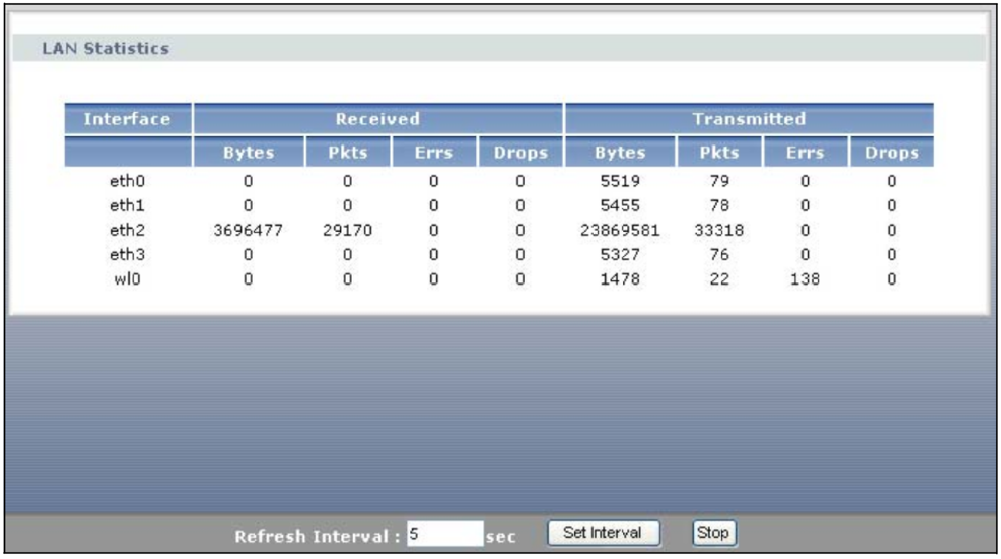
Table 12 Status > xDSL Statistics (continued)

LABEL	DESCRIPTION
Attainable Net Data Rate	These are the highest theoretically possible transfer rates at which the port could send and receive payload data without transport layer protocol headers and traffic.
xDSL Counters	
Downstream	These are the statistics for the traffic direction coming into the port from the service provider.
Upstream	These are the statistics for the traffic direction going out from the port to the service provider.
FEC	This is the number of Far End Corrected blocks.
CRC	This is the number of Cyclic Redundancy Checks.
ES	This is the number of Errored Seconds meaning the number of seconds containing at least one errored block or at least one defect.
SES	This is the number of Severely Errored Seconds meaning the number of seconds containing 30% or more errored blocks or at least one defect. This is a subset of ES.
UAS	This is the number of UnAvailable Seconds.
LOS	This is the number of Loss Of Signal seconds.
LOF	This is the number of Loss Of Frame seconds.
LOM	This is the number of Loss of Margin seconds.
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.

4.1.7 LAN Statistics

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

Figure 13 Status > 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

The following table describes the labels in this screen.

Table 13 Status > LAN Statistics

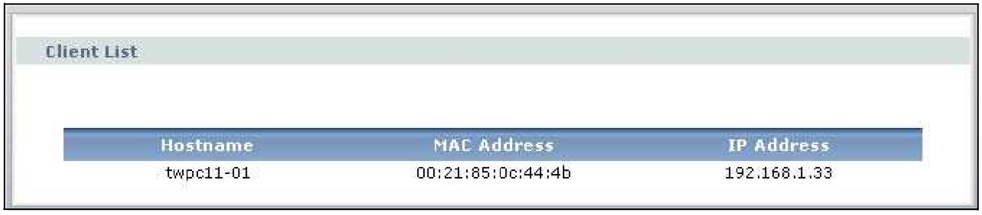
LABEL	DESCRIPTION
Interface	This shows the LAN or WLAN interface. **eth0~3** represent the physical Ethernet ports 1~ 4.
Received	
Bytes	This indicates the number of bytes received on this interface.
Pkts	This indicates the number of transmitted packets on this interface.
Errs	This indicates the number 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.

4.1.8 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 Device as a DHCP server or disable it. When configured as a server, the 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 Device's DHCP server.

Figure 14 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 14 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.

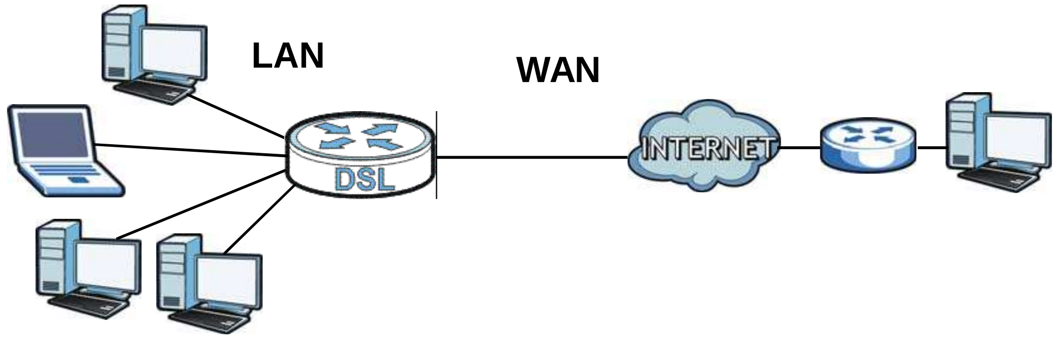
WAN Setup

5.1 Overview

This chapter discusses the Device's **WAN** screens. Use these screens to configure your 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 15 LAN and WAN



- See Section 5.7 on page 107 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 86).
- The **Internet Connection** screen lets you view and configure the WAN settings on the Device for Internet access (Section 5.5 on page 90).
- The **3G Backup** screen lets you configure the 3G WAN connection (Section 5.6 on page 105).

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 Device, which makes it accessible from an outside network. It is used by the Device to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the 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.

IPv6

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The ZyXEL device can use IPv4/IPv6 dual stack to connect to IPv4 and IPv6 networks, and supports IPv6 rapid deployment (6RD). See Appendix B on page 271 for background information about IPv6.

3G

3G (Third Generation) is a digital, packet-switched wireless technology. Bandwidth usage is optimized as multiple users share the same channel and bandwidth is only allocated to users when they send data. It allows fast transfer of voice and non-voice data and provides broadband Internet access to mobile devices.

5.3 Before You Begin

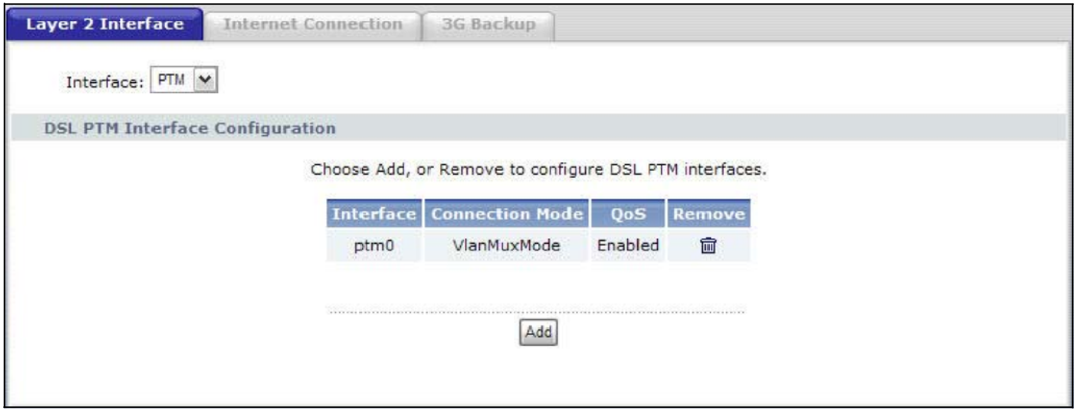
You need to know your Internet access settings such as encapsulation and WAN IP address. Get this information from your ISP.

5.4 The Layer 2 Interface Screen

The 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 16 Layer 2 Interface: PTM



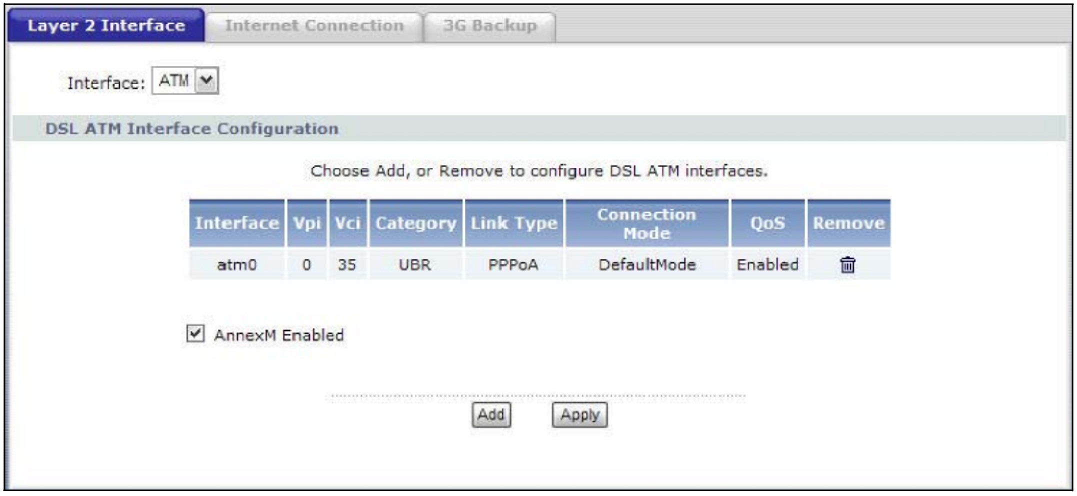
Interface: PTM

DSL PTM Interface Configuration

Choose Add, or Remove to configure DSL PTM interfaces.

Interface	Connection Mode	QoS	Remove
ptm0	VlanMuxMode	Enabled	🗑

Figure 17 Layer 2 Interface: ATM



Interface: ATM

DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	Category	Link Type	Connection Mode	QoS	Remove
atm0	0	35	UBR	PPPoA	DefaultMode	Enabled	🗑

☑ AnnexM Enabled

The following table describes the fields in this screen.

Table 15 Layer 2 Interface

LABEL	DESCRIPTION
Interface	Select an interface for which you want to configure here. **PTM**: The Device uses the VDSL technology for data transmission over the DSL port. **ATM**: The 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.
Connection Mode	This shows the connection mode of the layer-2 interface.
QoS	This displays whether QoS (Quality of Service) is enabled on the interface.

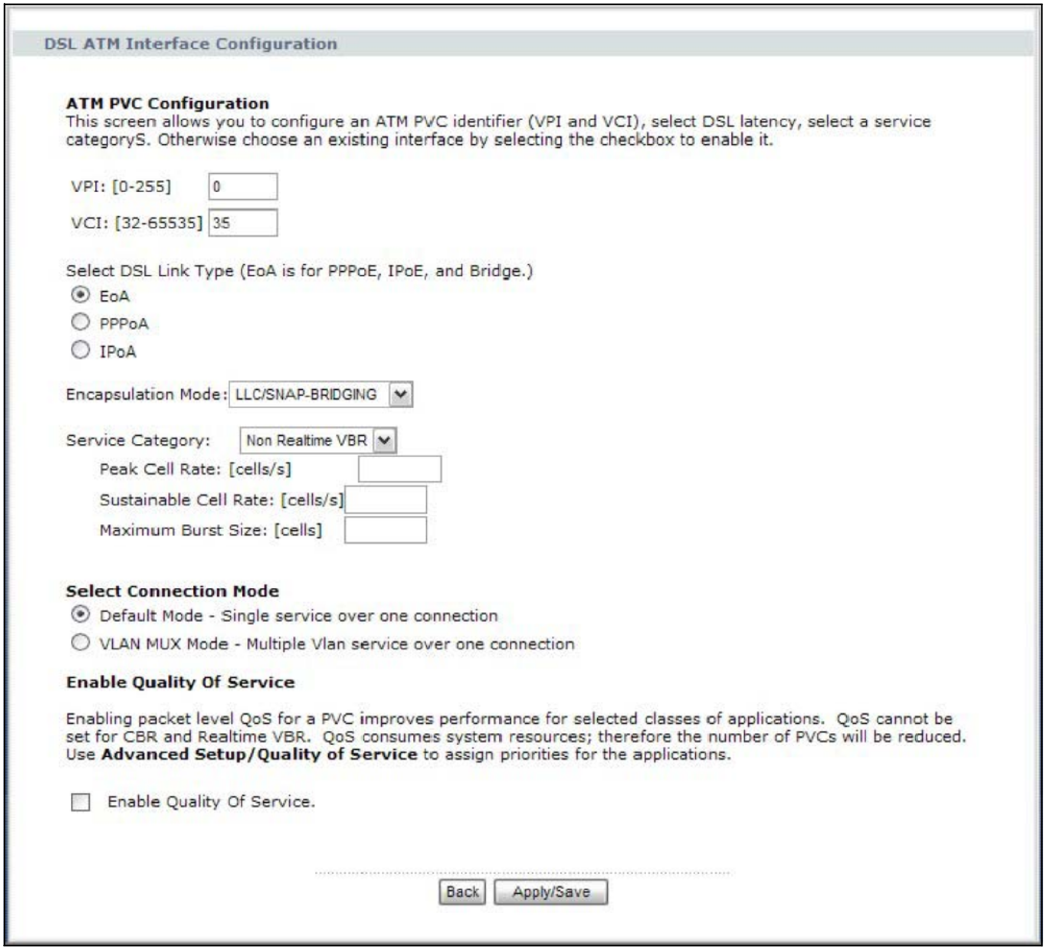
Table 15 Layer 2 Interface (continued)

LABEL	DESCRIPTION
Remove	Click the **Remove** button to delete this interface from the 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.
AnnexM Enabled	This option is available for an ATM (ADSL) interface. Select this to use double upstream mode to increase the maximum upstream transfer rate.
Add	Click this button to create a new layer-2 interface.
Apply	This button is available for an ATM (ADSL) interface. Click **Apply** to save your changes back to the Device.

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 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 18 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: Non Realtime VBR
Peak Cell Rate: [cells/s]
Sustainable Cell Rate: [cells/s]
Maximum Burst Size: [cells]

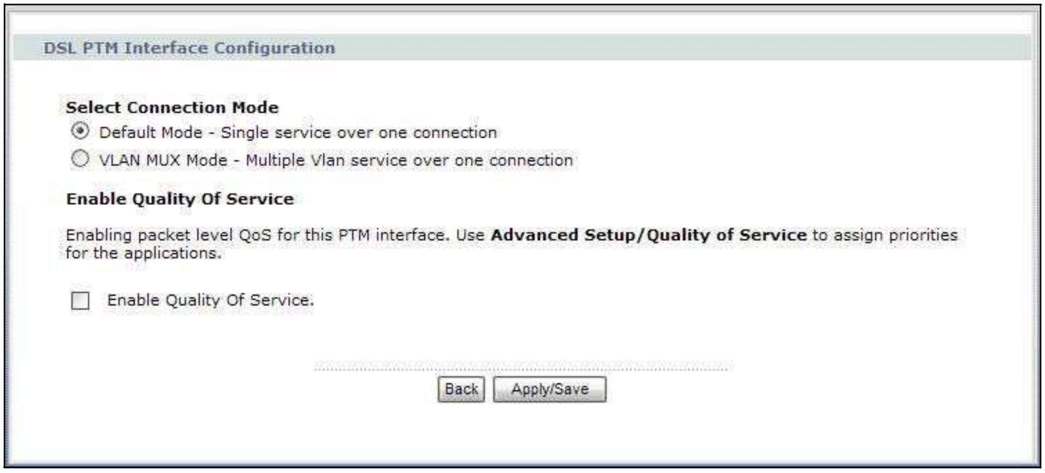
Select Connection Mode
● Default Mode - Single service over one connection
○ VLAN MUX Mode - Multiple Vlan service over one connection

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 19 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

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 16 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 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.

Table 16 DSL PTM Interface Configuration (continued)

LABEL	DESCRIPTION
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.
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. This field is not available if you select **PPPoA** or **IPoA** as the DSL link type. The 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. The QoS setting applies to all WAN connections over the same PVC. 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.

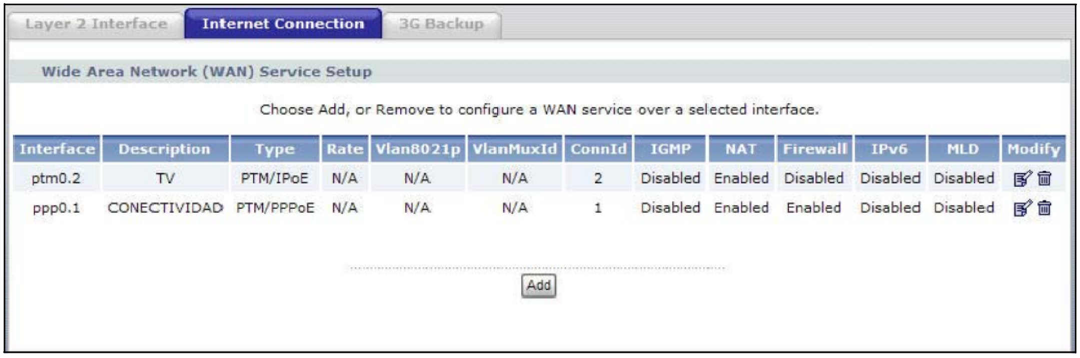
5.5 The Internet Connection Screen

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

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

Note: When a layer-2 interface is in **VLAN MUX Mode**, you can configure up to five WAN services on the Device.

Figure 20 Internet Connection



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	IPv6	MLD	Modify
ptm0.2	TV	PTM/IPoE	N/A	N/A	N/A	2	Disabled	Enabled	Disabled	Disabled	Disabled	✎ 🗑
ppp0.1	CONECTIVIDAD	PTM/PPPoE	N/A	N/A	N/A	1	Disabled	Enabled	Enabled	Disabled	Disabled	✎ 🗑

The following table describes the labels in this screen.

Table 17 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 **ppp*** 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**.
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.
IPv6	This shows whether IPv6 is activated or not for this connection. IPv6 is not available when the connection uses the bridging service.

Table 17 Internet Connection

LABEL	DESCRIPTION
MLD	This shows whether Multicast Listener Discovery (MLD) is activated or not for this connection. MLD 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.

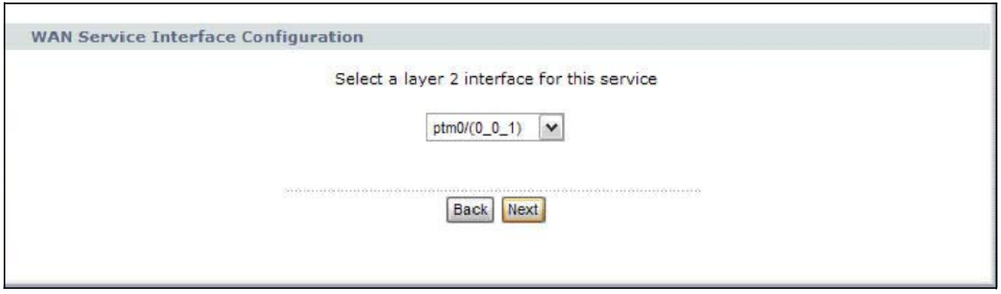
5.5.1 WAN Connection Configuration

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 21 WAN Configuration: WAN Interface



WAN Service Interface Configuration

Select a layer 2 interface for this service

ptm0/(0_0_1)

The following table describes the labels in this screen.

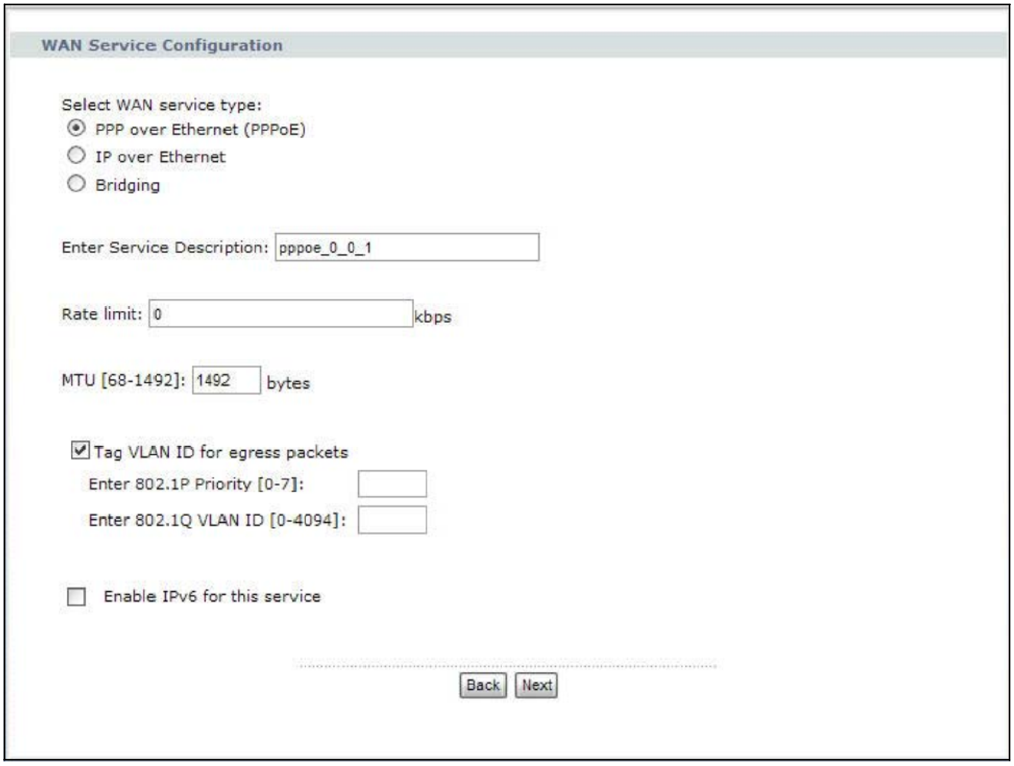
Table 18 WAN Configuration: WAN Interface

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 **atmx** or **ipoax** (where x starts from 0 and is the index number of ATM layer-2 interfaces using different VPI and/or VCI values) 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** and **MTU** fields in this screen.

Figure 22 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: 0 kbps

MTU [68-1492]: 1492 bytes

☑ Tag VLAN ID for egress packets

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

☐ Enable IPv6 for this service

Figure 23 The following table describes the labels in this screen.

Table 19 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.
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the Device divides it into smaller fragments.
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.

Table 19 WAN Configuration: Service Type

LABEL	DESCRIPTION
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.
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.
Enable IPv6 for this service	Select this option to enable IPv6 for this WAN service so that the Device can use an IPv6 address when sending traffic through this connection. You can only enable IPv6 for a WAN service that uses the PPPoE or IPoE encapsulation method over the ATM or PTM interface.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

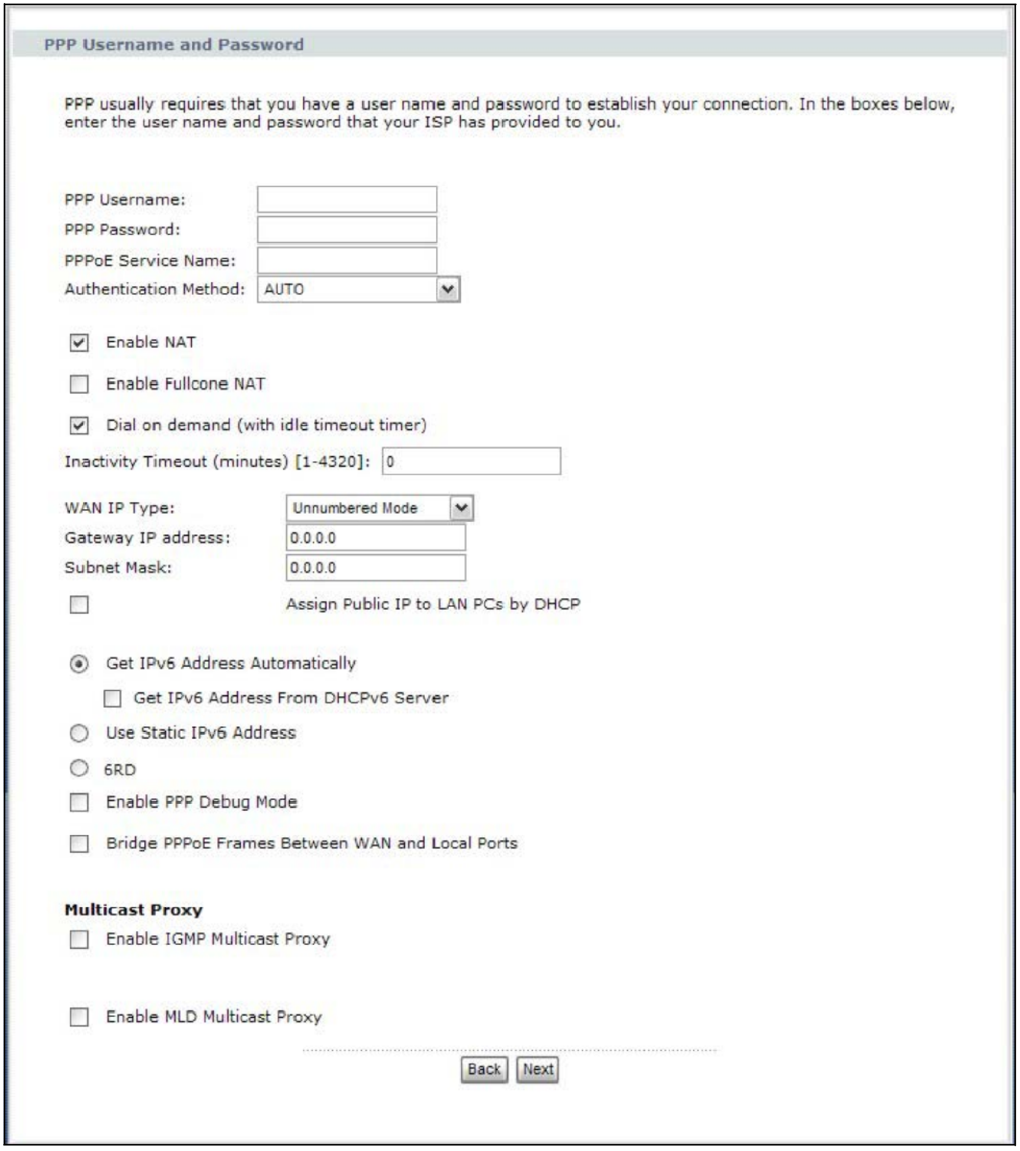
5.5.1.3 WAN IP Address and DNS Server

The screen differs by the encapsulation you selected in the previous screen. See Section 5.7 on page 107 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 24 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 NAT

□ Enable Fullcone NAT

☑ Dial on demand (with idle timeout timer)

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

WAN IP Type: Unnumbered Mode

Gateway IP address: 0.0.0.0

Subnet Mask: 0.0.0.0

□ Assign Public IP to LAN PCs by DHCP

● Get IPv6 Address Automatically

□ Get IPv6 Address From DHCPv6 Server

○ Use Static IPv6 Address

○ 6RD

□ Enable PPP Debug Mode

□ Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

□ Enable IGMP Multicast Proxy

□ Enable MLD Multicast Proxy

The following table describes the labels in this screen.

Table 20 WAN Configuration: PPPoE or PPPoA

LABEL	DESCRIPTION
PPP Username	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.

Table 20 WAN Configuration: PPPoE or PPPoA

LABEL	DESCRIPTION
PPPoE Service Name	Type the name of your PPPoE service here. This field is not available for a PPPoA connection.
Authentication Method	The 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 Device accepts either CHAP or PAP when requested by this remote node. **PAP** - Your Device accepts PAP only. **CHAP** - Your Device accepts CHAP only. **MSCHAP** - Your Device accepts MSCHAP only. MS-CHAP is the Microsoft version of the CHAP.
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**.
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.
WAN IP Type	Select how the WAN interface is to get its IP address. • **Dynamic IPv4 Address**: Has the Device get an IP address automatically from the PPPoE or PPPoA server. • **Static IPv4 Address**: Select this if your ISP provided a single static IP address for you to use. Then enter the static IP address provided by your ISP in the **IPv4 Address** field that displays. • **Unnumbered Mode**: Select this if your ISP provided a range of static public IP addresses for you to use. Enter the Device's WAN IP address and subnet mask in the **Gateway IP address** and **Subnet Mask** fields that display. The subnet mask must be smaller than C class (255.255.255.0). Select **Assign Public IP to LAN PCs by DHCP** to have the Device give the LAN DHCP clients public IP addresses. LAN clients can still configure static private IP addresses and access the Internet. Clear the **Assign Public IP to LAN PCs by DHCP** option to assign the LAN DHCP clients private IP addresses. LAN clients can still configure static public IP addresses and access the Internet.
Get IPv6 Address Automatically	Select this option if you want to have the Device use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address.
Get IPv6 Address From DHCPv6 Server	Select this checkbox if you want to obtain an IPv6 address from a DHCPv6 server. The IP address assigned by a DHCPv6 server has priority over the IP address automatically generated by the Device using the IPv6 prefix from an RA.
Use Static IPv6 Address	Select this option if you have a fixed IPv6 address assigned by your ISP.
WAN IPv6 Address	Enter the IPv6 address assigned by your ISP.
WAN IPv6 Address Prefix Length	Enter the address prefix length to specify how many most significant bits in an IPv6 address compose the network address.

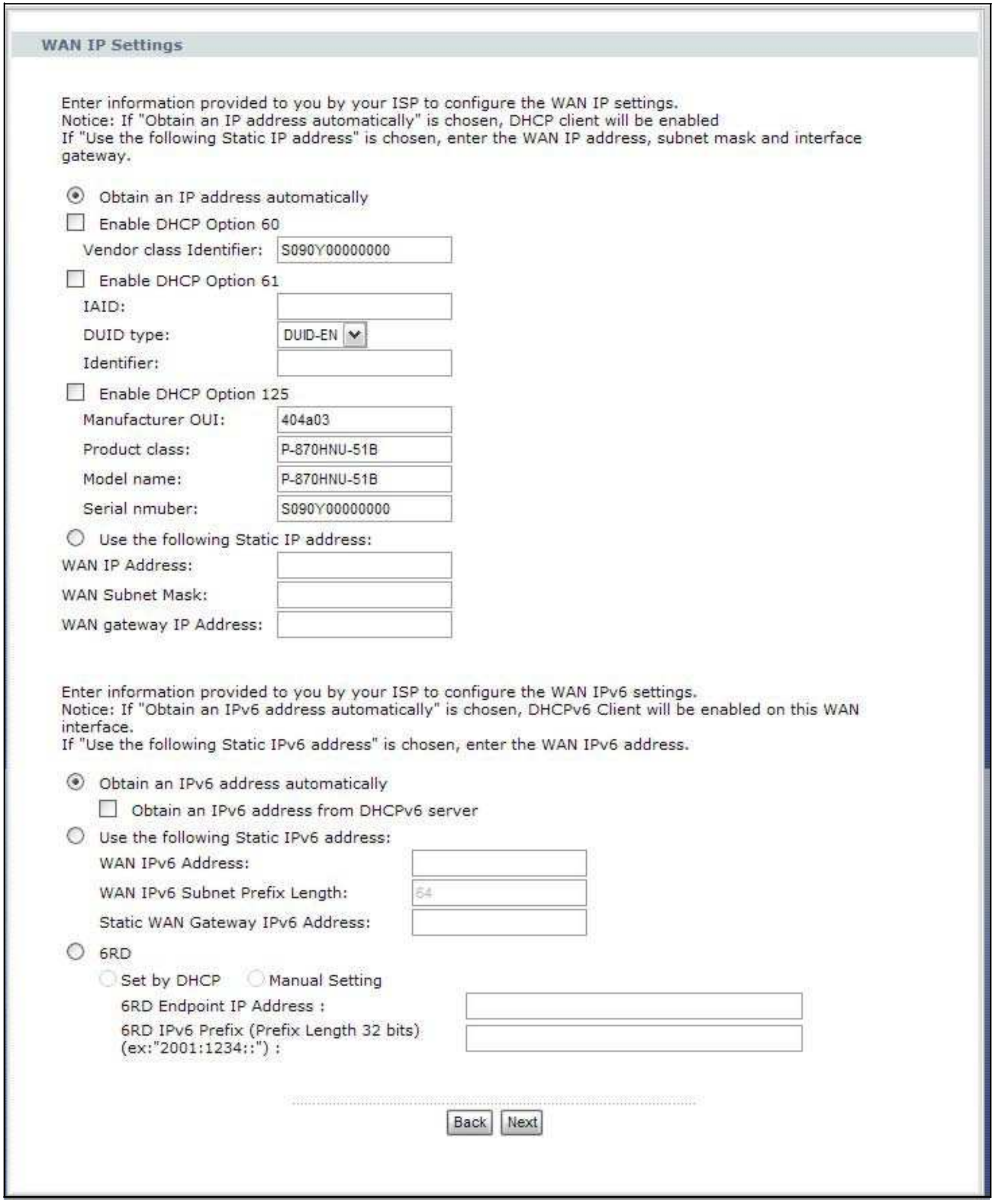
Table 20 WAN Configuration: PPPoE or PPPoA

LABEL	DESCRIPTION
6RD (6to4 Tunneling)	Select this option to enable IPv6 to IPv4 tunneling. This will encapsulate IPv6 to IPv4 packets. Select **Set by DCHP** if you want to obtain a 6RD endpoint IP address from a DHCP server. Select **Manual Setting** to specify the 6RD endpoint IP address manually.
6RD Endpoint IP Address	If you enabled 6RD, specify the 6RD endpoint IP address.
6RD IPv6 Prefix	If you enabled 6RD, specify the IPv6 prefix for the endpoint IP address.
Enable PPP Debug Mode	Select this option to display PPP debugging messages on the console.
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 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 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 Device act as an IGMP proxy on this connection. This allows the Device to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Enable MLD Multicast Proxy	Select **Enable** to have the ZyXEL Device act as an MLD proxy on this connection. This allows the ZyXEL Device to get subscription information and maintain a joined member list for each multicast group. It can reduce multicas 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 25 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:	S090Y00000000

□ Enable DHCP Option 61

IAID:	
DUID type:	DUID-EN
Identifier:	

□ Enable DHCP Option 125

Manufacturer OUI:	404a03
Product class:	P-870HNU-51B
Model name:	P-870HNU-51B
Serial nmuber:	S090Y00000000

○ Use the following Static IP address:

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

Enter information provided to you by your ISP to configure the WAN IPv6 settings.
Notice: If "Obtain an IPv6 address automatically" is chosen, DHCPv6 Client will be enabled on this WAN interface.
If "Use the following Static IPv6 address" is chosen, enter the WAN IPv6 address.

◉ Obtain an IPv6 address automatically

□ Obtain an IPv6 address from DHCPv6 server

○ Use the following Static IPv6 address:

WAN IPv6 Address:	
WAN IPv6 Subnet Prefix Length:	64
Static WAN Gateway IPv6 Address:	

○ 6RD

○ Set by DHCP ○ Manual Setting

6RD Endpoint IP Address :	
6RD IPv6 Prefix (Prefix Length 32 bits) (ex:"2001:1234::") :	

The following table describes the labels in this screen.

Table 21 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 Device in DHCP requests that the 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 Device in DHCP requests that the Device sends to a DHCP server when getting a WAN IP address.
IAID	Enter the Identity Association Identifier (IAID) of the Device. For example, the WAN connection index number.
DUID Type	Select **Other** to enter any string that identifies the Device in the **DUID** field. Select **DUID-LL** (DUID Based on Link-layer Address) to enter the 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.
DUID	Enter the DHCP Unique Identifier (DUID) of the Device. This field is not available when you select **DUID-EN** in the **DUID Type** field.
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 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 Device.
Model Name	Enter the model name of the Device.
Serial Number	Enter the serial number of the 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.
Obtain an IPv6 address automatically	Select this option if you want to have the Device use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address.
Obtain an IPv6 address from DHCPv6 server	Select this checkbox if you want to obtain an IPv6 address from a DHCPv6 server. The IP address assigned by a DHCPv6 server has priority over the IP address automatically generated by the Device using the IPv6 prefix from an RA.
Use the following Static IPv6 address	Select this option if you have a fixed IPv6 address assigned by your ISP.
WAN IPv6 Address	Enter the static IPv6 address provided by your ISP.

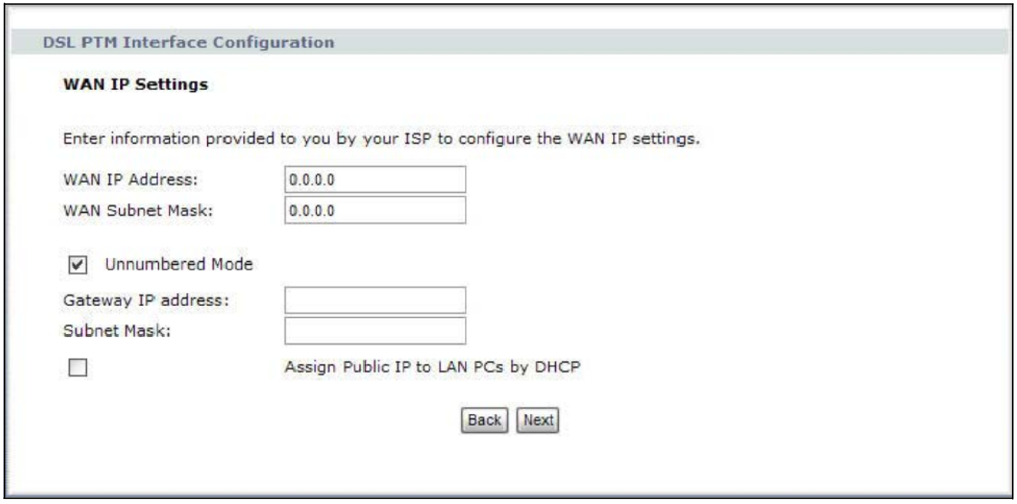
Table 21 WAN Configuration: IPoE

LABEL	DESCRIPTION
WAN IPv6 Subnet Prefix Length	Enter the bit number of the IPv6 subnet mask provided by your ISP.
Static WAN Gateway IPv6 Address	Enter the gateway IPv6 address provided by your ISP.
6RD (6to4 Tunneling)	Select this option to enable IPv6 to IPv4 tunneling. This will encapsulate IPv6 to IPv4 packets. Select **Set by DCHP** if you want to obtain a 6RD endpoint IP address from a DHCP server. Select **Manual Setting** to specify the 6RD endpoint IP address manually.
6RD Endpoint IP Address	If you enabled 6RD, specify the 6RD endpoint IP address.
6RD IPv6 Prefix	If you enabled 6RD, specify the IPv6 prefix for the endpoint IP address.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

IPoA

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.

Figure 26 WAN Configuration: IPoA



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

☑ Unnumbered Mode

Gateway IP address:

Subnet Mask:

☐ Assign Public IP to LAN PCs by DHCP

The following table describes the labels in this screen.

Table 22 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.
Unnumbered Mode	Select this if your ISP provided a range of static public IP addresses for you to use.
Gateway IP Address	Enter the Device’s WAN IP address.

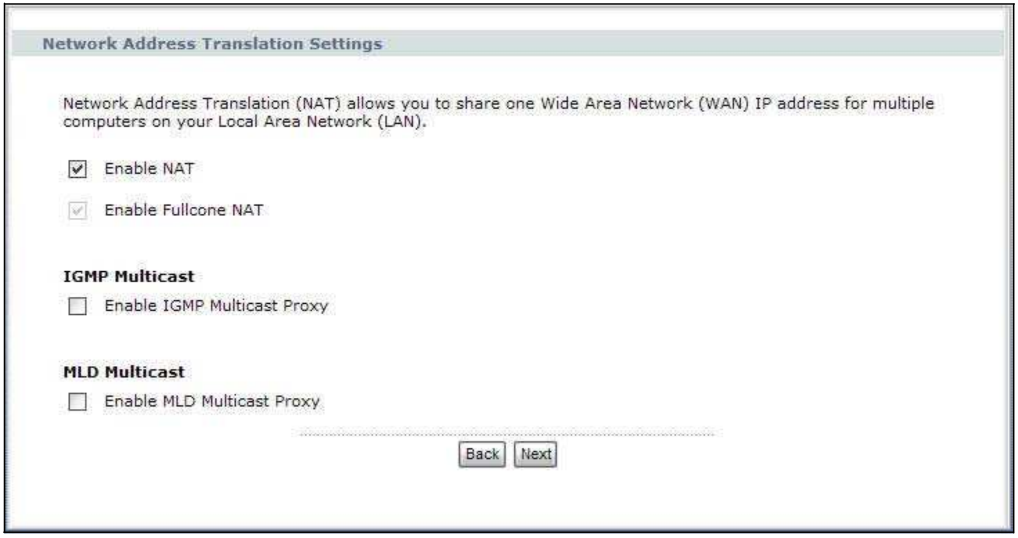
Table 22 WAN Configuration: IPoA

LABEL	DESCRIPTION
Subnet Mask	Enter the Device’s subnet mask. It must be smaller than C class (255.255.255.0).
Assign Public IP to LAN PCs by DHCP	Select this to have the Device give the LAN DHCP clients public IP addresses. LAN clients can still configure static private IP addresses and access the Internet. Clear this option to assign the LAN DHCP clients private IP addresses. LAN clients can still configure static public IP addresses and access the Internet.
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 27 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

IGMP Multicast

□ Enable IGMP Multicast Proxy

MLD Multicast

□ Enable MLD Multicast Proxy

The following table describes the labels in this screen.

Table 23 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 IGMP Multicast Proxy	Select this check box to have the Device act as an IGMP proxy on this connection. This allows the Device to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Enable MLD Multicast Proxy	Select **Enable** to have the ZyXEL Device act as an MLD proxy on this connection. This allows the ZyXEL Device to get subscription information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.

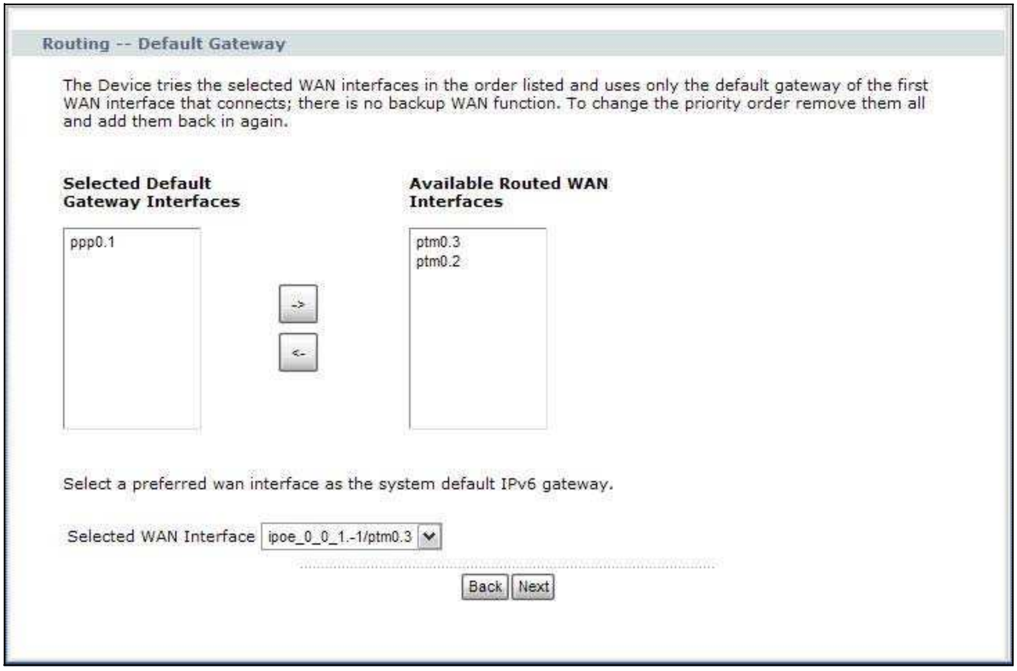
Table 23 WAN Configuration: NAT, IGMP Multicast and Firewall Activation: IPoE

LABEL	DESCRIPTION
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 28 WAN Configuration: Default Gateway: PPPoE, PPPoA, IPoE or IPoA



Routing -- Default Gateway

The Device tries the selected WAN interfaces in the order listed and uses only the default gateway of the first WAN interface that connects; there is no backup WAN function. To change the priority order remove them all and add them back in again.

Selected Default Gateway Interfaces: ppp0.1

Available Routed WAN Interfaces: ptm0.3, ptm0.2

Select a preferred wan interface as the system default IPv6 gateway.

Selected WAN Interface: ipoe_0_0_1.-1/ptm0.3

The following table describes the labels in this screen.

Table 24 WAN Configuration: Default Gateway: PPPoE or IPoE

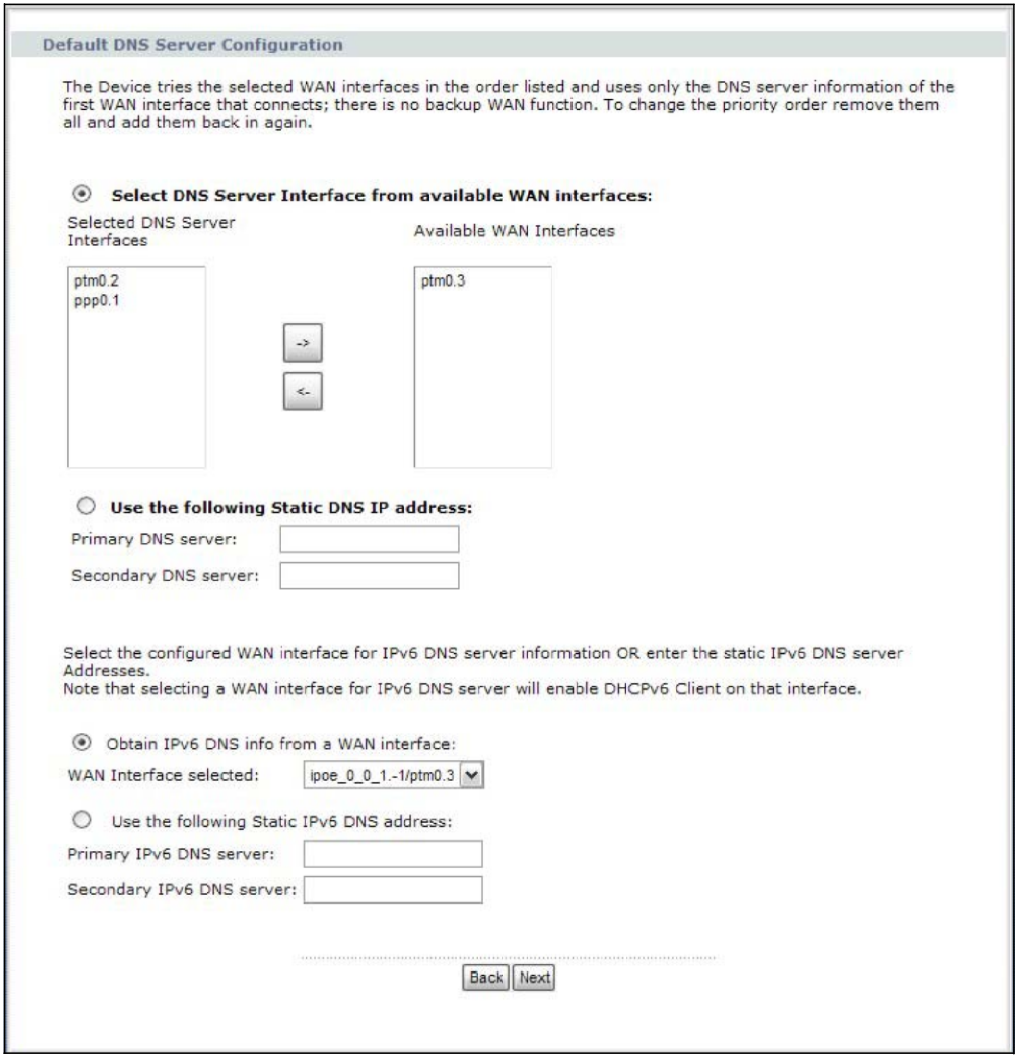
LABEL	DESCRIPTION
Selected Default Gateway Interfaces	Select a WAN interface through which you want to forward the traffic. You can select multiple WAN interfaces for the device to try. The Device tries the WAN interfaces in the order listed and uses only the default gateway of the first WAN interface that connects; there is no backup WAN function. To change the priority order remove them all and add them back in again.
Available Routed WAN Interfaces	These are the WAN interfaces you can select from.
Selected WAN Interface	Select a WAN interface through which to forward IPv6 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 Device, you must enter the static DNS server address.

Figure 29 WAN Configuration: DNS Server: PPPoE, PPPoA, IPoE or IPoA



Default DNS Server Configuration

The Device tries the selected WAN interfaces in the order listed and uses only the DNS server information of the first WAN interface that connects; there is no backup WAN function. To change the priority order remove them all and add them back in again.

● Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces: ptm0.2, ppp0.1

Available WAN Interfaces: ptm0.3

○ Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses.
Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.

● Obtain IPv6 DNS info from a WAN interface:

WAN Interface selected: ipoe_0_0_1.-1/ptm0.3

○ Use the following Static IPv6 DNS address:

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

The following table describes the labels in this screen.

Table 25 WAN Configuration: DNS Server: PPPoE or IPoE

LABEL	DESCRIPTION
Select DNS Server Interface from available WAN interfaces	Select this to have the Device get the DNS server addresses from one of the Device's WAN interfaces.
Selected DNS Server Interfaces	Select a WAN interface through which to get DNS server addresses. You can select multiple WAN interfaces for the device to try. The Device tries the WAN interfaces in the order listed and uses only the DNS server information of the first WAN interface that connects; there is no backup WAN function. To change the priority order remove them all and add them back in again.

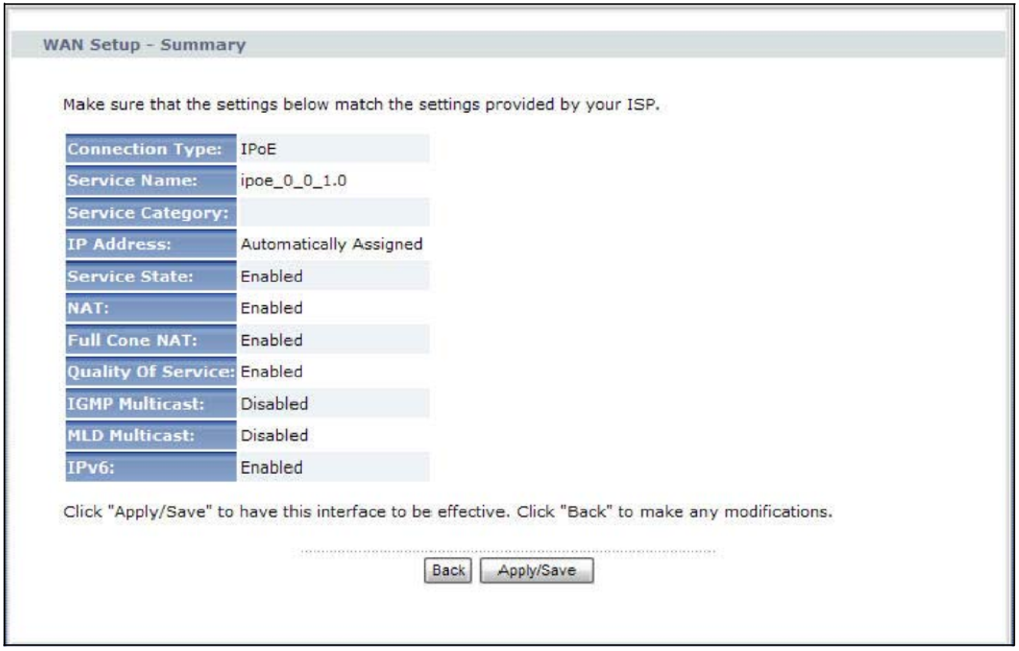
Table 25 WAN Configuration: DNS Server: PPPoE or IPoE

LABEL	DESCRIPTION
Available WAN Interfaces	These are the WAN interfaces you can select from.
Use the following Static DNS IP address	Select this to have the 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.
Obtain IPv6 DNS info from a WAN interface	Select this to have the Device get the IPv6 DNS server addresses from the ISP automatically.
WAN Interface selected	Select a WAN interface through which you want to obtain the IPv6 DNS related information.
Use the following Static IPv6 DNS address	Select this to have the Device use the IPv6 DNS server addresses you configure manually.
Primary IPv6 DNS server	Enter the first IPv6 DNS server address assigned by the ISP.
Secondary IPv6 DNS server	Enter the second IPv6 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 30 WAN Configuration: Configuration Summary



WAN Setup - Summary

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

Connection Type:	IPoE
Service Name:	ipoe_0_0_1.0
Service Category:	
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Full Cone NAT:	Enabled
Quality Of Service:	Enabled
IGMP Multicast:	Disabled
MLD Multicast:	Disabled
IPv6:	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 26 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 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.
Quality Of Service	This shows whether QoS is active or not for this connection.
IGMP Multicast	This shows whether IGMP multicasting is active or not for this connection.
MLD Multicast	This shows whether MLD multicasting is active or not for this connection.
IPv6	This shows whether IPv6 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 The 3G Backup Screen

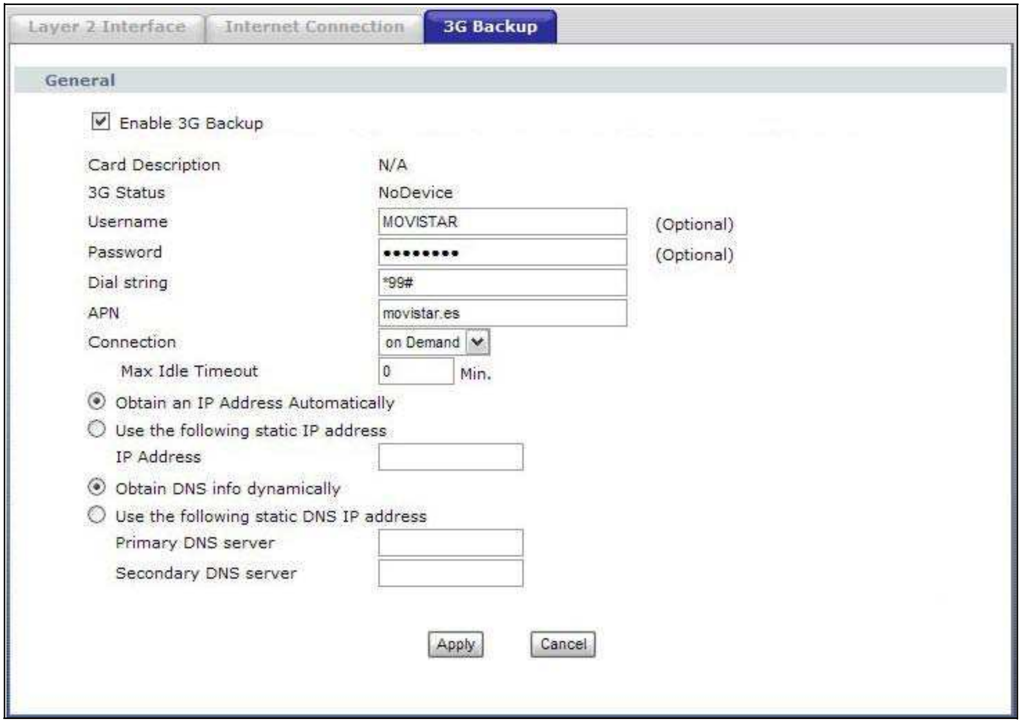
Use this screen to configure your 3G settings. Click **Network > WAN > 3G Backup**.

At the time of writing, the 3G cards you can use in the Device are Huawei E220, Huawei E169u, Huawei E161, Qisda H21, ZTE MF100, ZTE MF110 and Huawei E1752.

Note: The actual data rate you obtain varies depending the 3G card you use, the signal strength to the service provider’s base station, and so on.

If the signal strength of a 3G network is too low, the 3G card may switch to an available 2.5G or 2.75G network. Refer to Section 5.7 on page 107 for a comparison between 2G, 2.5G, 2.75G and 3G wireless technologies.

Figure 31 3G Backup



General

☑ Enable 3G Backup

Card Description	N/A	
3G Status	NoDevice	
Username	MOVISTAR	(Optional)
Password	••••••••	(Optional)
Dial string	*99#	
APN	movistar.es	
Connection	on Demand	
Max Idle Timeout	0	Min.

● Obtain an IP Address Automatically

○ Use the following static IP address

IP Address

● Obtain DNS info dynamically

○ Use the following static DNS IP address

Primary DNS server

Secondary DNS server

The following table describes the labels in this screen.

Table 27 3G Backup

LABEL	DESCRIPTION
Enable 3G Backup	Select this option to have the Device use the 3G connection as your WAN or a backup when the wired WAN connection fails.
Card Descriptioin	This field displays the manufacturer and model name of your 3G card if you inserted one in the Device. Otherwise, it displays **N/A**.
3G Status	This field displays: • **NoDevice** when no 3G card is inserted, • **Disabled** when the 3G WAN is not activated, • **Up** when the 3G connection is up, • **Down** when the 3G connection is down, • **NoResponse** when there is no response from the inserted 3G card, • **InvalidPIN** if the PIN code you entered in the **WAN > 3G Backup** screen is not the right one for the 3G card you inserted, • **NeedPUK** if you enter the PIN (Personal Identification Number) code incorrectly for three times and the SIM card is blocked by your ISP, • **DialFail** when the Device fails to dial up a 3G connection. • or **InvalidSIM** when the SIM card is damaged or not inserted.
User Name	Type the user name (of up to 70 ASCII printable characters) given to you by your service provider.
Password	Type the password (of up to 70 ASCII printable characters) associated with the user name above.

Table 27 3G Backup (continued)

LABEL	DESCRIPTION
Dial string	Enter the phone number (dial string) used to dial up a connection to your service provider's base station. Your ISP should provide the phone number. For example, *99# is the dial string to establish a GPRS or 3G connection in Taiwan.
APN	Enter the APN (Access Point Name) provided by your service provider. Connections with different APNs may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charge method. You can enter up to 31 ASCII printable characters. Spaces are allowed.
Connection	Select **Nailed Up** if you do not want the connection to time out. Select **on Demand** if you do not want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field.
Max Idle Timeout	This value specifies the time in minutes that elapses before the Device automatically disconnects from the ISP. **0** means the Internet session will not timeout.
Obtain an IP Address Automatically	Select this option If your ISP did not assign you a fixed IP address.
Use the following static IP address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected **Use the following static IP address**.
Obtain DNS info dynamically	Select this to have the Device get the DNS server addresses from the ISP automatically.
Use the following static DNS IP address	Select this to have the Device use the DNS server addresses you configure manually.
Primary DNS server	Enter the first DNS server address assigned by the ISP.
Secondary DNS server	Enter the second DNS server address assigned by the ISP.
Apply	Click **Apply** to save your changes back to the Device.
Cancel	Click **Cancel** to return to the previous configuration.

5.7 Technical Reference

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

Encapsulation

Be sure to use the encapsulation method required by your ISP. The Device can work in bridge mode or routing mode. When the 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 Device (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the 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 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.

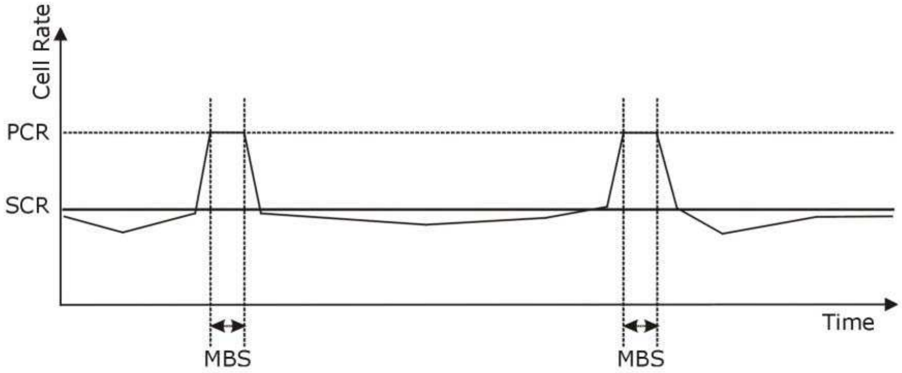
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

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 32 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

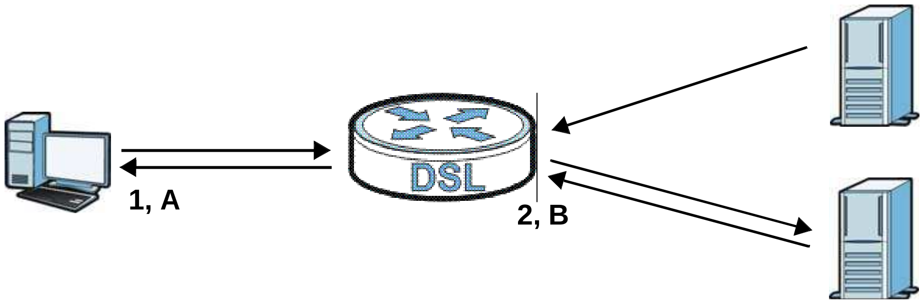
A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP address 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 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 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 33 Full Cone NAT Example



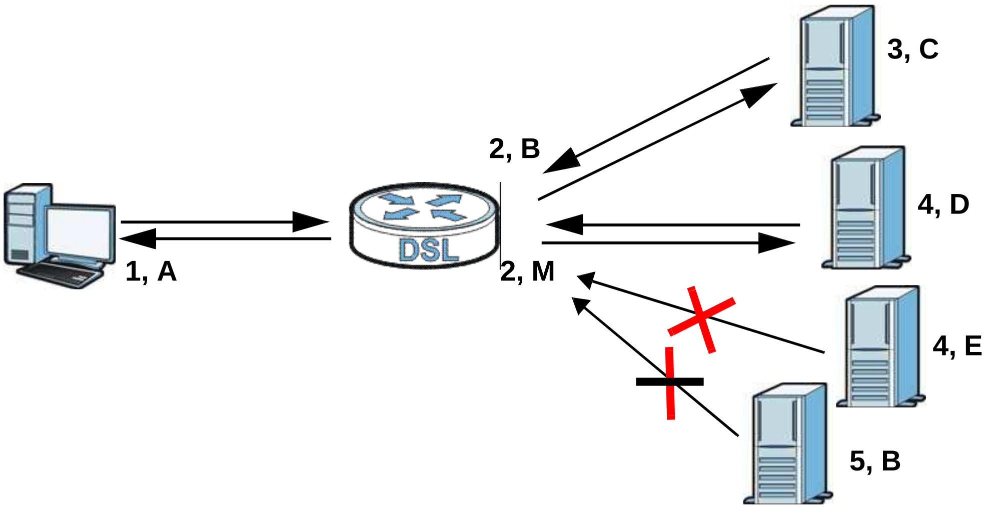
Symmetric NAT

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 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 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 34 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 Device queries all directly connected networks to gather group membership. After that, the 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 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 Device’s WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

3G Comparison Table

See the following table for a comparison between 2G, 2.5G, 2.75G and 3G wireless technologies.

Table 28 2G, 2.5G, 2.75G, 3G and 3.5G Wireless Technologies

NAME	TYPE	MOBILE PHONE AND DATA STANDARDS		DATA SPEED
		GSM-BASED	CDMA-BASED	
2G	Circuit-switched	GSM (Global System for Mobile Communications), Personal Handy-phone System (PHS), etc.	Interim Standard 95 (IS-95), the first CDMA-based digital cellular standard pioneered by Qualcomm. The brand name for IS-95 is cdmaOne. IS-95 is also known as TIA-EIA-95.	Slow
2.5G	Packet-switched	GPRS (General Packet Radio Services), High-Speed Circuit-Switched Data (HSCSD), etc.	CDMA2000 is a hybrid 2.5G / 3G protocol of mobile telecommunications standards that use CDMA, a multiple access scheme for digital radio. CDMA2000 1xRTT (1 times Radio Transmission Technology) is the core CDMA2000 wireless air interface standard. It is also known as 1x, 1xRTT, or IS-2000 and considered to be a 2.5G or 2.75G technology.	
2.75G	Packet-switched	Enhanced Data rates for GSM Evolution (EDGE), Enhanced GPRS (EGPRS), etc.		
3G	Packet-switched	UMTS (Universal Mobile Telecommunications System), a third-generation (3G) wireless standard defined in ITU[A] specification, is sometimes marketed as 3GSM. The UMTS uses GSM infrastructures and W-CDMA (Wideband Code Division Multiple Access) as the air interface.	CDMA2000 EV-DO (Evolution-Data Optimized, originally 1x Evolution-Data Only), also referred to as EV-DO, EVDO, or just EV, is an evolution of CDMA2000 1xRTT and enables high-speed wireless connectivity. It is also denoted as IS-856 or High Data Rate (HDR).	
3.5G	Packet-switched	HSDPA (High-Speed Downlink Packet Access) is a mobile telephony protocol, used for UMTS-based 3G networks and allows for higher data transfer speeds.		Fast

[A] The International Telecommunication Union (ITU) is an international organization within which governments and the private sector coordinate global telecom networks and services.

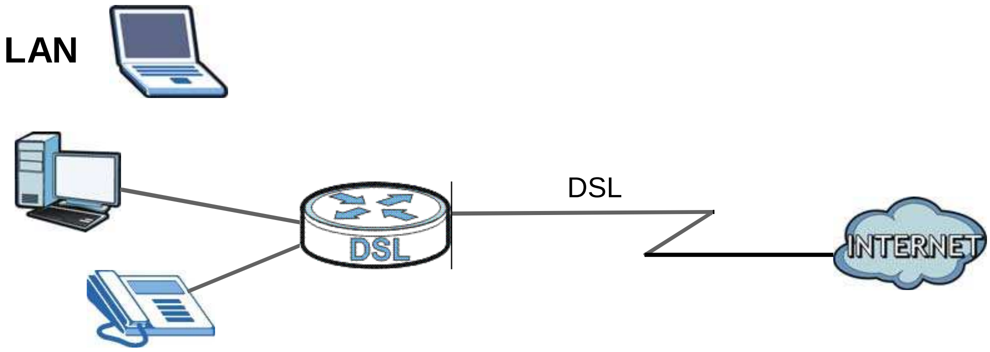
6

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 6.5 on page 120 for more information on LANs.

6.1.1 What You Can Do in this Chapter

- The **IP** screen (Section 6.3 on page 117) lets you set the LAN IP address and subnet mask of your ZyXEL device and configure other LAN TCP/IP settings.
- Use the **DHCP Client List** screen (Section 6.3 on page 117) to look at the IP addresses currently assigned to DHCP clients and the IP addresses reserved for specific MAC addresses.
- The **IPv6** screen lets you configure the IPv6 settings on your ZyXEL device's LAN interface (Section 6.5 on page 120).

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 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 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 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 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.

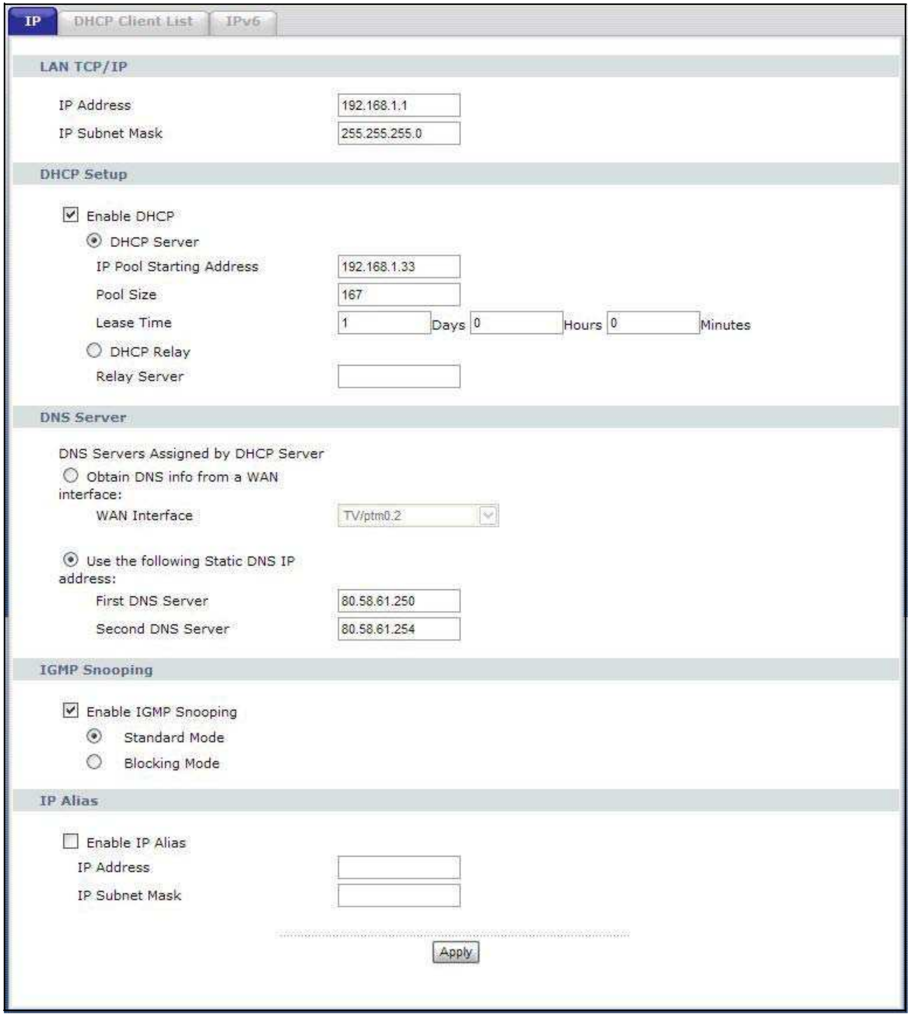
DNS

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 IP Screen

Click **Network > LAN > IP** to open the **IP** screen. See Section 6.5 on page 120 for background information. Use this screen to set the Local Area Network IP address and subnet mask of your Device.

Figure 35 Network > LAN > IP



LAN TCP/IP

IP Address: 192.168.1.1
IP Subnet Mask: 255.255.255.0

DHCP Setup

☑ Enable DHCP
● DHCP Server
IP Pool Starting Address: 192.168.1.33
Pool Size: 167
Lease Time: 1 Days 0 Hours 0 Minutes
○ DHCP Relay
Relay Server:

DNS Server

DNS Servers Assigned by DHCP Server
○ Obtain DNS info from a WAN interface:
WAN Interface: TV/ptm0.2
● Use the following Static DNS IP address:
First DNS Server: 80.58.61.250
Second DNS Server: 80.58.61.254

IGMP Snooping

☑ Enable IGMP Snooping
● Standard Mode
○ Blocking Mode

IP Alias

□ Enable IP Alias
IP Address:
IP Subnet Mask:

The following table describes the fields in this screen.

Table 29 Network > LAN > IP

LABEL	DESCRIPTION
LAN TCP/IP	
IP Address	Enter the LAN IP address you want to assign to your 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	

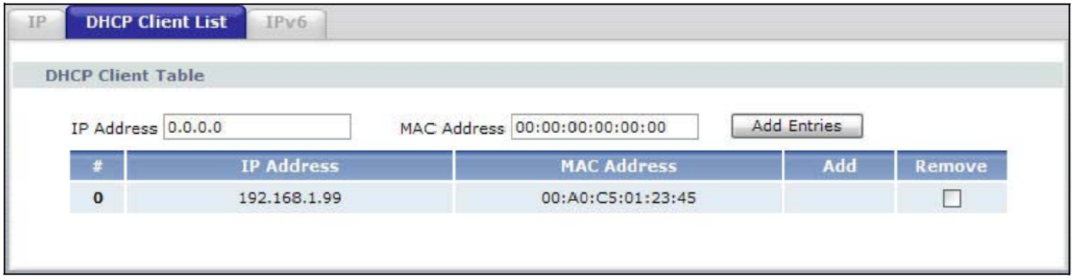
Table 29 Network > LAN > IP (continued)

LABEL	DESCRIPTION
Enable DHCP	Select this to have the Device act as a DHCP server or DHCP relay agent. Otherwise, deselect this to not have the Device provide any DHCP services. The DHCP server will be disabled.
DHCP Server	Select this option to have the Device assign IP addresses and provide subnet mask, gateway, and DNS server information to the network. The Device is the DHCP server for the network. When the 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.
Lease Time	This field specifies the lease time in days, hours and minutes of the IP address assigned by the DHCP server.
DHCP Relay	Select this option to have the Device forward DHCP request to the DHCP server.
Relay Server	If you select **DHCP Relay**, enter the IP address of the DHCP server.
DNS Server	
DNS Servers Assigned by DHCP Server If you do not configure DNS servers, the 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 Device, the Device forwards the query to its system DNS server you configured in the WAN screen.	
Obtain DNS info from a WAN interface:	Select this to have the Device get the DNS server addresses from one of the Device’s WAN interfaces.
WAN Interface	Select a WAN interface through which to get DNS server addresses.
Use the following Static DNS IP address	Select this to have the Device use the DNS server addresses you configure manually.
First DNS Server	Enter the first DNS (Domain Name System) server IP address the Device passes to the DHCP clients.
Second DNS Server	Enter the second DNS (Domain Name System) server IP address the Device passes to the DHCP clients.
IGMP Snooping	
Enable IGMP Snooping	Select this option to enable IGMP snooping. This allows the Device to passively learn multicast group.
Standard Mode	Select this to have the 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 Device block all unknown multicast packets from the WAN.
IP Alias	
Enable IP Alias	Select the check box to configure another LAN network for the Device.
IP Address	Enter the IP address of your 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 Device.

6.4 The DHCP Client List Screen

Click **Network > LAN > DHCP Client List** to open the **DHCP Client List** screen. Use this screen to look at the IP addresses currently assigned to DHCP clients and the IP addresses reserved for specific MAC addresses.

Figure 36 Network > LAN > DHCP Client List



IP Address 0.0.0.0 MAC Address 00:00:00:00:00:00

#	IP Address	MAC Address	Add	Remove
0	192.168.1.99	00:A0:C5:01:23:45		□

The following table describes the fields in this screen.

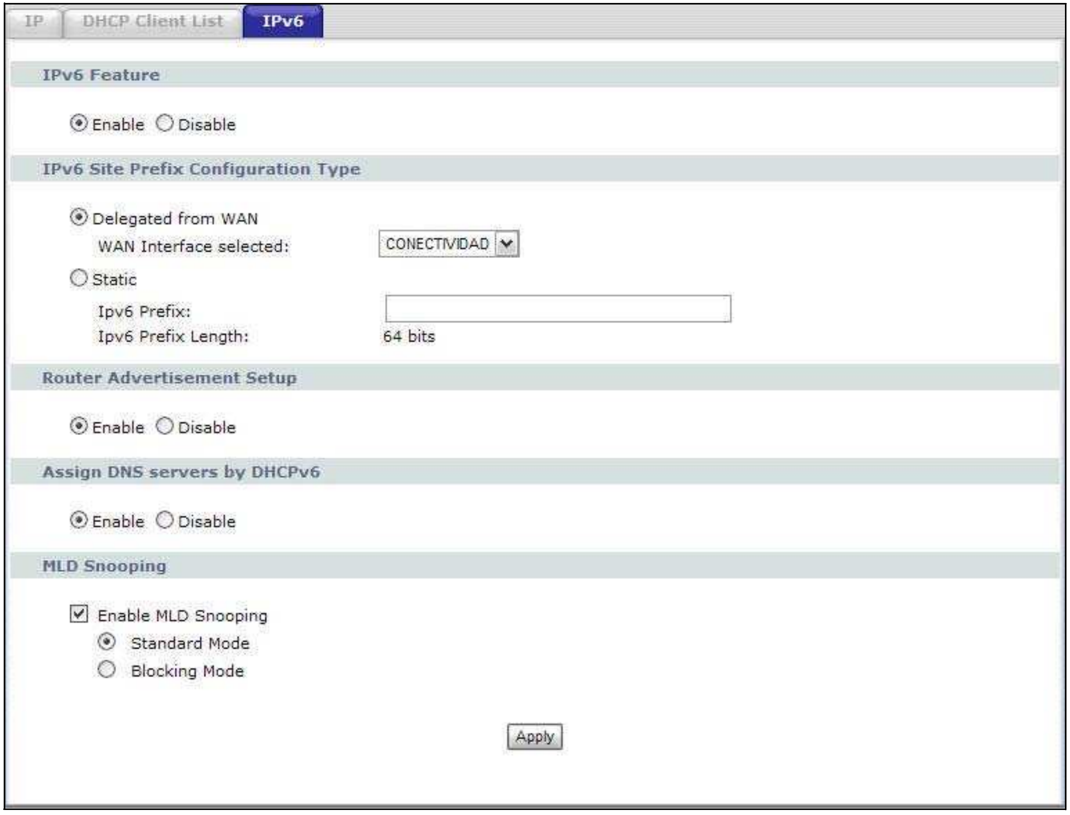
Table 30 Network > LAN > DHCP Client List

LABEL	DESCRIPTION
IP Address	Enter an IP address that you want to reserve for a specific device.
MAC Address	Enter an MAC address of a device on your LAN to which you want to assign the specified IP address.
Add Entries	Click this to add a entry that reserves the specified IP address for the device with the specified MAC address.
#	This field is a sequential value, and it is not associated with a specific entry.
IP Address	This field displays the IP address currently assigned to a DHCP client or reserved for a specific MAC address.
MAC Address	This field displays the MAC address to which the IP address is currently assigned or for which the IP address is reserved.
Add	This option is available for regular DHCP table entries. Select this to make a regular DHCP table entry into a static DHCP entry to always assign the listed IP address to the device with the specified MAC address. This field is blank for dynamic DHCP entries.
Remove	This is only available for static DHCP entries. If the static DHCP entry is for a device that is not connected, click **Remove** to delete the static DHCP entry. If the static DHCP entry is for a device that is connected, click **Remove** to change the static DHCP entry into a regular DHCP entry.

6.5 The IPv6 screen

Click **Network > LAN > IPv6** to open the **IPv6** screen. Use this screen to configure the IPv6 settings for your Device's LAN interface. See Appendix B on page 271 for background information about IPv6.

Figure 37 IPv6



IPv6 Feature

● Enable ○ Disable

IPv6 Site Prefix Configuration Type

● Delegated from WAN

WAN Interface selected: CONECTIVIDAD

○ Static

Ipv6 Prefix:

Ipv6 Prefix Length: 64 bits

Router Advertisement Setup

● Enable ○ Disable

Assign DNS servers by DHCPv6

● Enable ○ Disable

MLD Snooping

☑ Enable MLD Snooping

● Standard Mode

○ Blocking Mode

The following table describes the fields in this screen.

Table 31 IPv6

LABEL	DESCRIPTION
IPv6 Feature	Select **Enable** to activate IPv6. Select this option to enable IPv6 for this LAN connection.
IPv6 Site Prefix Configuration Type	Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. The Device uses the prefix to generate an IPv6 address.
Delegated from WAN	Select this option to automatically obtain an IPv6 network prefix from the service provider or an uplink router.
WAN Interface selected	Select a WAN interface through which you want to get an IPv6 network prefix. You should already have configured a WAN service with IPv6 enabled.
Static	Select this option to configure a fixed IPv6 network prefix for the Device's LAN interface.
IPv6 Prefix	Enter the IPv6 prefix that the Device uses to generate its LAN IPv6 address.

Table 31 IPv6

LABEL	DESCRIPTION
IPv6 Prefix Length	An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. This field displays the bit number of the IPv6 subnet mask.
Router Advertisement Setup	Select **Enable** to have the Device send router advertisement messages to the LAN hosts. Router advertisement is a response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters, such as IPv6 prefix and DNS information. Router solicitation is a request from a host to locate a router that can act as the default router and forward packets. Note: The LAN hosts neither generate global IPv6 addresses nor communicate with other networks if you disable this feature.
Assign DNS servers by DHCPv6	Select this option to have the Device act as a DHCP server to assign and pass DNS server information to its DHCP clients.
MLD Snooping	Select this option to activate MLD snooping on the Device. This allows the Device to check MLD packets passing through it and learn the multicast group membership. It helps reduce multicast traffic.
Standard Mode	Select this to have the 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 Device block all unknown multicast packets from the WAN.
Apply	Click **Apply** to save your changes back to the Device.

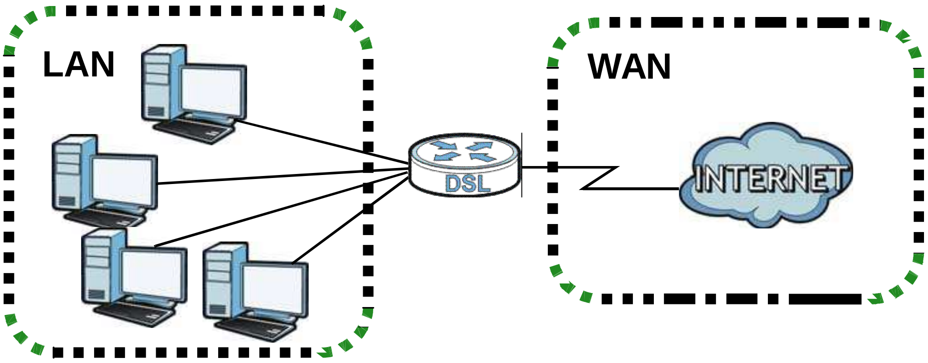
6.6 Technical Reference

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

LANs, WANs and the ZyXEL Device

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

Figure 38 LAN and WAN IP Addresses



DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the Device as a DHCP server or disable it. When configured as a server, the 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 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 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 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 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 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 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 Device supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the Device queries all directly connected networks to gather group membership. After that, the Device periodically updates this information. IP multicasting can be enabled/disabled on the Device LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

IP Alias

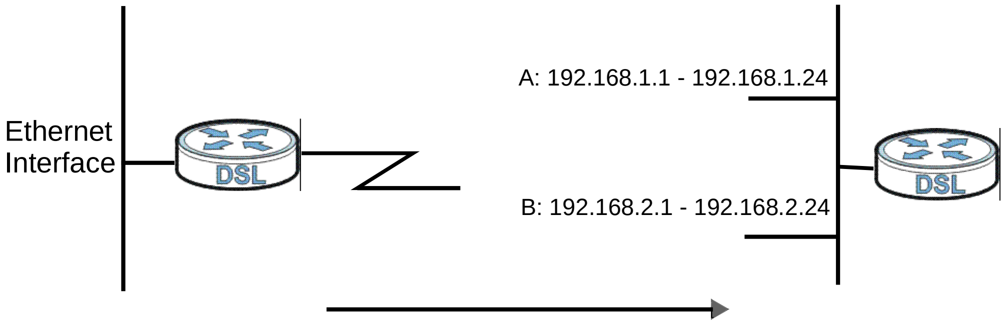
IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The Device supports three logical LAN interfaces via its single physical Ethernet interface with the Device itself as the gateway for each LAN network.

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 39 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 25 for a tutorial showing how to set up your wireless connection in an example scenario.

See Section 7.8 on page 141 for advanced technical information on wireless networks.

7.1.1 What You Can Do in this Chapter

This chapter describes the Device's **Network > Wireless LAN** screens. Use these screens to set up your 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 128). You can also configure the MAC filter to allow or block access to the Device based on the MAC addresses of the wireless stations.
- 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 7.5 on page 137) to enable or disable WPS, generate a security PIN (Personal Identification Number) and see information about the Device's WPS status.

  Use the **WPS Station** (see Section 7.6 on page 138) screen to set up WPS by pressing a button or using a PIN.
- The **Advanced Setup** screen lets you change the wireless mode, and make other advanced wireless configuration changes (Section 7.7 on page 139).

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 126 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.

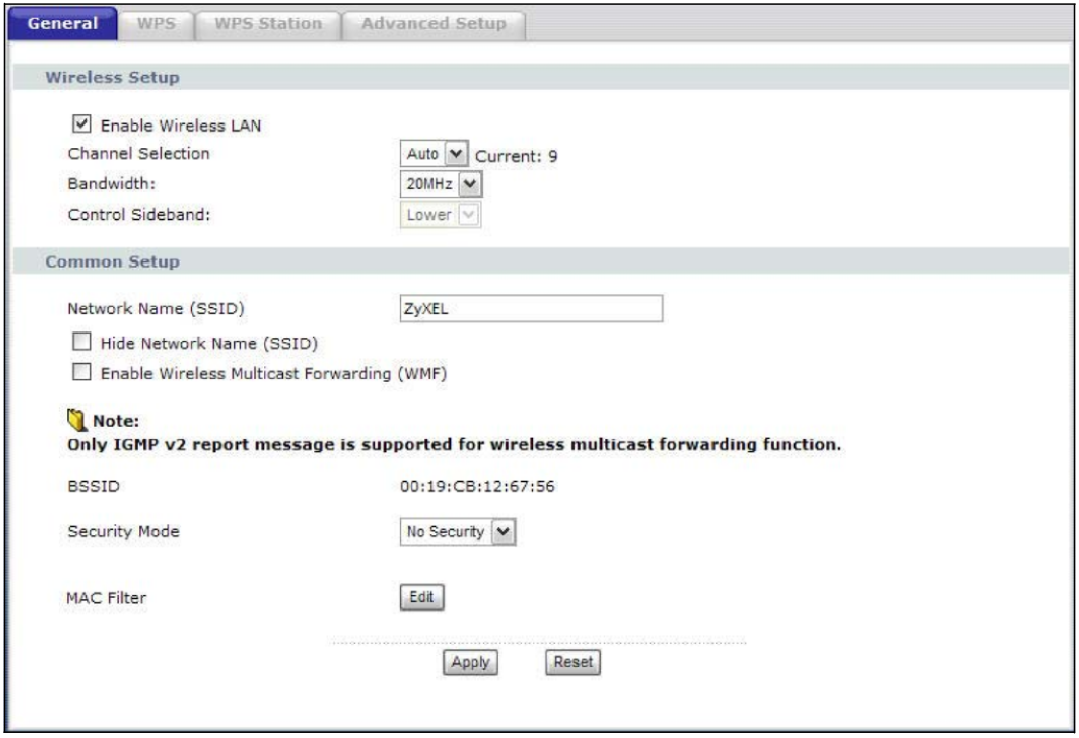
  Even if some of your devices support WPS and some do not, you can use WPS to set up your network and then add the non-WPS devices manually, although this is somewhat more complicated to do.
- What advanced options do you want to configure, if any? If you want to configure advanced options, ensure that 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 Device from a computer connected to the wireless LAN and you change the 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 Device's new settings.

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

Figure 40 Network > Wireless LAN > General



☑ Enable Wireless LAN
Channel Selection: Auto Current: 9
Bandwidth: 20MHz
Control Sideband: Lower

Network Name (SSID): ZyXEL
☐ Hide Network Name (SSID)
☐ Enable Wireless Multicast Forwarding (WMF)

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

BSSID: 00:19:CB:12:67:56
Security Mode: No Security

The following table describes the labels in this screen.

Table 32 Network > Wireless LAN > General

LABEL	DESCRIPTION
Enable 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 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 Device is currently using then displays next to this field.
Bandwidth	Select whether the 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 Device from a computer connected to the wireless LAN and you change the 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 Device's new settings.
Auto Generate Key	This is available when you use WEP or WPA(2)-PSK security. Select this option to have the Device generate the wireless security key automatically.
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 Device to transmit wireless multicast traffic.
BSSID	This shows the MAC address of the wireless interface on the 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 Device using this SSID.

Table 32 Network > Wireless LAN > General

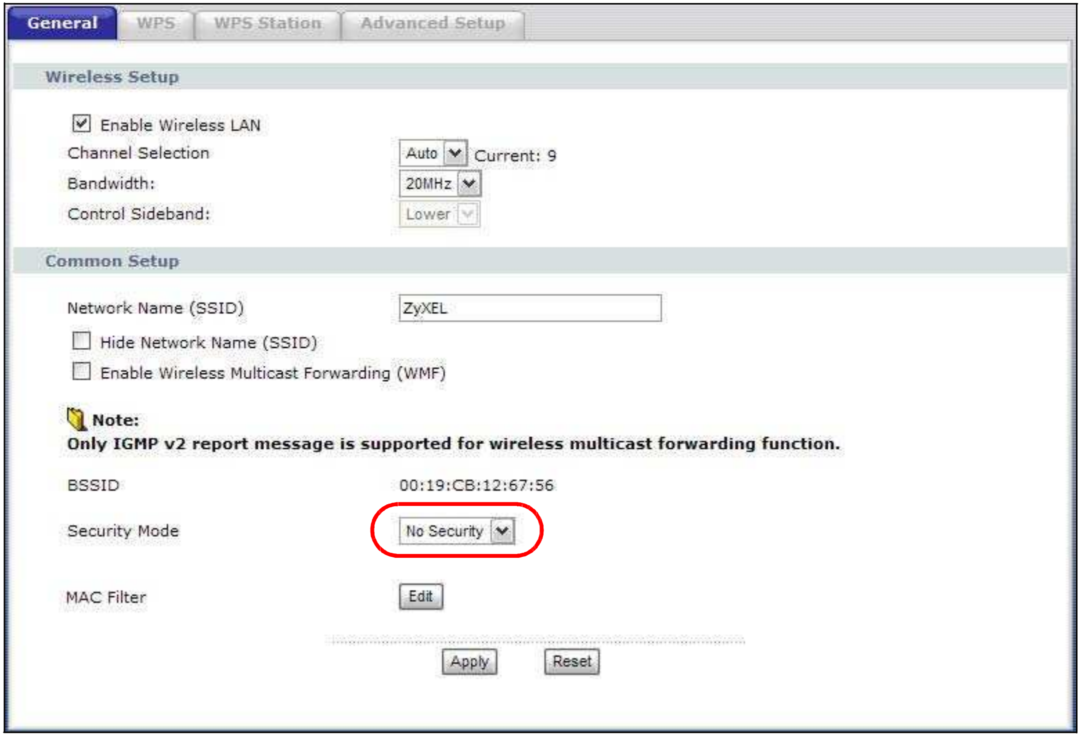
LABEL	DESCRIPTION
Apply	Click this to save your changes back to the Device.
Reset	Click this to reload the previous configuration for this screen.

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 Device, your network is accessible to any wireless networking device that is within range.

Figure 41 Wireless LAN > General: No Security



Wireless Setup

☑ Enable Wireless LAN

Channel Selection: Auto Current: 9

Bandwidth: 20MHz

Control Sideband: Lower

Common Setup

Network Name (SSID): ZyXEL

□ Hide Network Name (SSID)

□ Enable Wireless Multicast Forwarding (WMF)

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

BSSID: 00:19:CB:12:67:56

Security Mode: No Security

MAC Filter: Edit

The following table describes the labels in this screen.

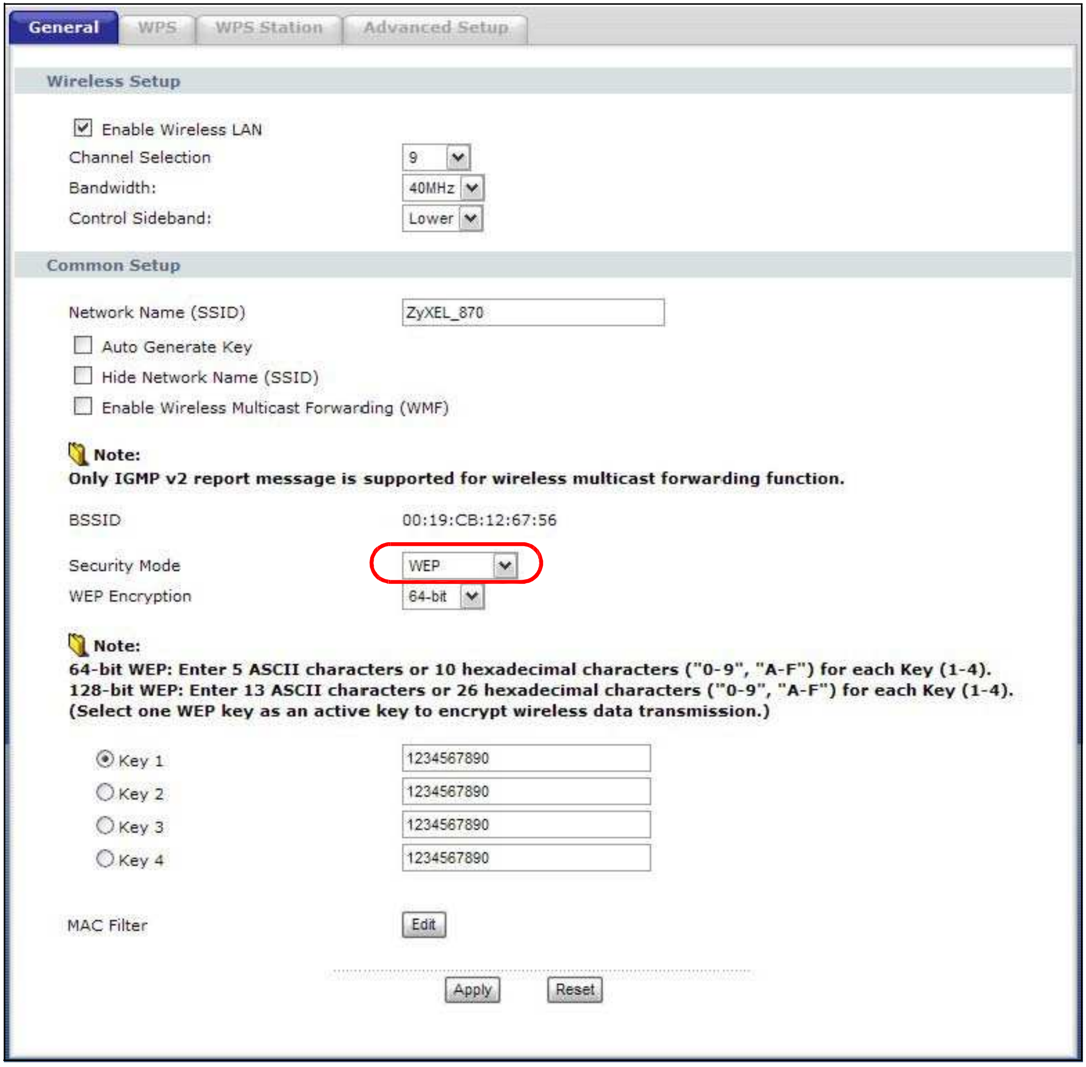
Table 33 Wireless LAN > General: No Security

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 42 Wireless LAN > General: Static WEP Encryption



Wireless Setup

☑ Enable Wireless LAN

Channel Selection: 9

Bandwidth: 40MHz

Control Sideband: Lower

Common Setup

Network Name (SSID): ZyXEL_870

□ Auto Generate Key

□ Hide Network Name (SSID)

□ Enable Wireless Multicast Forwarding (WMF)

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

BSSID: 00:19:CB:12:67:56

Security Mode: WEP

WEP Encryption: 64-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: 1234567890

○ Key 2: 1234567890

○ Key 3: 1234567890

○ Key 4: 1234567890

MAC Filter

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

Table 34 Network > Wireless LAN > General: Static WEP Encryption

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

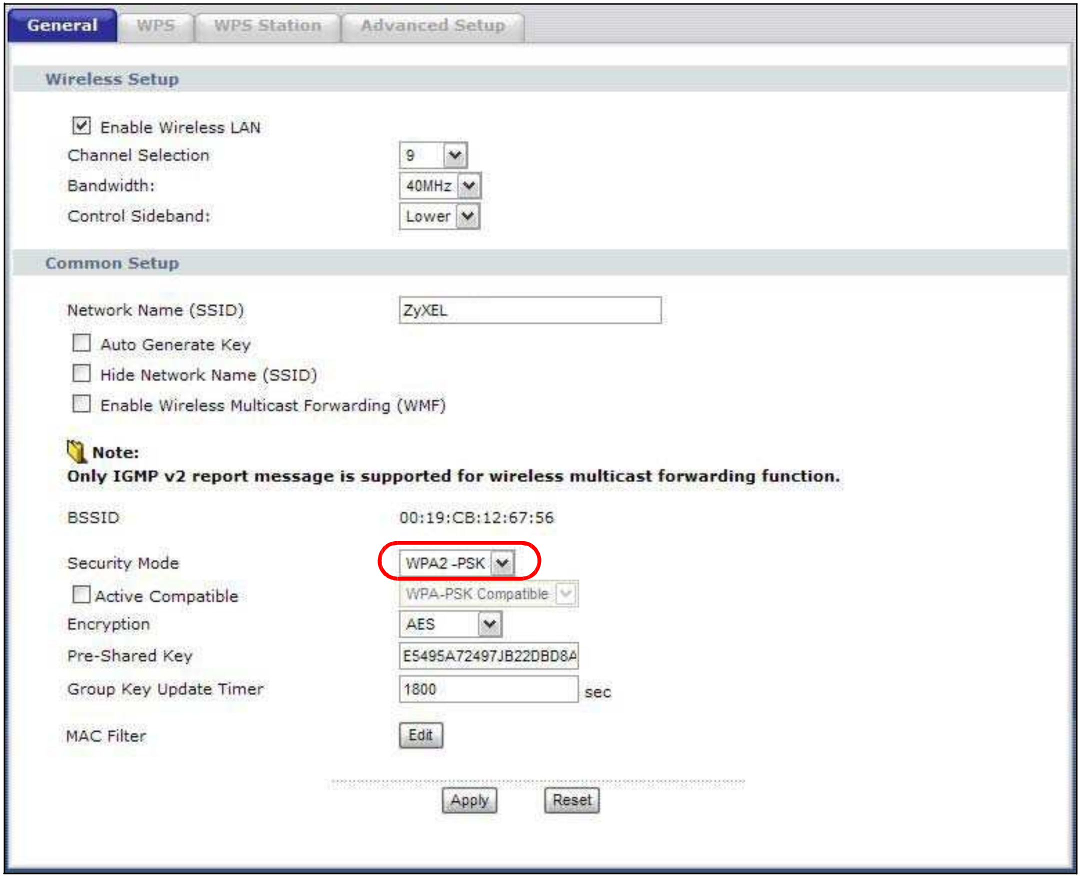
Table 34 Network > Wireless LAN > General: Static WEP Encryption

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** or **128-bit** 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 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** 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** 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 43 Wireless LAN > General: WPA(2)-PSK



Wireless Setup

☑ Enable Wireless LAN

Channel Selection: 9

Bandwidth: 40MHz

Control Sideband: Lower

Common Setup

Network Name (SSID): ZyXEL

☐ Auto Generate Key

☐ Hide Network Name (SSID)

☐ Enable Wireless Multicast Forwarding (WMF)

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

BSSID: 00:19:CB:12:67:56

Security Mode: WPA2 -PSK

☐ Active Compatible: WPA-PSK Compatible

Encryption: AES

Pre-Shared Key: E5495A72497JB22DBD8A

Group Key Update Timer: 1800 sec

MAC Filter: Edit

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

Table 35 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 Device to support WPA-PSK and WPA2-PSK simultaneously.
Encryption	Select the encryption type (**AES** or **TKIP+AES**) for data encryption. 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 Device default is **1800** seconds (30 minutes).

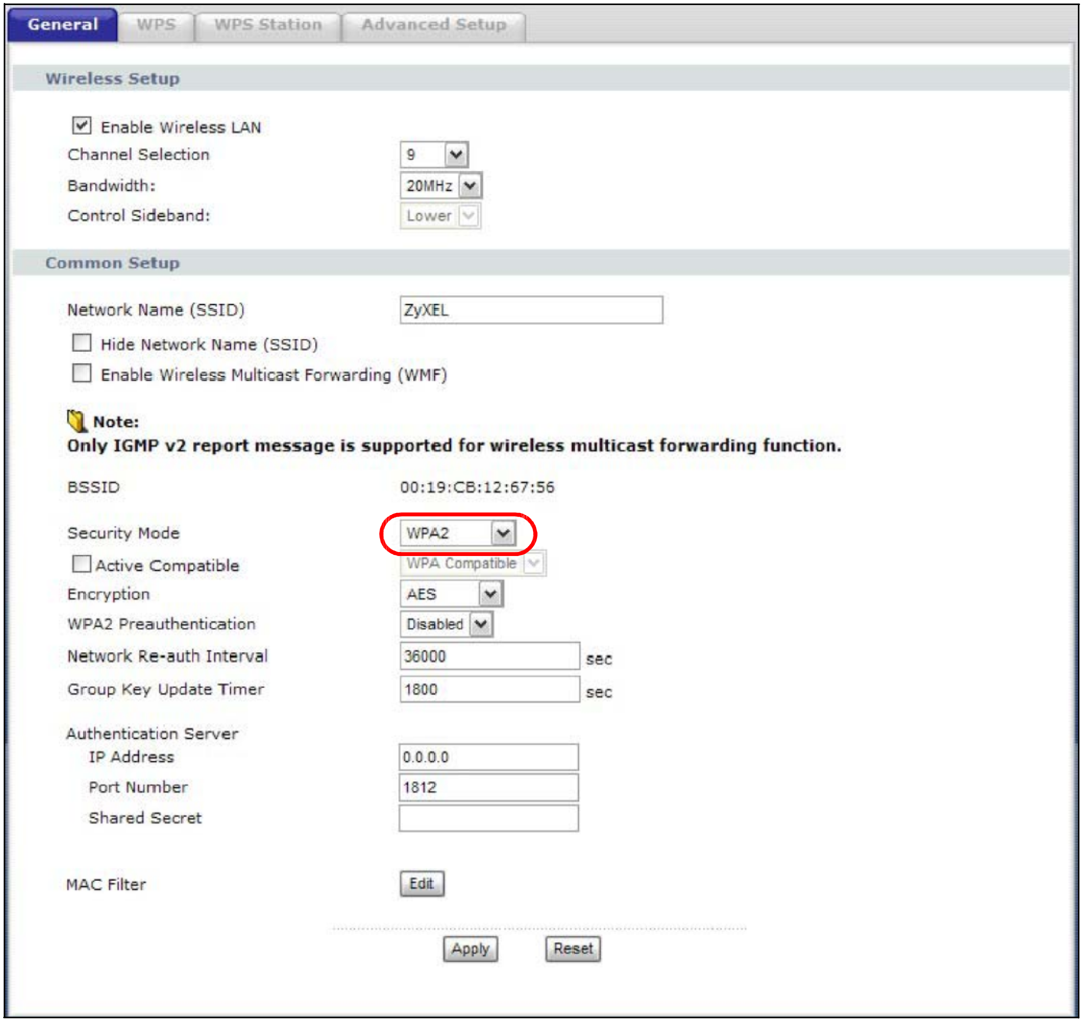
7.4.4 WPA(2) Authentication

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.

Note: WPA or WPA2 is not available if you enable WPS before you configure WPA or WPA2 in the **Wireless LAN** > **General** screen.

Note: If you select **WPA** or **WPA2** in the **Wireless LAN > General** screen, the WPS feature is not available on the Device.

Figure 44 Wireless LAN > General: WPA(2)



Wireless Setup

☑ Enable Wireless LAN

Channel Selection: 9

Bandwidth: 20MHz

Control Sideband: Lower

Common Setup

Network Name (SSID): ZyXEL

☐ Hide Network Name (SSID)

☐ Enable Wireless Multicast Forwarding (WMF)

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

BSSID: 00:19:CB:12:67:56

Security Mode: WPA2

☐ Active Compatible: WPA Compatible

Encryption: AES

WPA2 Preauthentication: Disabled

Network Re-auth Interval: 36000 sec

Group Key Update Timer: 1800 sec

Authentication Server

IP Address: 0.0.0.0

Port Number: 1812

Shared Secret:

MAC Filter

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

Table 36 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 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 36 Wireless LAN > General: WPA(2)

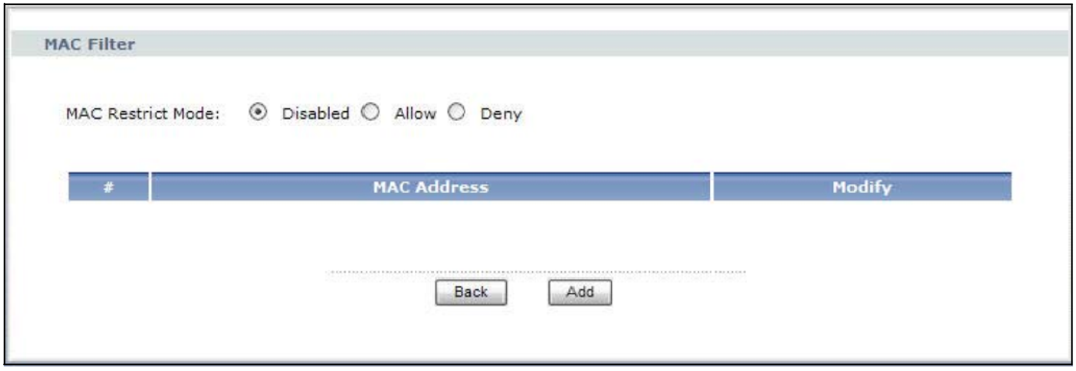
LABEL	DESCRIPTION
WPA2 Preauthentication	This field is available only when you select **WPA2**. Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it. Select **Enabled** to turn 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 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 Device. The key must be the same on the external authentication server and your Device. The key is not sent over the network.

7.4.5 MAC Filter

This screen allows you to configure the Device to give exclusive access to specific devices (**Allow**) or exclude specific devices from accessing the 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 Device's MAC filter settings. Click the **Edit** button in the **Wireless LAN > General** screen. The following screen displays.

Figure 45 Wireless LAN > MAC Filter



MAC Filter

MAC Restrict Mode: ● Disabled ○ Allow ○ Deny

#	MAC Address	Modify

Back Add

The following table describes the labels in this screen.

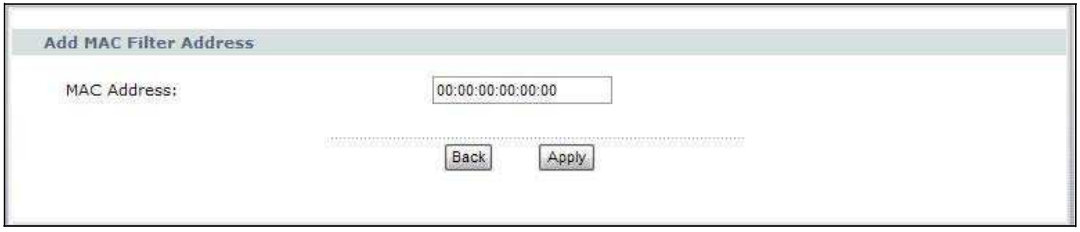
Table 37 Wireless LAN > MAC Filter

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 Device, MAC addresses not listed will be denied access to the Device. Select **Deny** to block access to the Device, MAC addresses not listed will be allowed to access the 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 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 46 Wireless LAN > MAC Filter > Add



Add MAC Filter Address

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

Back Apply

The following table describes the labels in this screen.

Table 38 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 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.

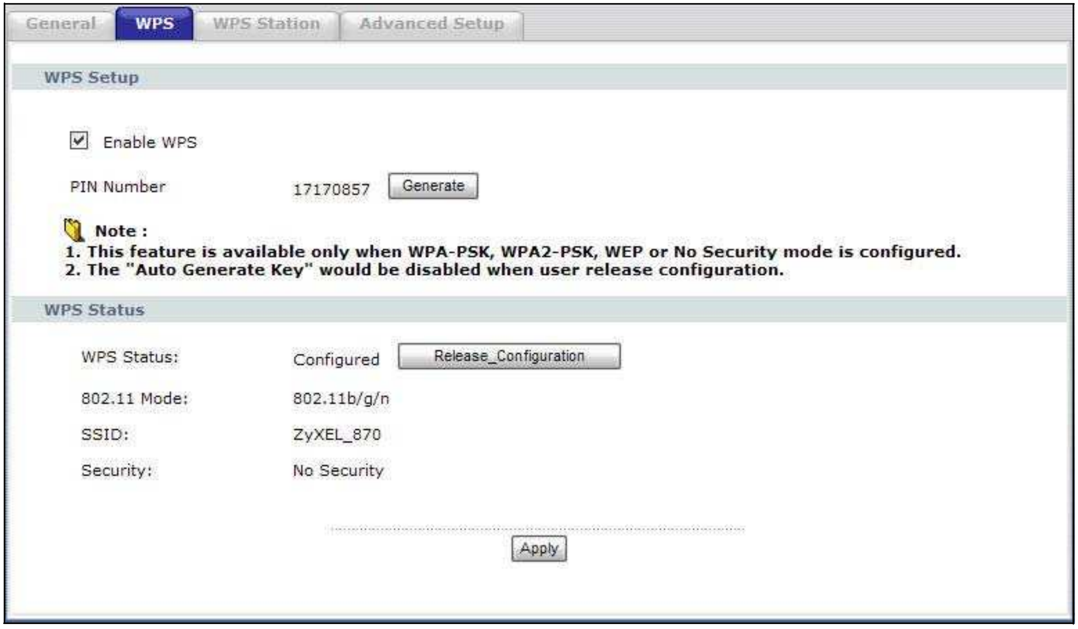
7.5 The WPS Screen

Use this screen to configure WiFi Protected Setup (WPS) on your 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 47 Network > Wireless LAN > WPS



☑ Enable WPS

PIN Number 17170857

Note :
1. This feature is available only when WPA-PSK, WPA2-PSK, WEP or No Security mode is configured.
2. The "Auto Generate Key" would be disabled when user release configuration.

WPS Status:	Configured
802.11 Mode:	802.11b/g/n
SSID:	ZyXEL_870
Security:	No Security

The following table describes the labels in this screen.

Table 39 Network > Wireless LAN > WPS

LABEL	DESCRIPTION
WPS Setup	
Enable WPS	Select the check box to activate WPS on the Device.

Table 39 Network > Wireless LAN > WPS

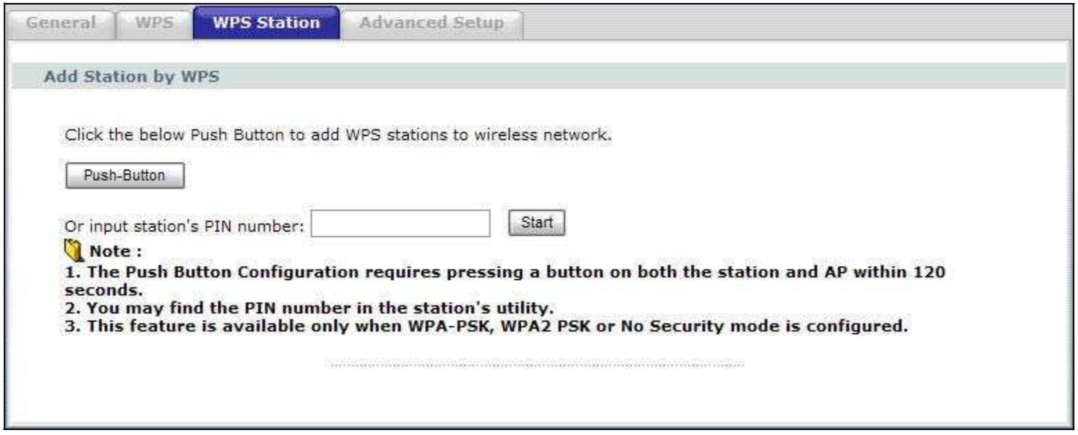
LABEL	DESCRIPTION
PIN Number	This shows the PIN (Personal Identification Number) of the Device. Enter this PIN in the configuration utility of the device you want to connect to using WPS. The PIN is not necessary when you use WPS push-button method.
Generate	Click this button to have the Device create a new PIN.
WPS Status	This displays **Configured** when the 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 Device or you click **Release_Configuration** to remove the configured wireless and wireless security settings.
Release_Configuration	This button is available when the WPS status is **Configured** but not configurable if you disable WPS. Click this button to remove all configured wireless and wireless security settings for WPS connections on the Device.
Apply	Click **Apply** to save your changes back to the Device.

7.6 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 48 Network > Wireless LAN > WPS Station



Add Station by WPS

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.

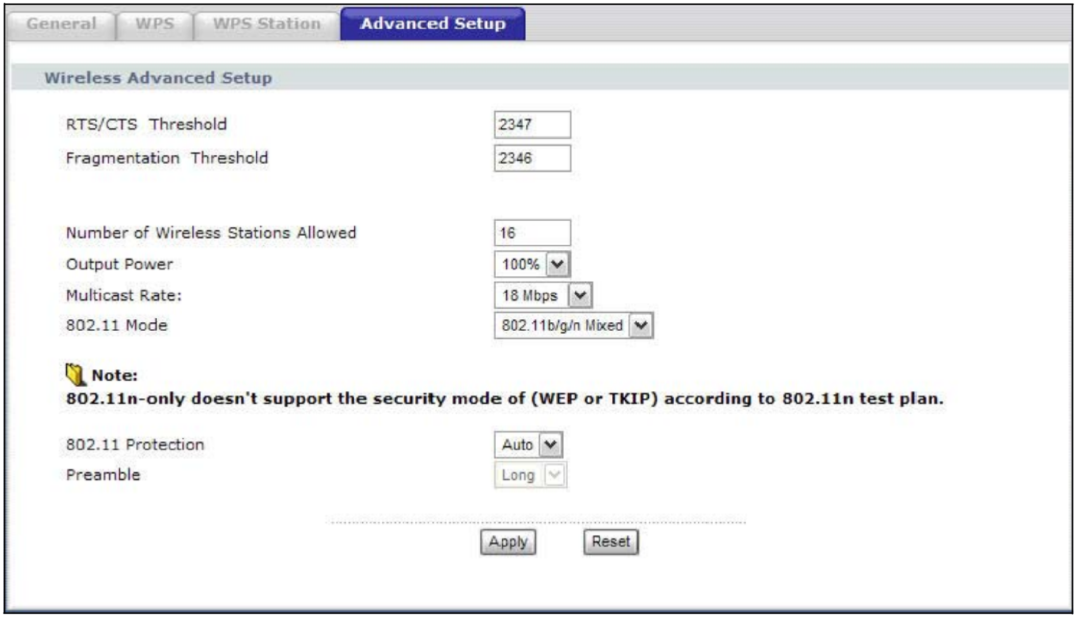
Table 40 Network > Wireless LAN > WPS Station

LABEL	DESCRIPTION
Push Button	Click this button to add another WPS-enabled wireless device (within wireless range of the 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 Device.

7.7 The Advanced Setup Screen

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

Figure 49 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/n Mixed

Note:
802.11n-only doesn't support the security mode of (WEP or TKIP) according to 802.11n test plan.

802.11 Protection: Auto

Preamble: Long

The following table describes the labels in this screen.

Table 41 Wireless LAN > Advanced Setup

LABEL	DESCRIPTION
RTS/CTS Threshold	Enter a value between 0 and 2347.
Fragmentation Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2346.
Number of Wireless Stations Allowed	Specify the maximum number (from 1 to 64) of the wireless stations that may connect to the Device.
Output Power	Set the output power of the 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 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 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 Device. IEEE 802.11b compliant WLAN devices can associate with the 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 Device. This can increase transmission rates, although IEEE 802.11b or IEEE 802.11g clients will not be able to connect to the Device. If you select **802.11 Only**, WEP and TKIP security modes are not supported. Select **802.11b/g Mixed** to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the Device. The Device adjusts the transmission rate automatically according to the wireless standard supported by the wireless devices. Select **802.11 b/g/n Mixed** to allow both IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the Device. The transmission rate of your 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 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**.
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 Device uses **Short** when you set **802.11 Mode** to **802.11g Only**. This field is not configurable and the Device uses **Long** when you set **802.11 Mode** to **802.11n Only** or **802.11 b/g/n Mixed**.
Apply	Click this to save your changes back to the Device.
Reset	Click this to reload the previous configuration for this screen.

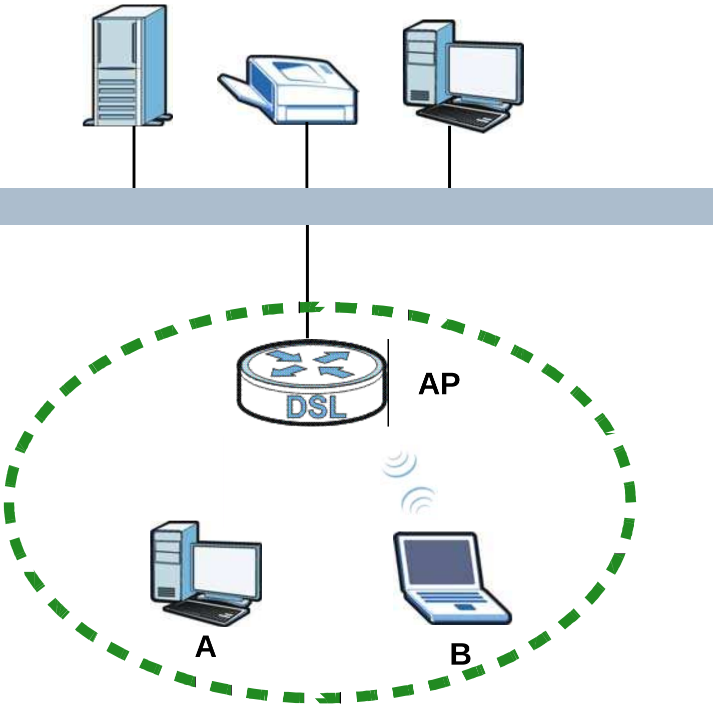
7.8 Technical Reference

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

7.8.1 Wireless Network Overview

The following figure provides an example of a wireless network.

Figure 50 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 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.

7.8.2 Additional Wireless Terms

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

Table 42 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 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 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 Device does, it cannot communicate with the 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.

7.8.3 Wireless Security Overview

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

7.8.3.1 SSID

Normally, the Device acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the 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.

7.8.3.2 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 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

[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.

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.

7.8.3.3 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.

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.

7.8.3.4 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 7.8.3.3 on page 143 for information about this.)

Table 43 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 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 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 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.

7.8.4 WiFi Protected Setup

Your 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.

7.8.4.1 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 Device, see Section 7.6 on page 138).

3 Press the button on one of the devices (it doesn't matter which). For the 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.

7.8.4.2 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 Device, see Section 7.5 on page 137).

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.

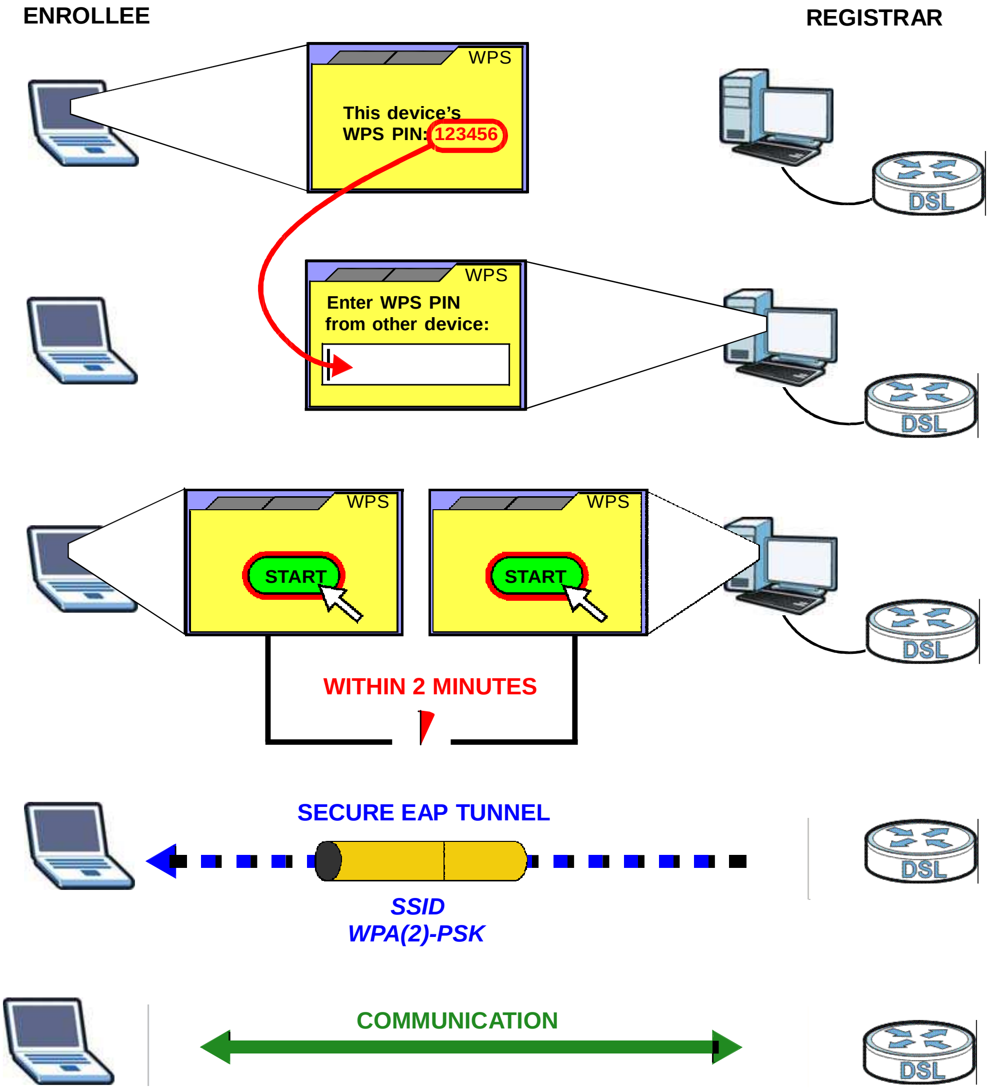
Note: Use the configuration utility to activate WPS, not the push-button on the device itself.

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 51 Example WPS Process: PIN Method

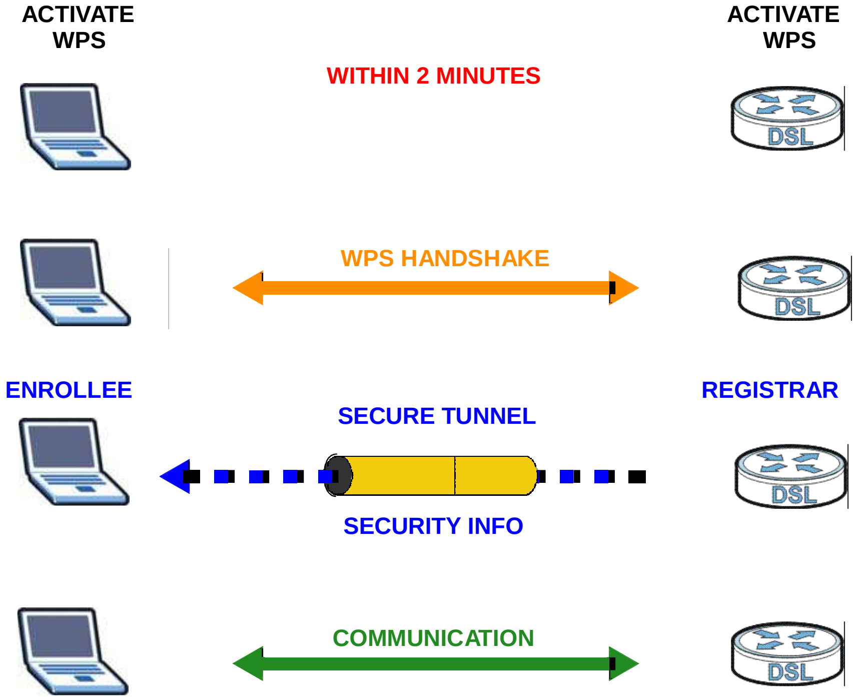


7.8.4.3 How WPS Works

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 52 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.

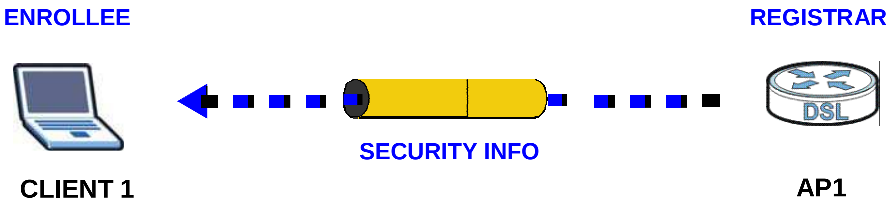
By default, a WPS devices is "unconfigured". This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled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

7.8.4.4 Example WPS Network Setup

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

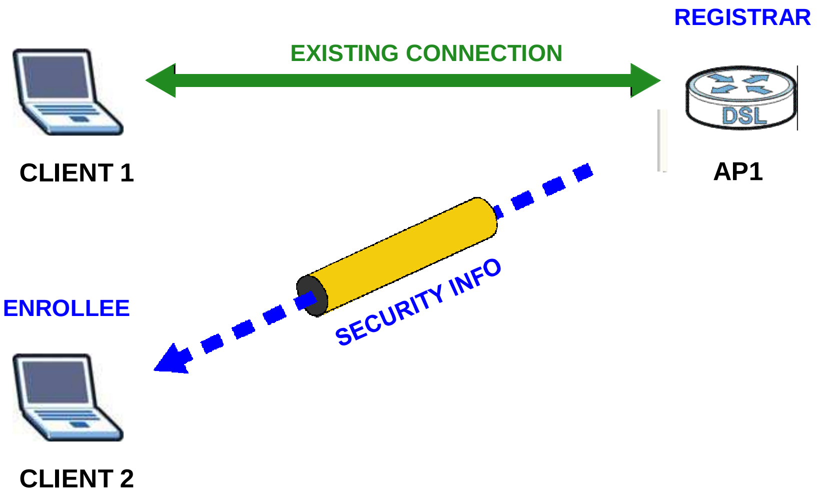
The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information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

Figure 53 WPS: Example Network Step 1



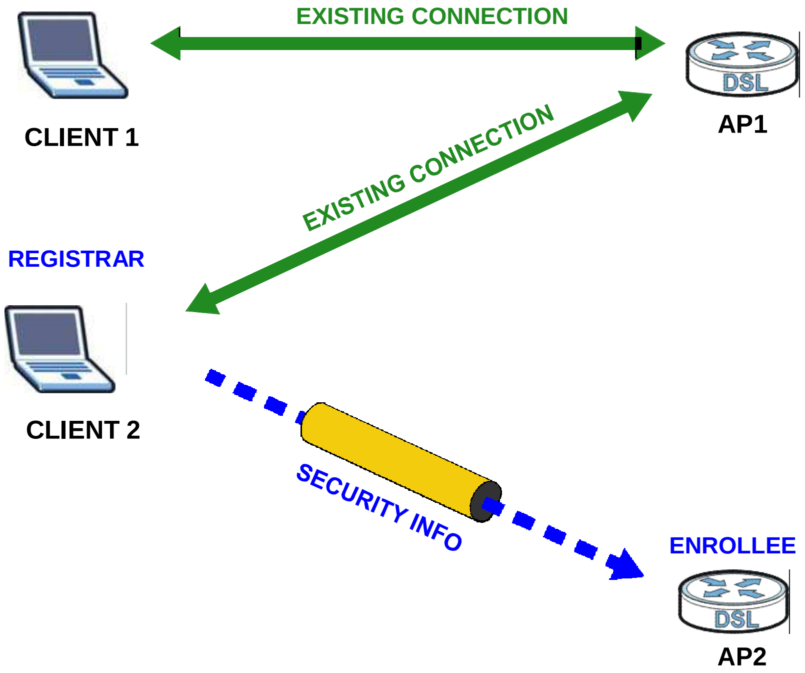
In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the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

Figure 54 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 55 WPS: Example Network Step 3



7.8.4.5 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.

Network Address Translation (NAT)

8.1 Overview

This chapter discusses how to configure NAT on the 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 151).
- The **DMZ Host** screen lets you configure a default server (Section 8.4 on page 155).
- The **ALG** screen lets you enable SIP ALG on the Device (Section 8.5 on page 155).

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

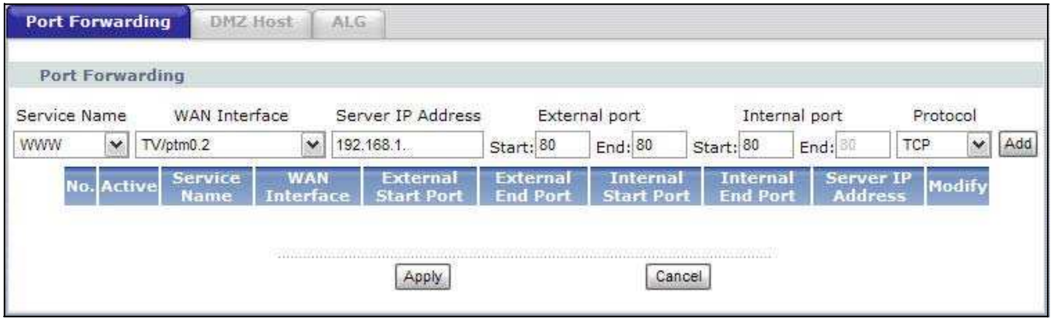
This summary screen provides a summary of all port forwarding rules and their configuration. In addition, this screen allows you to create new port forwarding rules and delete existing rules.

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 56 NAT Port Forwarding



Port Forwarding

Service Name	WAN Interface	Server IP Address	External port		Internal port		Protocol
WWW	TV/ptm0.2	192.168.1.	Start: 80	End: 80	Start: 80	End: 80	TCP

No.	Active	Service Name	WAN Interface	External Start Port	External End Port	Internal Start Port	Internal End Port	Server IP Address	Modify

The following table describes the labels in this screen.

Table 44 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.

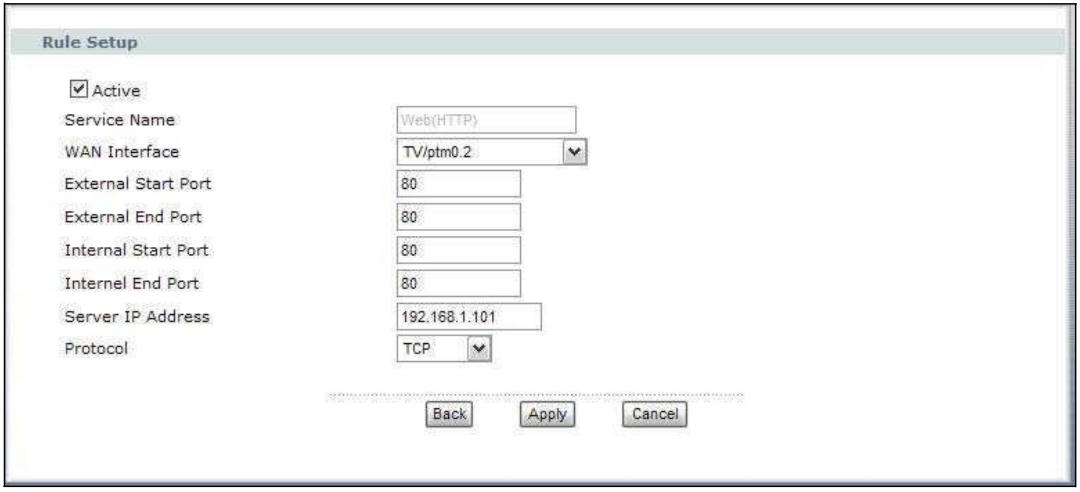
Table 44 NAT Port Forwarding (continued)

LABEL	DESCRIPTION
Internal Port Start	Enter the port number to which you want the 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.
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 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 57 Port Forwarding Edit



Rule Setup

☑ Active

Service Name: Web(HTTP)

WAN Interface: TV/ptm0.2

External Start Port: 80

External End Port: 80

Internal Start Port: 80

Internel End Port: 80

Server IP Address: 192.168.1.101

Protocol: TCP

The following table describes the labels in this screen.

Table 45 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 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.

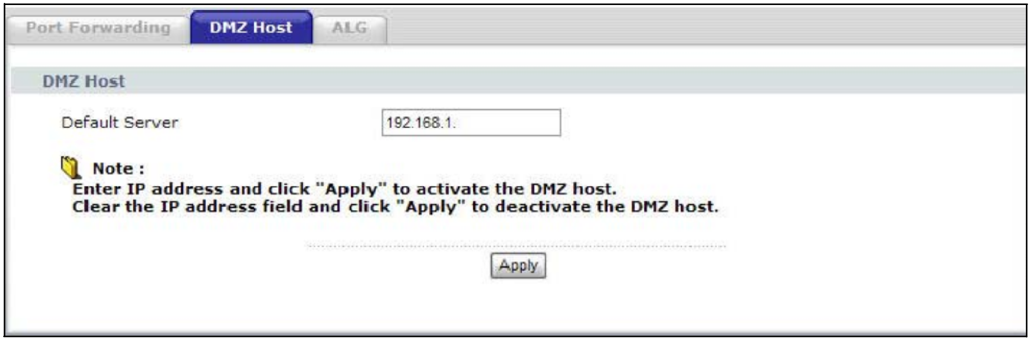
Table 45 Port Forwarding Edit (continued)

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

8.4 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 58 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.

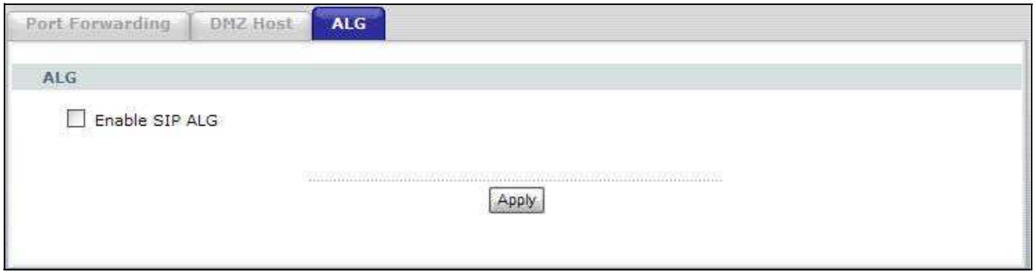
Table 46 NAT > DMZ Host

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 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 Device.

8.5 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 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 Device. To access this screen, click **NAT > ALG**.



ALG

□ Enable SIP ALG

Figure 59 NAT > ALG

Each field is described in the following table.

Table 47 NAT > ALG

LABEL	DESCRIPTION
Enable SIP ALG	Select this check box to allow SIP sessions to pass through the 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.

8.6 Technical Reference

The following section contains additional technical information about the 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.

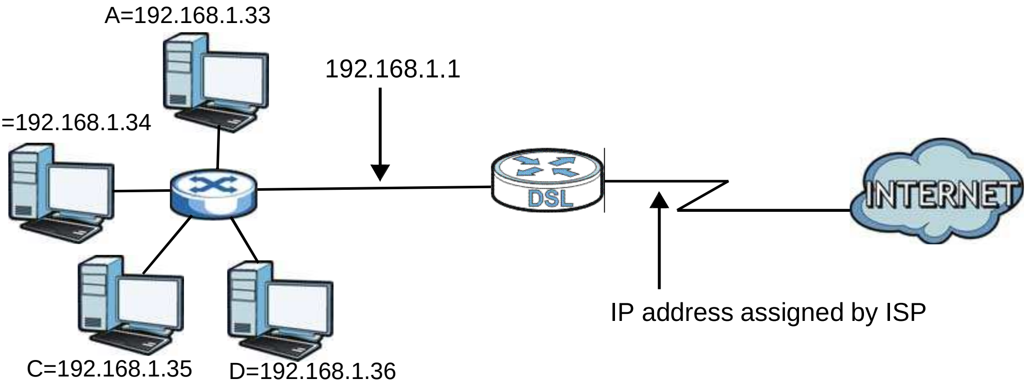
Table 48 Services and Port Numbers

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

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 60 Multiple Servers Behind NAT Example



9

Firewall

9.1 Overview

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

The 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.

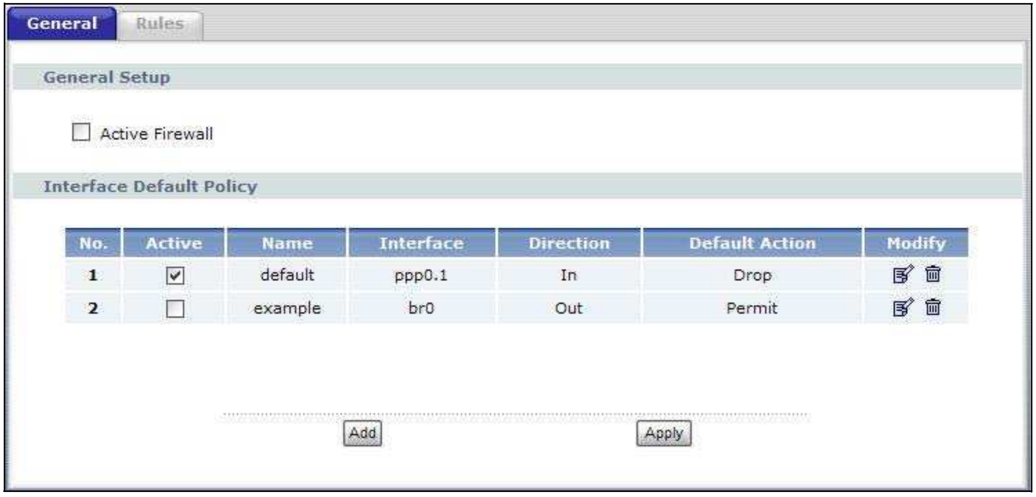
9.1.1 What You Can Do in this Chapter

- Use the **General** screen (Section 9.2 on page 159) to enable firewall on the Device, and set the default action that the firewall takes on packets that do not match any of the firewall rules.
- Use the **Rules** screen (Section 9.3 on page 161) to view the configured firewall rules and add, edit or remove a firewall rule.

9.2 The Firewall General Screen

Click **Security > Firewall** to display the following screen. Activate the firewall by selecting the **Active Firewall** check box as seen in the following screen.

Figure 61 Security > Firewall > General



General Setup

□ Active Firewall

Interface Default Policy

No.	Active	Name	Interface	Direction	Default Action	Modify
1	☑	default	ppp0.1	In	Drop	✎ 🗑
2	□	example	br0	Out	Permit	✎ 🗑

The following table describes the labels in this screen.

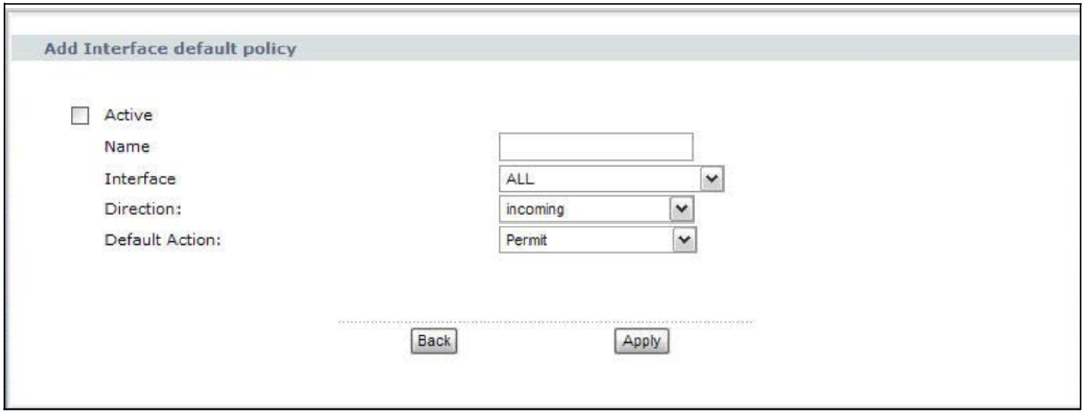
Table 49 Security > Firewall > General

LABEL	DESCRIPTION
Active Firewall	Select this check box to activate the firewall. The Device performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
No.	This displays the index number of the default firewall policy.
Active	This field displays whether a policy is turned on or not. Select the check box to enable the policy. Clear the check box to disable the policy.
Name	This displays the name of the policy.
Interface	This displays the LAN or WAN interface(s) to which this policy is applied.
Direction	This displays the direction of travel of packets (**In** and **Out**). Firewall rules are grouped based on the direction of travel of packets to which they apply.
Default Action	This displays the default action that the firewall is to take on packets that are traveling in the selected direction and do not match any of the firewall rules. **Drop**: the Device silently discards the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender. **Permit**: the Device allows the passage of the packets.
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 policy.
Apply	Click **Apply** to save your changes back to the Device.

9.2.1 Default Policy Configuration

In the **Firewall > General** screen, click **Add** or click an entry's **Edit** icon to configure a firewall policy.

Figure 62 Security > Firewall > General: Add



Add Interface default policy

☐ Active

Name	
Interface	ALL
Direction:	incoming
Default Action:	Permit

The following table describes the labels in this screen.

Table 50 Security > Firewall > General: Add

LABEL	DESCRIPTION
Active	Select this check box to enable the rule.
Name	Enter a descriptive name of up to 16 printable English keyboard characters.
Interface	Select **All** to apply the policy to all interfaces on the Device or select the specific LAN or WAN interface to which this policy applies.
Direction	Specify the direction of travel of packets (**incoming** or **outgoing**) in this policy.
Default Action	Specify whether the firewall silently discards packets (**Drop**) or allows the passage of packets (**Permit**).
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your customized settings and exit this screen.

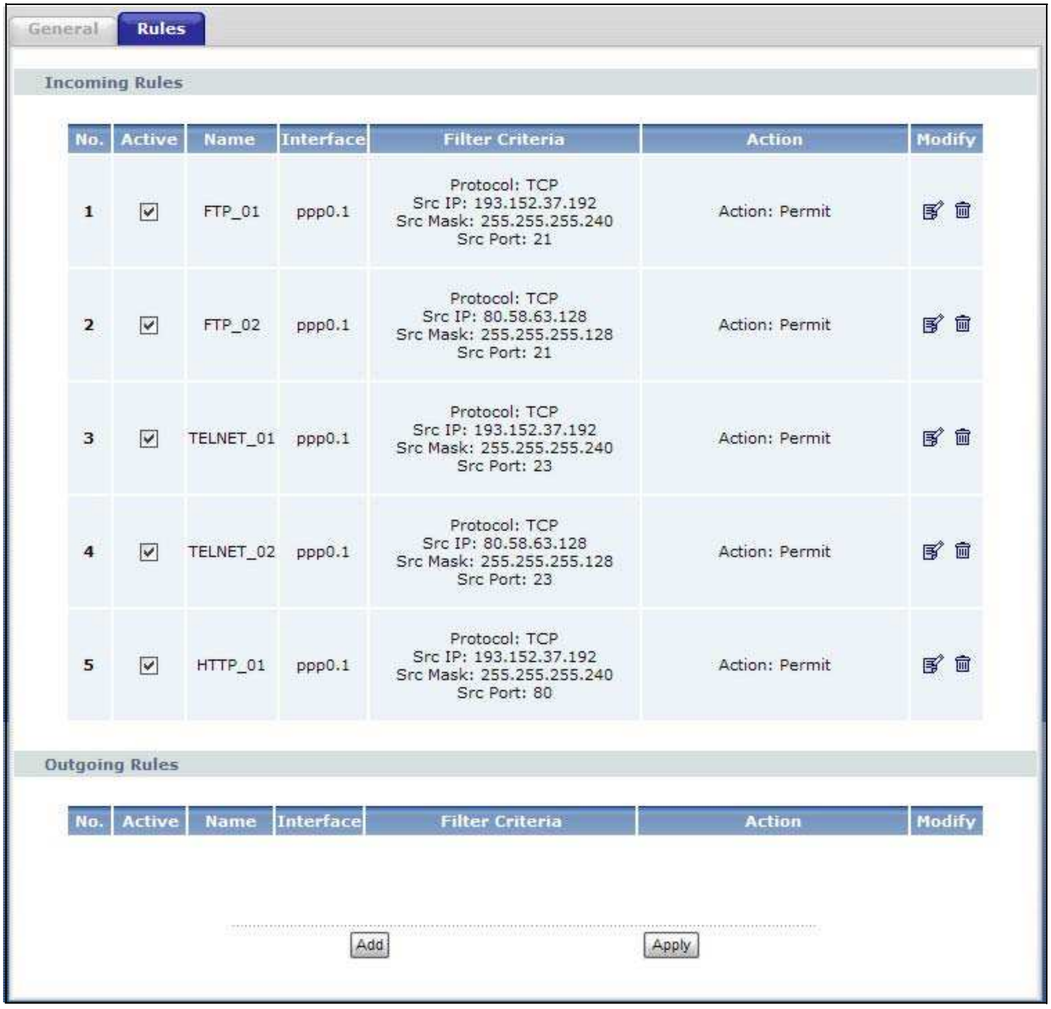
9.3 The Firewall Rules Screen

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

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

Note: The firewall rules that you configure here take priority over the general firewall action settings in the **General** screen.

Figure 63 Security > Firewall > Rules



Incoming Rules

No.	Active	Name	Interface	Filter Criteria	Action	Modify
1	☑	FTP_01	ppp0.1	Protocol: TCP Src IP: 193.152.37.192 Src Mask: 255.255.255.240 Src Port: 21	Action: Permit	✎ 🗑
2	☑	FTP_02	ppp0.1	Protocol: TCP Src IP: 80.58.63.128 Src Mask: 255.255.255.128 Src Port: 21	Action: Permit	✎ 🗑
3	☑	TELNET_01	ppp0.1	Protocol: TCP Src IP: 193.152.37.192 Src Mask: 255.255.255.240 Src Port: 23	Action: Permit	✎ 🗑
4	☑	TELNET_02	ppp0.1	Protocol: TCP Src IP: 80.58.63.128 Src Mask: 255.255.255.128 Src Port: 23	Action: Permit	✎ 🗑
5	☑	HTTP_01	ppp0.1	Protocol: TCP Src IP: 193.152.37.192 Src Mask: 255.255.255.240 Src Port: 80	Action: Permit	✎ 🗑

Outgoing Rules

No.	Active	Name	Interface	Filter Criteria	Action	Modify

The following table describes the labels in this screen.

Table 51 Security > Firewall > Rules

LABEL	DESCRIPTION
Incoming/ Outgoing Rules	The following fields summarize the rules you have created that apply to traffic traveling in the selected packet direction.
No.	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.
Active	This field displays whether a firewall rule is turned on or not. Select the check box to enable the rule. Clear the check box to disable the rule.
Name	This displays the name of the rule.
Interface	This displays the LAN or WAN interface(s) to which this rule is applied.
Filter Criteria	This displays the filtering criteria, such as the source or destination IP addresses and subnet mask to which this rule applies.

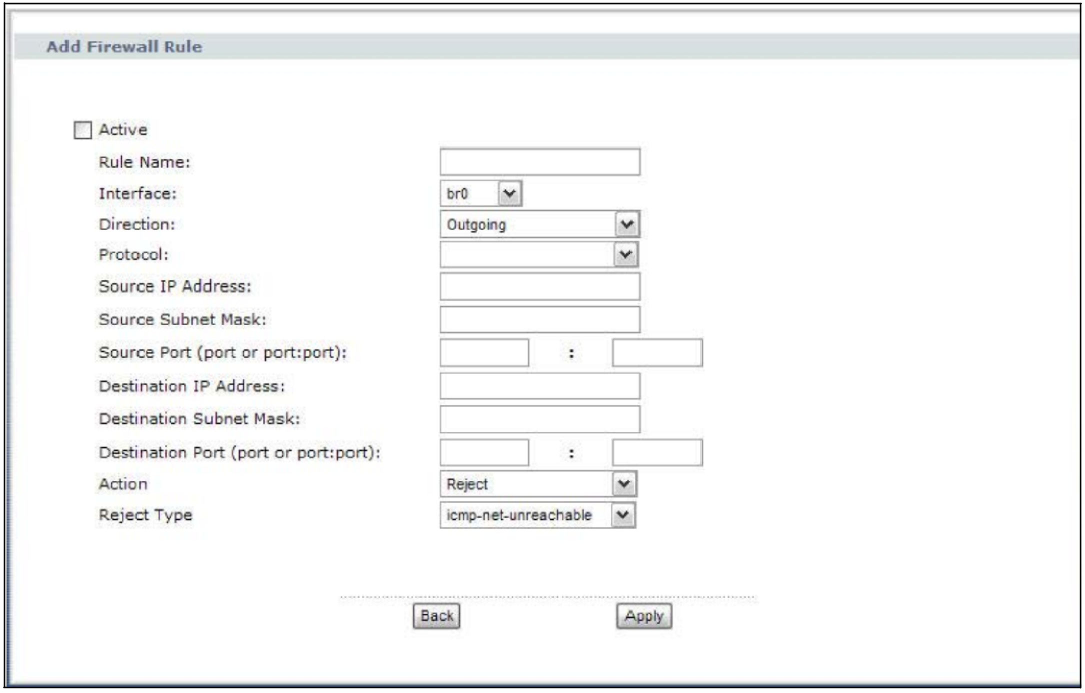
Table 51 Security > Firewall > Rules (continued)

LABEL	DESCRIPTION
Action	This displays whether the firewall silently discards packets (**Drop**), discards packets and sends an ICMP message to the sender (**Reject**) or allows the passage of packets (**Permit**).
Modify	Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Remove** icon to delete an existing firewall rule. A window displays asking you to confirm that you want to delete the firewall rule. Note that subsequent firewall rules move up by one when you take this action.
Add	Click **Add** to create a new firewall rule.
Apply	Click **Apply** to save your changes back to the Device.

9.3.1 Firewall Rules Configuration

In the **Firewall > Rules** screen, click **Add** or click a rule's **Edit** icon to display this screen and refer to the following table for information on the labels.

Figure 64 Security > Firewall > Rules: Add



Add Firewall Rule

□ Active

Rule Name:

Interface: br0

Direction: Outgoing

Protocol:

Source IP Address:

Source Subnet Mask:

Source Port (port or port:port): :

Destination IP Address:

Destination Subnet Mask:

Destination Port (port or port:port): :

Action: Reject

Reject Type: icmp-net-unreachable

The following table describes the labels in this screen.

Table 52 Security > Firewall > Rules: Add

LABEL	DESCRIPTION
Active	Select this check box to enable the rule.
Rule 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).
Interface	Select an interface on the Device to which this rule applies.

Table 52 Security > Firewall > Rules: Add (continued)

LABEL	DESCRIPTION
Direction	Select a direction of travel of packets for which you want to configure the firewall rule.
Protocol	Select the IP protocol (**TCP**, **UDP** or **ICMP**) and enter the protocol (service type) number in the port field.
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.
Destination Subnet Mask	Enter the destination subnet mask.
Destination Port	Enter the port number of the destination.
Action	Use the drop-down list box to select whether to discard (**Drop**), deny and send an ICMP message to the sender of (**Reject**) or allow the passage of (**Permit**) packets that match this rule.
Reject Type	If you select **Reject**, specify which type of ICMP message is sent to the sender.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your customized settings and exit this screen.

10

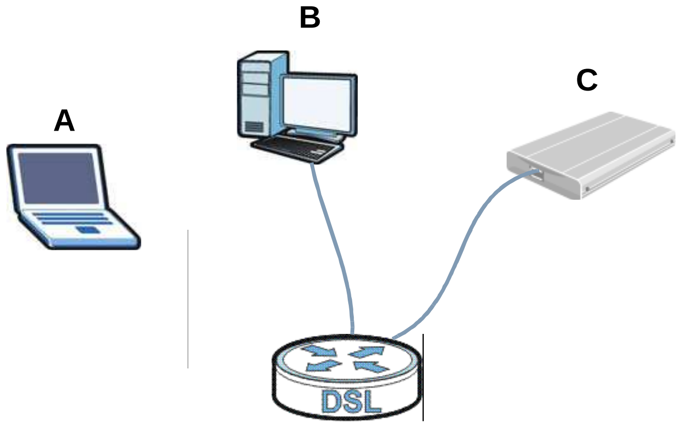
File Sharing

10.1 Overview

Share files on a USB memory stick or hard drive connected to your Device with users on your network.

The following figure is an overview of the Device’s file server feature. Computers **A** and **B** can access files on a USB device (**C**) which is connected to the Device.

Figure 65 File Sharing Overview



- See Section 10.1.2 on page 165 for an explanation of file-sharing terms.
- See Section 2.4 on page 38 for file-sharing examples.

10.1.1 What You Can Do in this chapter

The **File Sharing** screen lets you enable file-sharing server on the Device and configure the workgroup name (Section 10.2 on page 167).

10.1.2 What You Need to Know

Workgroup name

This is the name given to a set of computers that are connected on a network and share resources such as a printer or files. Windows automatically assigns the workgroup name when you set up a network.

Shares

When settings are set to default, each USB device connected to the Device is given a folder, called a “share”. If a USB hard drive connected to the Device has more than one partition, then each partition will be allocated a share. You can also configure a “share” to be a sub-folder or file on the USB device.

File Systems

A file system is a way of storing and organizing files on your hard drive and storage device. Often different operating systems such as Windows or Linux have different file systems. The file-sharing feature on your Device supports File Allocation Table (FAT) and FAT32 file systems.

Windows/CIFS

Common Internet File System (CIFS) is a standard protocol supported by most operating systems in order to share files across the network.

CIFS runs over TCP/IP but uses the SMB (Server Message Block) protocol found in Microsoft Windows for file and printer access; therefore, CIFS will allow all applications, not just Web browsers, to open and share files across the Internet.

The Device uses Common Internet File System (CIFS) protocol for its file sharing functions. CIFS compatible computers can access the USB file storage devices connected to the Device. CIFS protocol is supported on Microsoft Windows, Linux Samba and other operating systems (refer to your systems specifications for CIFS compatibility).

NFS

Network File System (NFS) is a protocol most commonly used on Unix-like systems in order to share files across the network.

Samba

SMB is a client-server protocol used by Microsoft Windows systems for sharing files, printers, and so on.

Samba is a free SMB server that runs on most Unix and Unix-like systems. It provides an implementation of an SMB client and server for use with non-Microsoft operating systems.

File Transfer Protocol

This is a method of transferring data from one computer to another over a network such as the Internet.

10.1.3 Before You Begin

Make sure the Device is connected to your network and turned on.

1 Connect the USB device to one of the Device’s USB ports. Make sure the Device is connected to your network.

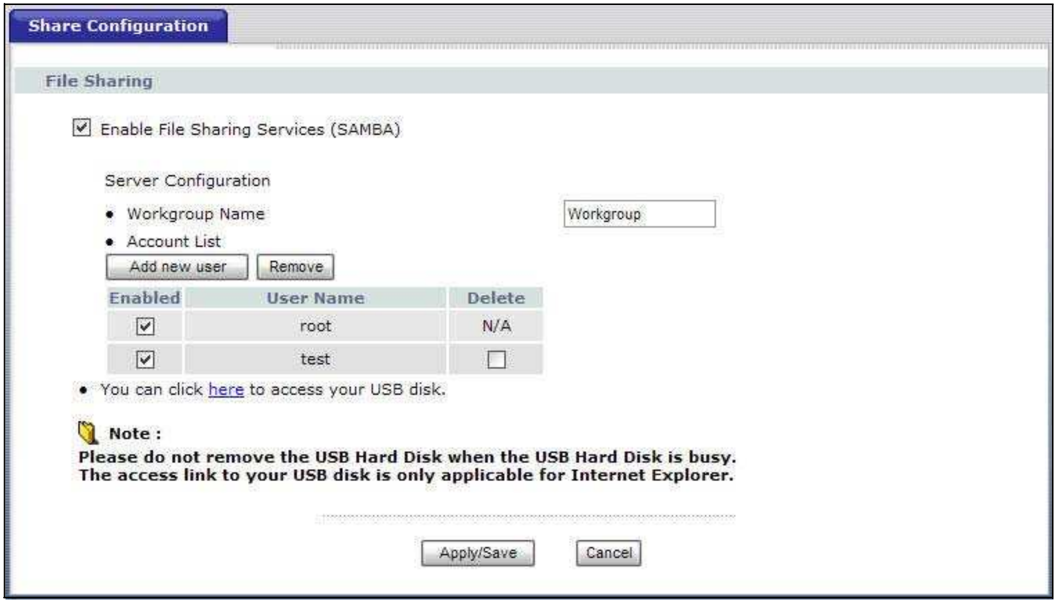
2 The Device detects the USB device and makes its contents available for browsing. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.

Note: If your USB device cannot be detected by the Device, see the troubleshooting for suggestions.

10.2 The File Sharing Screen

Use this screen to set up file sharing via the Device. To access this screen, click **USB Services > File Sharing**.

Figure 66 USB Services > File Sharing



☑ Enable File Sharing Services (SAMBA)

Server Configuration

- Workgroup Name: Workgroup
- Account List

Enabled	User Name	Delete
☑	root	N/A
☑	test	□

- You can click here to access your USB disk.

Note :
Please do not remove the USB Hard Disk when the USB Hard Disk is busy.
The access link to your USB disk is only applicable for Internet Explorer.

Each field is described in the following table.

Table 53 USB Services > File Sharing

LABEL	DESCRIPTION
Enable File Sharing Services	Select this to enable file sharing through the Device.
Server Configuration	
Workgroup Name	You can add the Device to an existing or a new workgroup on your network. Enter the name of the workgroup which your Device automatically joins. You can set the Device's workgroup name to be exactly the same as the workgroup name to which your computer belongs to. Note: The Device will not be able to join the workgroup if your local area network has restrictions set up that do not allow devices to join a workgroup. In this case, contact your network administrator.
Add new user	Click this to set up a file-sharing account. Before you can share files you need a user account.

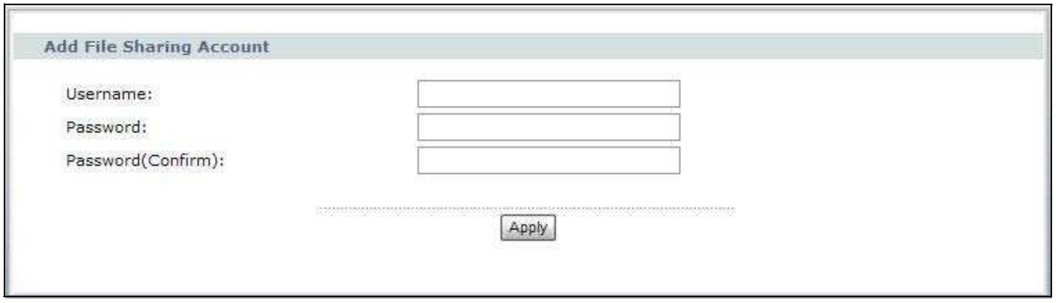
Table 53 USB Services > File Sharing

LABEL	DESCRIPTION
Remove	Click this to delete the user account(s) who's **Delete** check box is selected.
Enabled	This field displays whether a user account is activated or not. Select the check box to enable the account. Clear the check box to disable the account.
User Name	This displays the user name that has been configured on the Device for file sharing.
Delete	Select the check box of the user account that you want to remove from the list.
Apply/Save	Click this to save your changes to the Device.
Cancel	Click this to set every field in this screen to its last-saved value.

10.2.1 Add New User

Click **Add new user** in the **File Sharing** screen to set up a new user on the Device.

Figure 67 USB Services > File Sharing > Add new user



Add File Sharing Account

Username:	
Password:	
Password(Confirm):	

Each field is described in the following table.

Table 54 USB Services > File Sharing > Add new user

LABEL	DESCRIPTION
Username	Enter a user name that will be allowed to access shares. You can enter up to 16 characters. Only letters and numbers allowed.
Password	Enter the password used to access the share. You can enter up to 16 characters. Only letters and numbers are allowed. The password is case sensitive.
Password(Confirm)	Retype the password that you entered above.
Apply	Click this to save your changes to the Device.

11

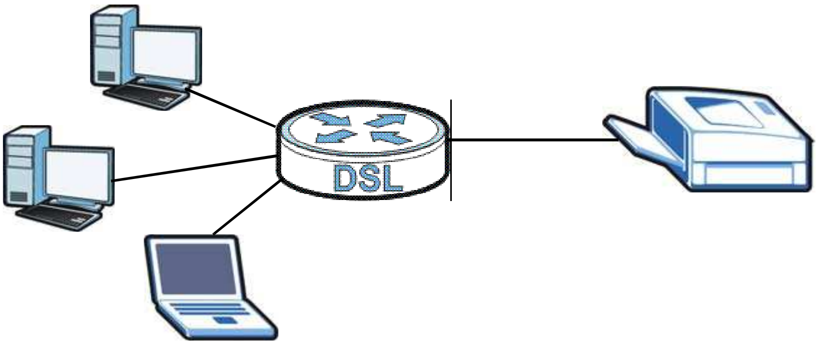
Sharing a USB Printer

This chapter describes how you can share a USB printer via your Device.

11.1 Overview

The Device allows you to share a USB printer on your LAN. You can do this by connecting a USB printer to one of the USB ports on the Device and then allowing the computers connected to your network to communicate with the print server (Device) using the Internet Printing Protocol.

Figure 68 Sharing a USB Printer



11.1.1 What You Can Do in this chapter

- The **Print Server** screen lets you enable the print server on the Device and get the model name of the associated printer. (Section 11.4 on page 170).
- This chapter also shows you examples of adding a new network printer using Windows (Section 11.5 on page 171) and adding a new network printer using Macintosh OS X (Section 11.6 on page 175).

11.2 What You Need to Know

Print Server

This is a computer or other device which manages one or more printers, and which sends print jobs to each printer from the computer itself or other devices.

Operating System

An operating system (OS) is the interface which helps you manage a computer. Common examples are Microsoft Windows, Mac OS or Linux.

Port

A port maps a network service such as http to a process running on your computer, such as a process run by your web browser. When traffic from the Internet is received on your computer, the port number is used to identify which process running on your computer it is intended for.

Internet Printing Protocol

The Internet Printing Protocol (IPP) uses TCP and UDP with port 631. It can run locally or over the Internet on top of HTTP. It allows users to send print jobs to a printer, cancel a previous print job, and know the status of the printer and print jobs.

Supported OSs

The following OSs support Device’s printer sharing feature.

- Microsoft Windows 2000, Windows XP, Windows 7, Windows Vista or Macintosh OS X and later versions.

11.3 Before You Begin

To configure the print server you need the following:

- Your Device must be connected to your computer and any other devices on your network. The USB printer must be connected to your Device.
- The computers on your network must have the printer software already installed before they can use the printer. Follow your printer manufacturers instructions on how to install the printer software on your computer.

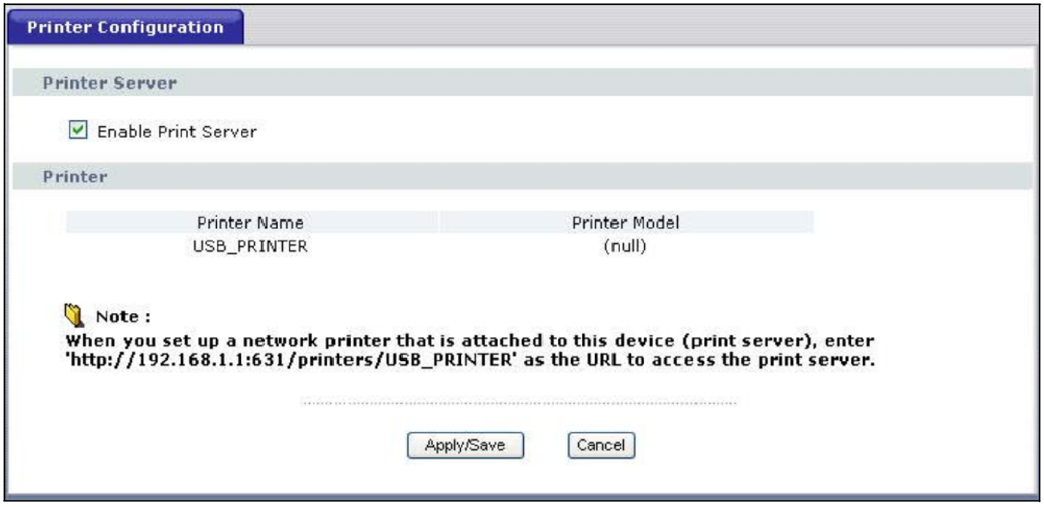
Note: Your printer’s installation instructions may ask that you connect the printer to your computer. Connect your printer to the Device instead.

11.4 The Print Server Screen

The print server screen is used to enable the print server function on the Device and confirm that the Device and the USB printer are able to communicate successfully.

Click **USB Service > Print Server** to display the **Print Server** screen.

Figure 69 USB Service > Print Server



Printer Name	Printer Model
USB_PRINTER	(null)

Note :
When you set up a network printer that is attached to this device (print server), enter 'http://192.168.1.1:631/printers/USB_PRINTER' as the URL to access the print server.

The following table describes the labels in this screen.

Table 55 USB Service > Print Server

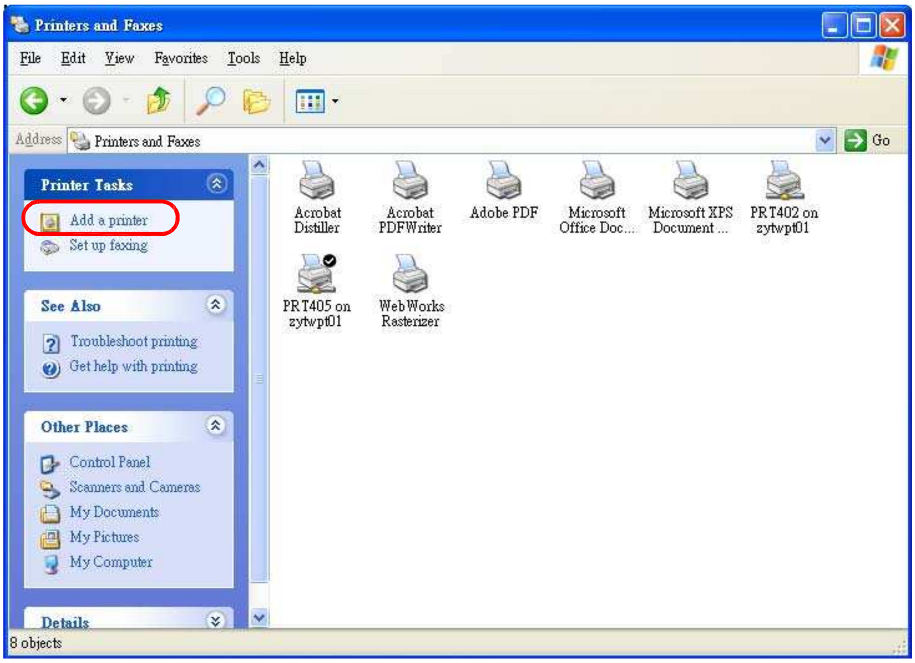
LABEL	DESCRIPTION
Enable Print Server	Select this option to have the Device act as a print server.
Printer Name	This displays the descriptive name of the associated printer for its recognition on the print server network. This name is displayed on a computer on the print server network when a print job is executed.
Printer Model	This displays the model name of the printer currently connected to the Device print server.
Apply/Save	Click **Apply/Save** to save your changes back to the Device.
Cancel	Click **Cancel** to return to the previous configuration.

11.5 Add a New Printer Using Windows

This example shows how to connect a printer behind the Device to your computer using the Windows XP Professional operating system. Some menu items may look different on your operating system.

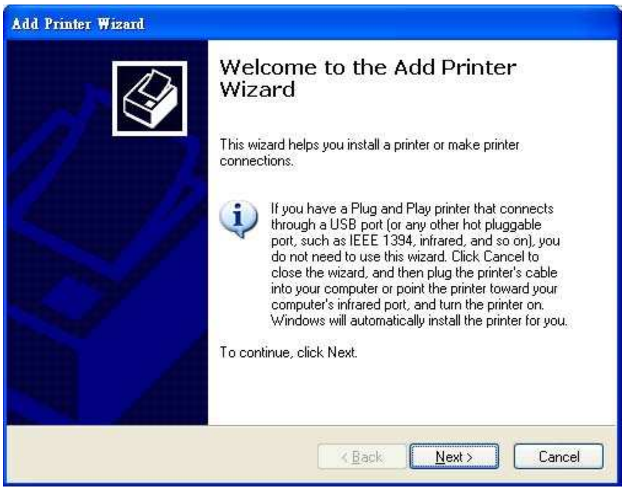
1 Click **Start** > **Control Panel** > **Printers and Faxes** to open the **Printers and Faxes** screen. Click **Add a Printer**.

Figure 70 Printers Folder



2 The **Add Printer Wizard** screen displays. Click **Next**.

Figure 71 Add Printer Wizard: Welcome



Welcome to the Add Printer Wizard

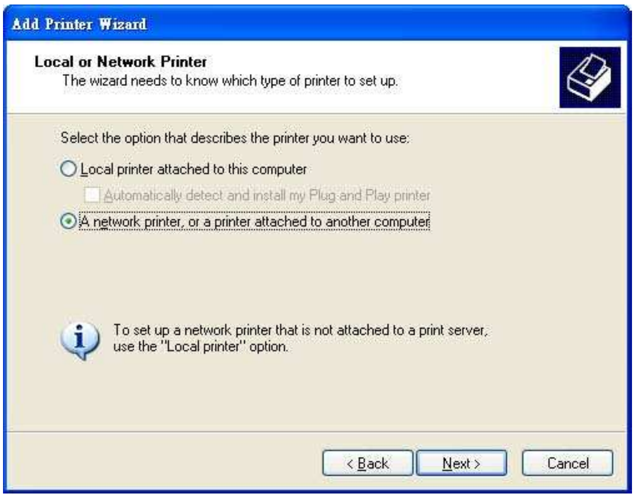
This wizard helps you install a printer or make printer connections.

If you have a Plug and Play printer that connects through a USB port (or any other hot pluggable port, such as IEEE 1394, infrared, and so on), you do not need to use this wizard. Click Cancel to close the wizard, and then plug the printer's cable into your computer or point the printer toward your computer's infrared port, and turn the printer on. Windows will automatically install the printer for you.

To continue, click Next.

3 Select **A network printer, or a printer attached to another computer** and click **Next**.

Figure 72 Add Printer Wizard: Local or Network Printer



Add Printer Wizard

Local or Network Printer
The wizard needs to know which type of printer to set up.

Select the option that describes the printer you want to use:

○ Local printer attached to this computer

□ Automatically detect and install my Plug and Play printer

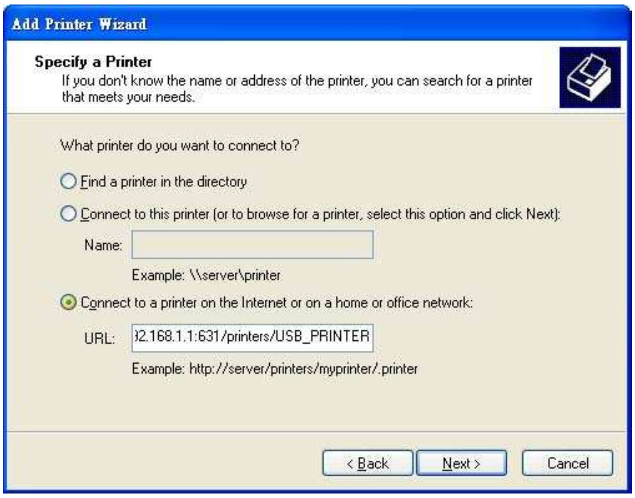
● A network printer, or a printer attached to another computer

To set up a network printer that is not attached to a print server, use the "Local printer" option.

4 Select **Connect to a printer on the Internet or on a home or office network:** and enter “http://192.168.1.1:631/printers/USB_PRINTER” as the URL to access the print server (Device). Click **Next**.

Note: If you change the Device’s LAN IP address, use the new IP address in the URL to access the print server.

Figure 73 Add Printer Wizard: Specify a Printer



Add Printer Wizard

Specify a Printer
If you don't know the name or address of the printer, you can search for a printer that meets your needs.

What printer do you want to connect to?

○ Find a printer in the directory

○ Connect to this printer (or to browse for a printer, select this option and click Next):

Name:

Example: \\server\printer

● Connect to a printer on the Internet or on a home or office network:

URL: 32.168.1.1:631/printers/USB_PRINTER

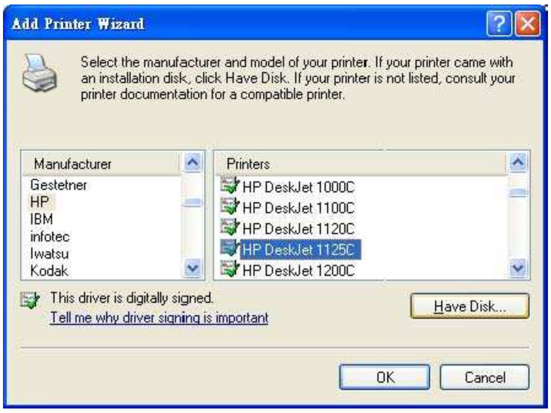
Example: http://server/printers/myprinter/.printer

5 Select the make of the printer that you want to connect to the print server in the **Manufacturer** list of printers.

6 Select the printer model from the list of **Printers**.

7 If your printer is not displayed in the list of **Printers**, you can insert the printer driver installation CD/disk or download the driver file to your computer, click **Have Disk...** and install the new printer driver.

8 Click **Next** to continue.



Add Printer Wizard

Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for a compatible printer.

Manufacturer
Gestetner
HP
IBM
infotec
Iwatsu
Kodak

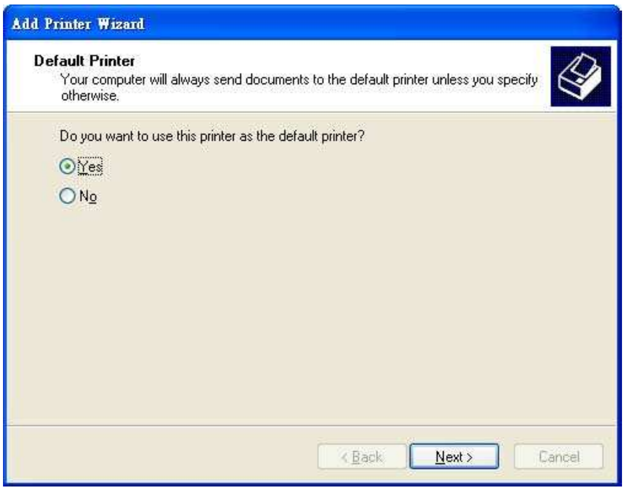
Printers
HP DeskJet 1000C
HP DeskJet 1100C
HP DeskJet 1120C
HP DeskJet 1125C
HP DeskJet 1200C

This driver is digitally signed.

Tell me why driver signing is important

Figure 74 Add Printer Wizard: Printer Model

9 Select **Yes** and then click the **Next** button if you want to use this printer as the default printer on your computer. Otherwise select **No** and then click **Next** to continue.



Add Printer Wizard

Default Printer

Your computer will always send documents to the default printer unless you specify otherwise.

Do you want to use this printer as the default printer?

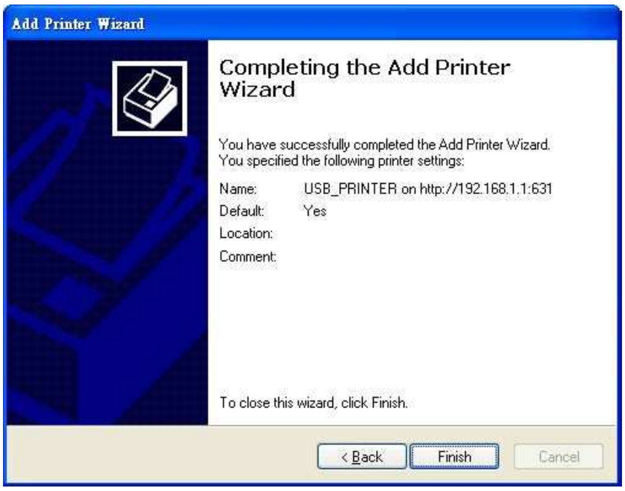
● Yes

○ No

Figure 75 Add Printer Wizard: Default Printer

10 The following screen shows your current printer settings. Select **Finish** to complete adding a new printer.

Figure 76 Add Printer Wizard Complete



Completing the Add Printer Wizard

You have successfully completed the Add Printer Wizard.
You specified the following printer settings:

Name: USB_PRINTER on http://192.168.1.1:631
Default: Yes
Location:
Comment:

To close this wizard, click Finish.

11.6 Add a New Printer Using Macintosh OS X

Complete the following steps to set up a print server driver on your Macintosh computer.

11.6.1 Mac OS 10.3 and 10.4

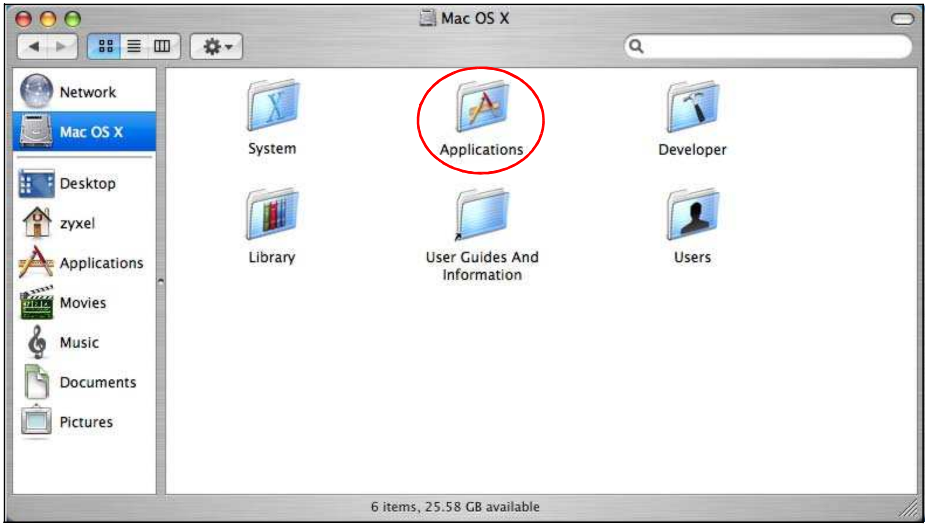
This example shows how to connect a printer behind the Device to your computer using Mac OS X v10.4.11. Some menu items may look different on your operating system.

11 Click the Finder icon on the Dock (a place holding a series of icons/shortcuts at the bottom of the desktop) or double-click your Mac hard disk icon (**Mac OS X** in this example) on your desktop to open the Mac HD window.

Figure 77 Mac OS X HD

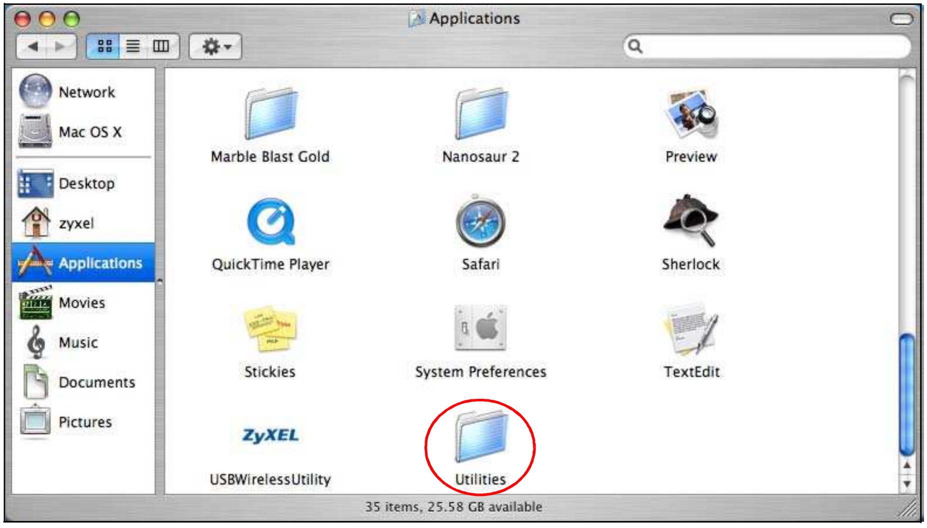
12 Open the **Applications** folder.

Figure 78 Macintosh HD Folder



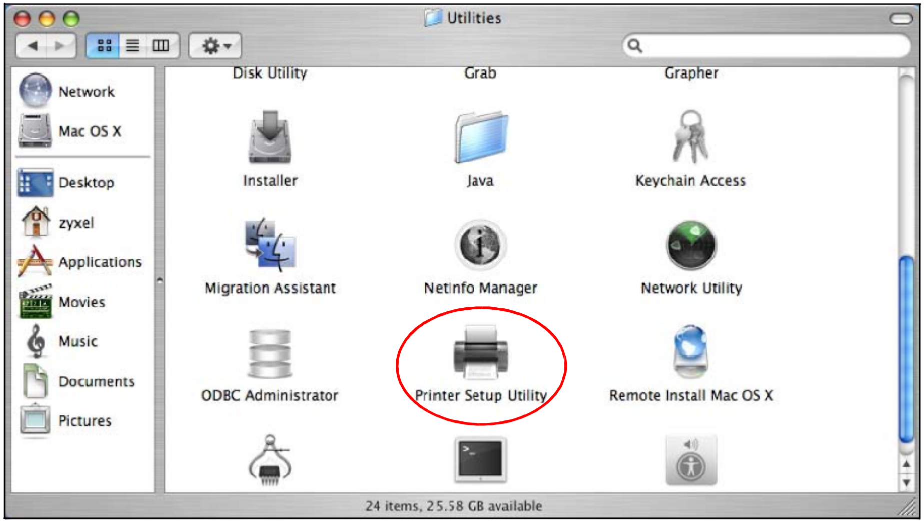
13 Open the **Utilities** folder.

Figure 79 Applications Folder



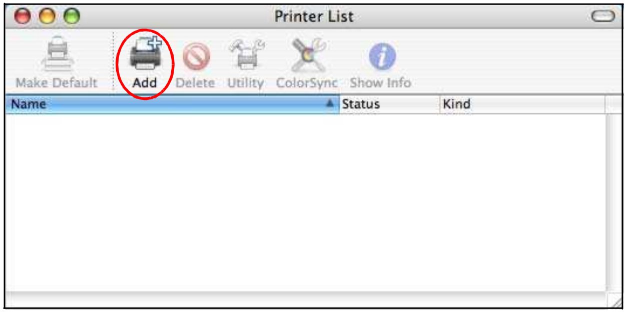
14 Double-click the **Printer Setup Utility** icon.

Figure 80 Utilities Folder



15 Click the **Add** icon at the top of the screen.

Figure 81 Printer List: Add



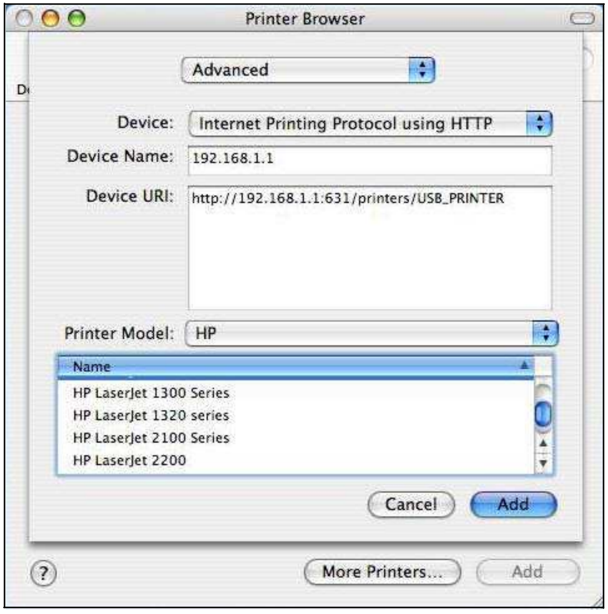
16 Click the **IP Printer** tab to set up your printer.

- Press the `alt` key and click **More Printers** in the **Printer Browser** screen.
- Select **Advanced** from the top drop-down list.
- Select **Internet Printing Protocol using HTTP** from the **Device** drop-down list.
- Enter a descriptive name for the printer in the **Device Name** field.
- In the **Device URL** field, enter "http://192.168.1.1:631/printers/USB_PRINTER" as the URL to access the print server (Device).

Note: If you change the Device's LAN IP address, use the new IP address in the URL to access the print server.

- Select your printer manufacturer from the **Printer Model** drop-down list and then select a printer model. Click **Add** to save and close the **Printer Browser** configuration screen.

Figure 82 Printer Browser



Device: Internet Printing Protocol using HTTP

Device Name: 192.168.1.1

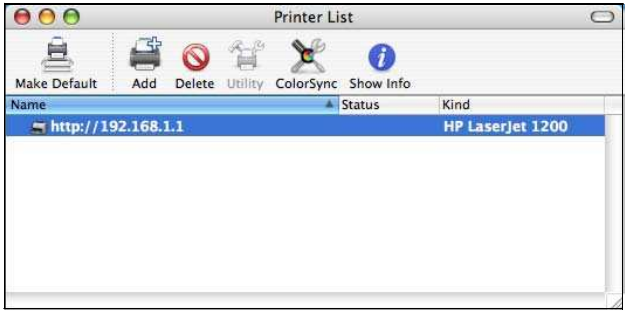
Device URI: http://192.168.1.1:631/printers/USB_PRINTER

Printer Model: HP

Name
HP LaserJet 1300 Series
HP LaserJet 1320 series
HP LaserJet 2100 Series
HP LaserJet 2200

17 The new network printer displays in the **Printer List**. The default printer **Name** displays in bold type.

Figure 83 Printer List



Name	Status	Kind
http://192.168.1.1		**HP LaserJet 1200**

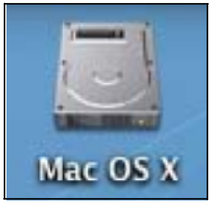
18 Your print server driver setup is complete. You can now use the Device's print server to print from a Mac computer.

11.6.2 Mac OS 10.5 and 10.6

This example shows how to connect a printer behind the Device to your computer using Mac OS X v10.6.2. Some menu items may look different on your operating system.

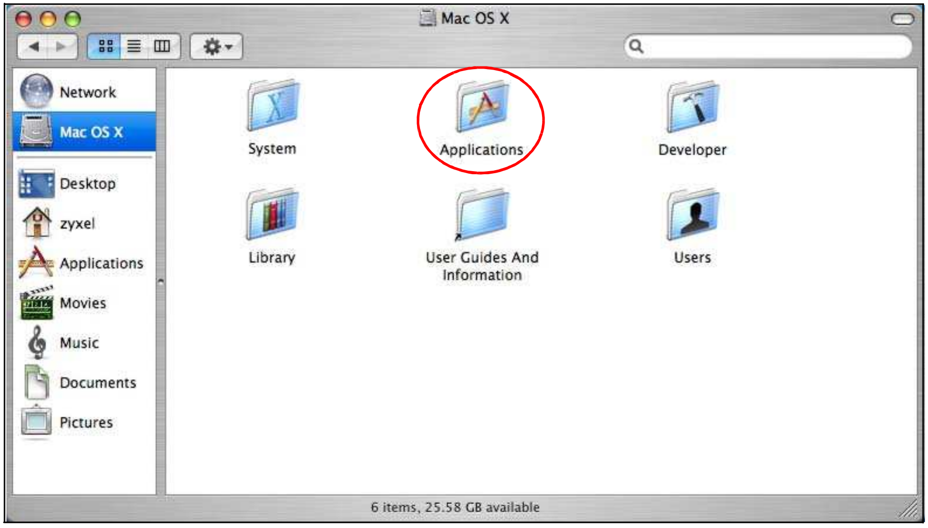
1 Click the Finder icon on the Dock or double-click your Mac hard disk icon (**Mac OS X** in this example) on your desktop to open the Mac HD window.

Figure 84 Mac OS X HD



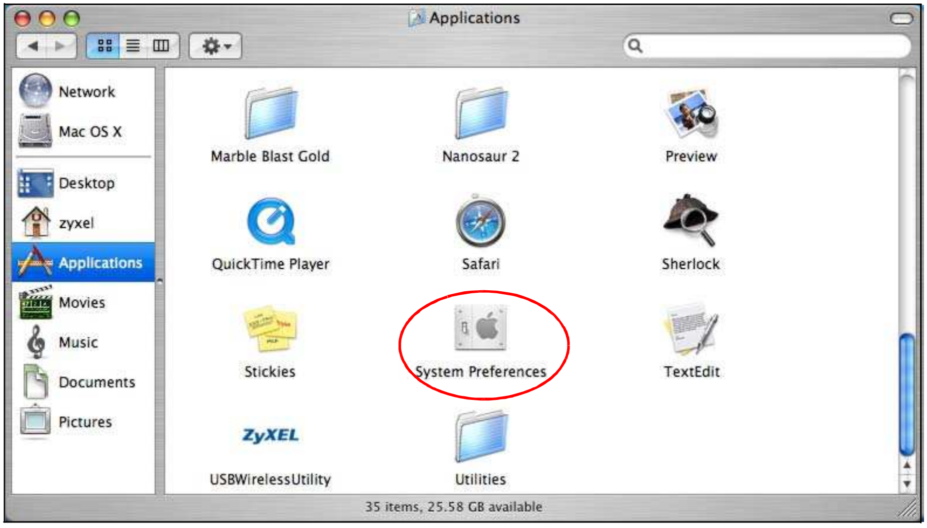
2 Open the **Applications** folder.

Figure 85 Macintosh HD Folder



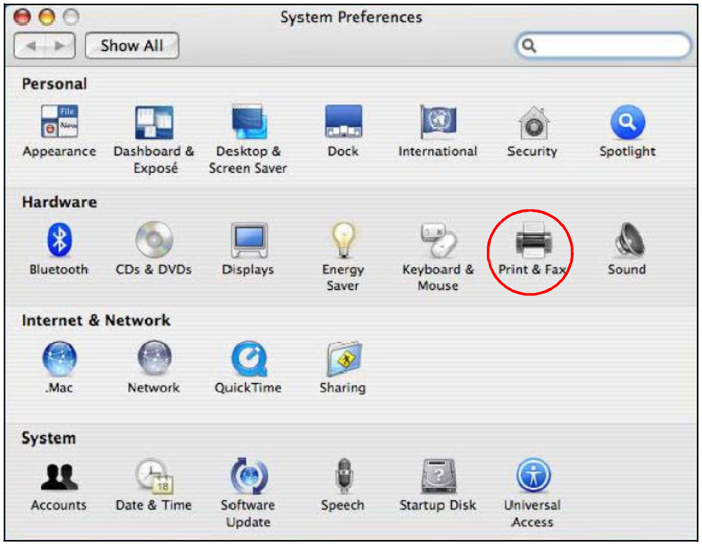
3 Double-click the **System Preferences** icon.

Figure 86 Applications Folder



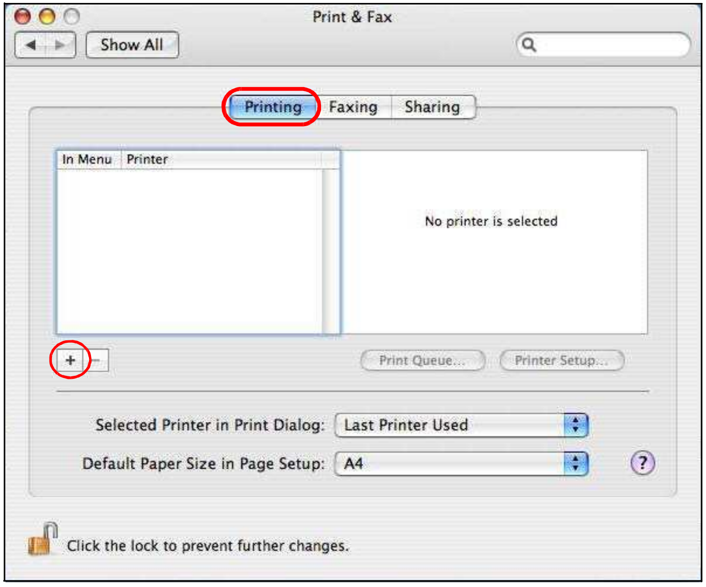
4 Click the **Print & Fax** icon.

Figure 87 System Preferences



5 Select the **Printing** tab and click the **+** icon to add a new printer.

Figure 88 Print & Fax



No printer is selected

Selected Printer in Print Dialog: Last Printer Used

Default Paper Size in Page Setup: A4

Click the lock to prevent further changes.

6 Click the **Advanced** button on the **Add Printer** toolbar to set up your printer.

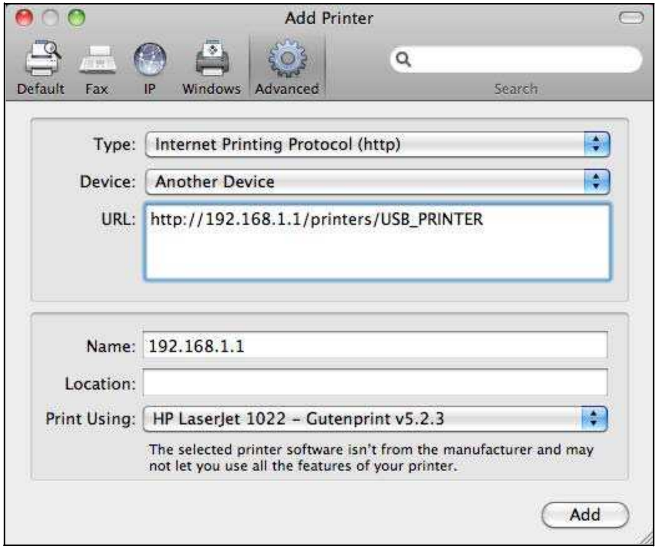
If the **Advanced** button doesn't appear, Ctrl-click the toolbar, select **Customize Toolbar...** and then drag the **Advanced** button onto the toolbar.

- Select **Internet Printing Protocol (HTTP)** from the **Type** drop-down list.
- Select **Another Device** from the **Device** drop-down list.
- In the **URL** field, enter "http://192.168.1.1:631/printers/USB_PRINTER" as the URL to access the print server (Device).

Note: If you change the Device's LAN IP address, use the new IP address in the URL to access the print server.

- Enter a descriptive name for the printer and where it is located.
- Select your printer manufacturer from the **Print Using** drop-down list and then select a printer model. Click **Add** to save and close the **Printer Browser** configuration screen.

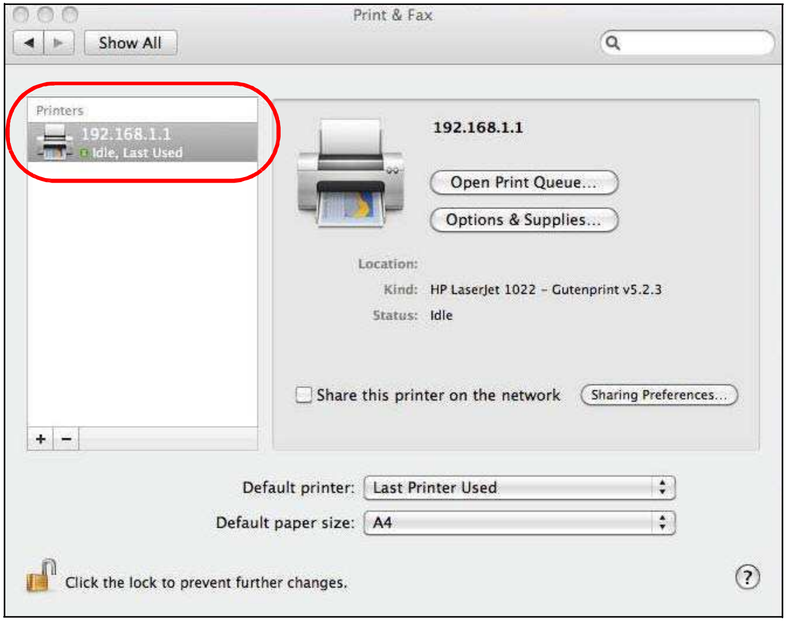
Figure 89 Add Printer



Type: Internet Printing Protocol (http)
Device: Another Device
URL: http://192.168.1.1/printers/USB_PRINTER
Name: 192.168.1.1
Location:
Print Using: HP LaserJet 1022 - Gutenprint v5.2.3
The selected printer software isn't from the manufacturer and may not let you use all the features of your printer.

7 The new network printer displays in the **Printers** list.

Figure 90 Printer List



192.168.1.1
Location:
Kind: HP LaserJet 1022 - Gutenprint v5.2.3
Status: Idle
□ Share this printer on the network
Default printer: Last Printer Used
Default paper size: A4

8 Your print server driver setup is complete. You can now use the Device’s print server to print from a Mac computer.

12

Media Server

12.1 Overview

You can set up your Device to act as a media server to provide media (like video) to DLNA-compliant players, such as Windows Media Player, ZyXEL DMAs (Digital Media Adapters), Xboxes or PS3s. The media server and the clients must have IP addresses in the same subnet.

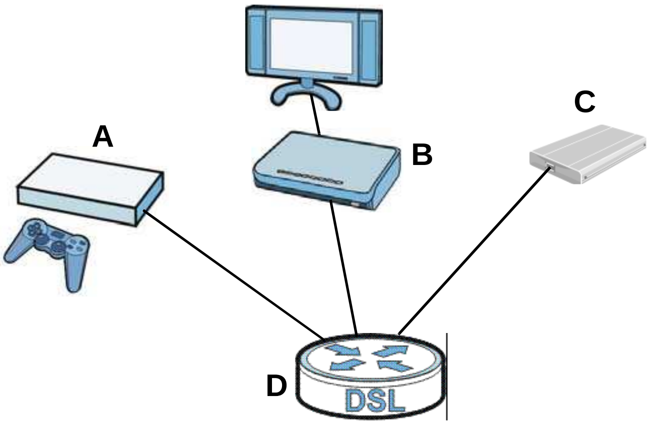
The Device media server enables you to:

- Publish all shares for everyone to play media files in the USB storage device connected to the Device.
- Use hardware-based media clients like the DMA-2500 to play the files.

Note: Anyone on your network can play the media files in the published shares. No user name and password or other form of security is used. The media server is enabled by default with the video, photo, and music shares published.

The following figure is an overview of the Device's media server feature. DLNA devices **A** and **B** can access and play files on a USB device (**C**) which is connected to the Device (**D**).

Figure 91 Media Server Overview



12.1.1 What You Can Do in this chapter

The **Media Server** screen lets you use the Device as a media server and allow DLNA-compliant devices to play files stored in the attached USB hard drive (Section 12.2 on page 184).

12.1.2 What You Need to Know

Media Server

The media server feature lets anyone on your network play video, music, and photos from the Device (without having to copy them to another computer). The Device streams files to DLNA-compliant media clients without any configuration.

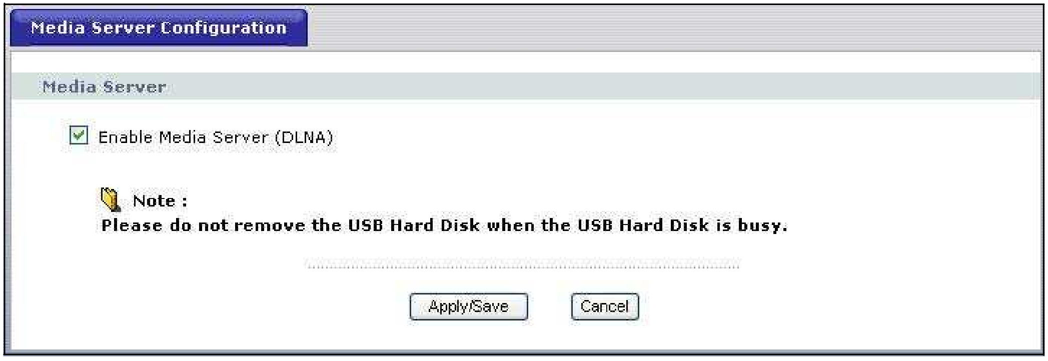
DLNA

The Digital Living Network Alliance (DLNA) is a group of personal computer and electronics companies that works to make products compatible in a home network in order to make digital living easy and seamless. DLNA clients play files stored on DLNA servers.

12.2 The Media Server Screen

Use this screen to have the Device work as a media server. To access this screen, click **USB Services > Media Server**.

Figure 92 USB Services > Media Server



☑ Enable Media Server (DLNA)

Note :
Please do not remove the USB Hard Disk when the USB Hard Disk is busy.

Each field is described in the following table.

Table 56 USB Services > Media Server

LABEL	DESCRIPTION
Enable Media Server (DLNA)	Select this to have the Device function as a DLNA-compliant media server.
Apply/Save	Click **Apply/Save** to save your changes back to the Device.
Cancel	Click **Cancel** to return to the previous configuration.

13

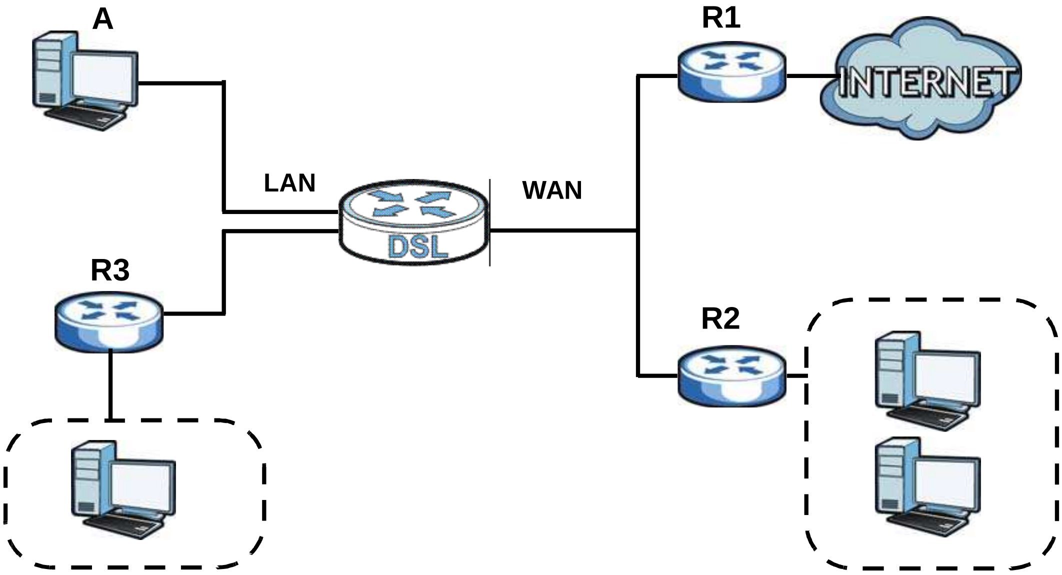
Static Route

13.1 Overview

The Device usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the 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 Device's LAN interface. The Device routes most traffic from **A** to the Internet through the 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 93 Example of Static Routing Topology



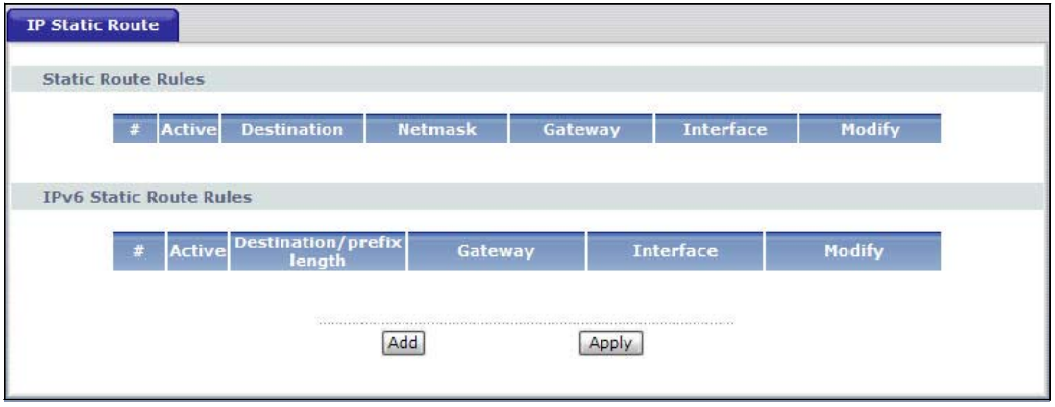
13.1.1 What You Can Do in this Chapter

The **Static Route** screens let you view and configure IP static routes on the Device (Section 13.2 on page 186).

13.2 The Static Route Screen

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

Figure 94 Advanced > Static Route


IP Static Route
Static Route Rules
# Active Destination Netmask Gateway Interface Modify
IPv6 Static Route Rules
# Active Destination/prefix length Gateway Interface Modify
Add
Apply

The following table describes the labels in this screen.

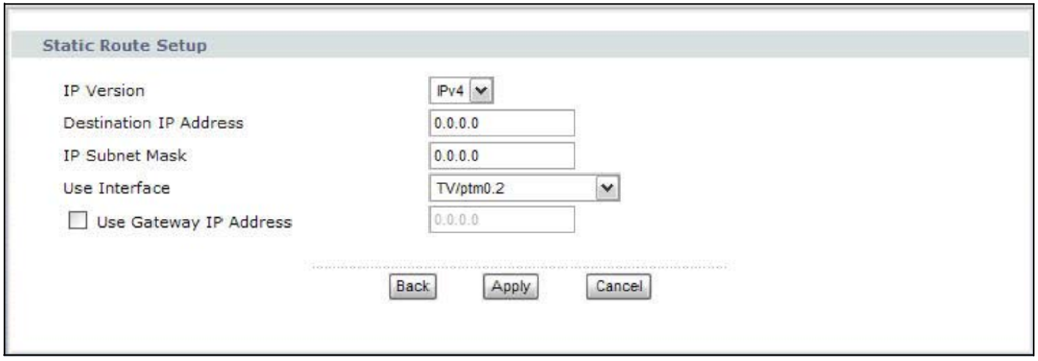
Table 57 Advanced > Static Route

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.
Destination / prefix length	If an IPv6 static route rule is specified, this parameter specifies the IPv6 network address and prefix length 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 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 Device. Click the Remove icon to remove a static route from the 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 Device.

13.2.1 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 95 Static Route: Add



Static Route Setup

IP Version: IPv4

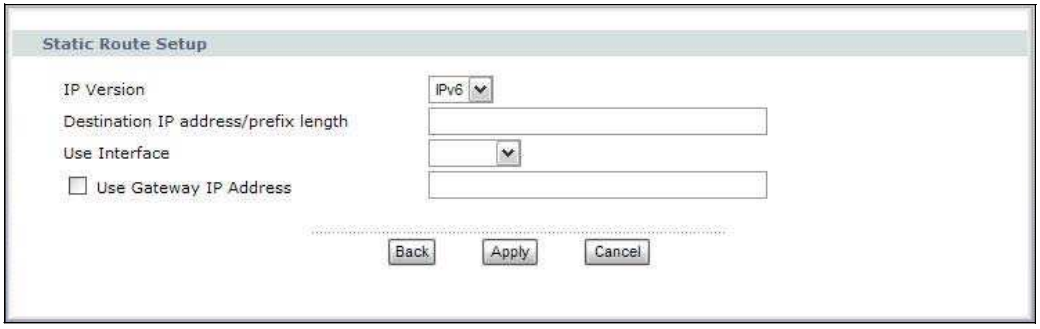
Destination IP Address: 0.0.0.0

IP Subnet Mask: 0.0.0.0

Use Interface: TV/ptm0.2

□ Use Gateway IP Address: 0.0.0.0

Figure 96 Static Route: Add: IPv6



Static Route Setup

IP Version: IPv6

Destination IP address/prefix length

Use Interface

□ Use Gateway IP Address

The following table describes the labels in these screens.

Table 58 Static Route: Add

LABEL	DESCRIPTION
IP Version	Select the IP version to use for this static route's traffic.
Destination IP Address	If **IPv4** is selected as the IP version, 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.
Destination IP address/prefix length	If **IPv6** is selected as the IP version, this parameter specifies the IPv6 network address and prefix length of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use the prefix length of 128 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 or LAN 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 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 Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

14

RIP

14.1 Overview

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

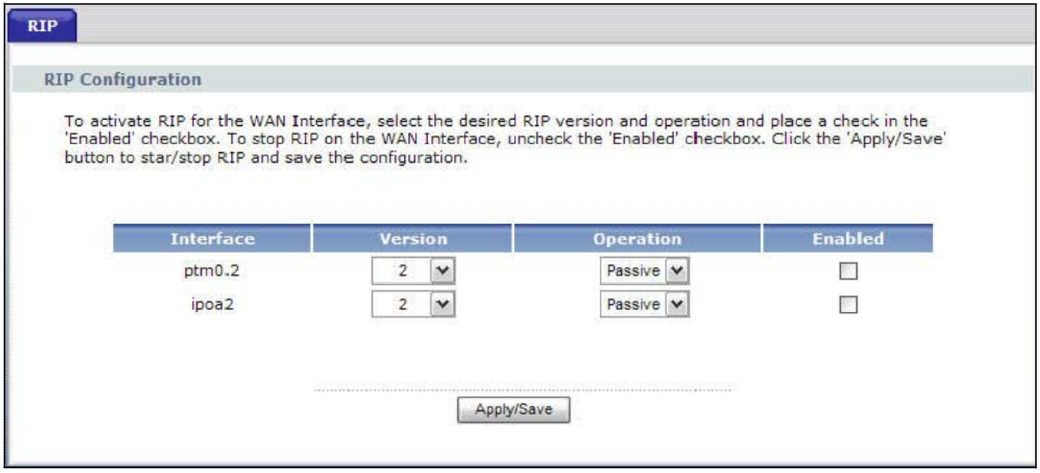
14.1.1 What You Can Do in this Chapter

The **RIP** screen lets you set up RIP settings on the Device (Section 14.2 on page 189).

14.2 The RIP Screen

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

Figure 97 Advanced > RIP



RIP Configuration

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	□
ipoa2	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 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.

Table 59 Advanced > RIP

LABEL	DESCRIPTION
Operation	Select **Passive** to have the 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 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 Device.

15

Quality of Service (QoS)

15.1 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 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 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.

15.1.1 What You Can Do in this Chapter

- The **General** screen lets you enable or disable QoS, and set the bandwidth (Section 15.3 on page 193).
- The **Queue Setup** screen lets you lets you configure QoS queue assignment (Section 15.4 on page 194).
- The **Class Setup** screen lets you add, edit or delete QoS classifiers (Section 15.5 on page 196).
- The **Policer Setup** screens lets you add, edit or delete QoS policers (Section 15.6 on page 201).
- The **Monitor** screen lets you view the Device's QoS-related packet statistics (Section 15.7 on page 204).

15.2 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.

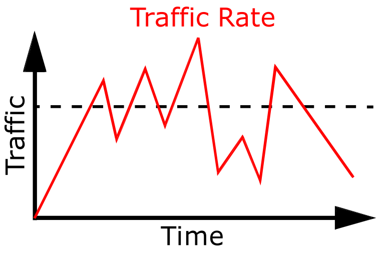
CoS technologies include IEEE 802.1p layer 2 tagging and DiffServ (Differentiated Services or DS). IEEE 802.1p tagging makes use of three bits in the packet header, while DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit ToS (Type of Service) field in the IP header.

Tagging and Marking

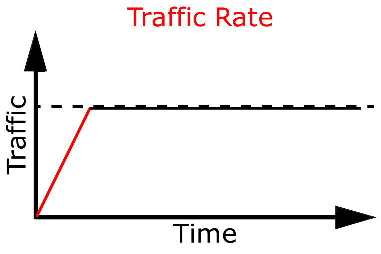
In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or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

Traffic Shaping

Bursty traffic may cause network congestion. Traffic shaping regulates packets to be transmitted with a pre-configured data transmission rate using buffers (or queues). Your Device uses the Token Bucket algorithm to allow a certain amount of large bursts while keeping a limit at the average rate.



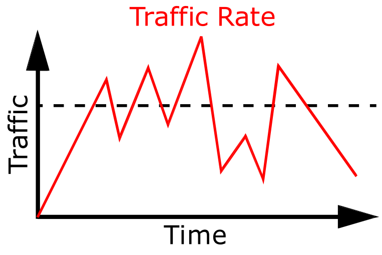
(Before Traffic Shaping)



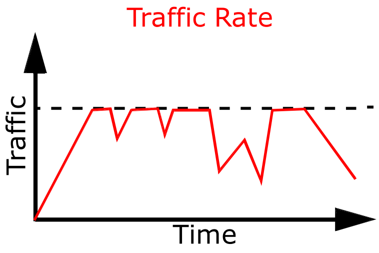
(After Traffic Shaping)

Traffic Policing

Traffic policing is the limiting of the input or output transmission rate of a class of traffic on the basis of user-defined criteria. Traffic policing methods measure traffic flows against user-defined criteria and identify it as either conforming, exceeding or violating the criteria.



(Before Traffic Policing)



(After Traffic Policing)

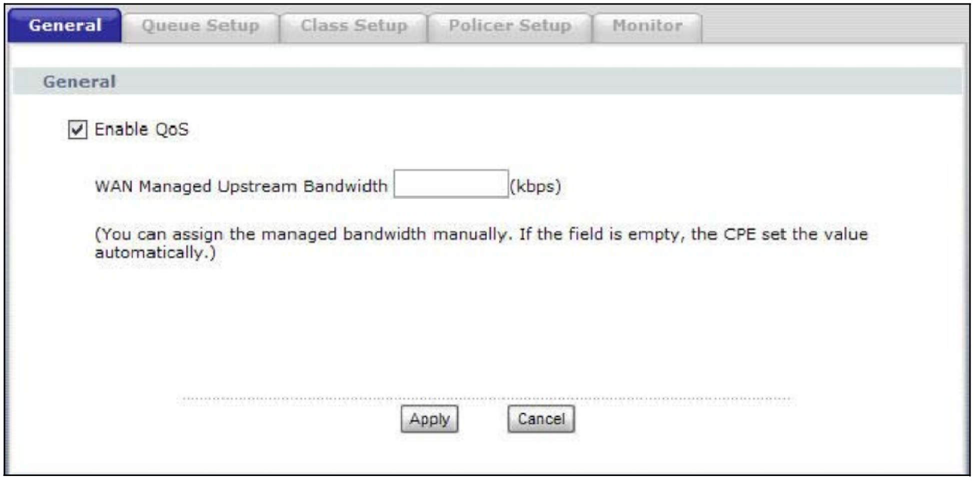
The Device supports three incoming traffic metering algorithms: Token Bucket Filter (TBF), Single Rate Two Color Maker (srTCM), and Two Rate Two Color Marker (trTCM). You can specify actions which are performed on the colored packets. See Section 15.8 on page 205 for more information on each metering algorithm.

15.3 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 bandwidth. See Section 15.1 on page 191 for more information.

Figure 98 QoS General



General

☑ Enable QoS

WAN Managed Upstream Bandwidth [ ] (kbps)

(You can assign the managed 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

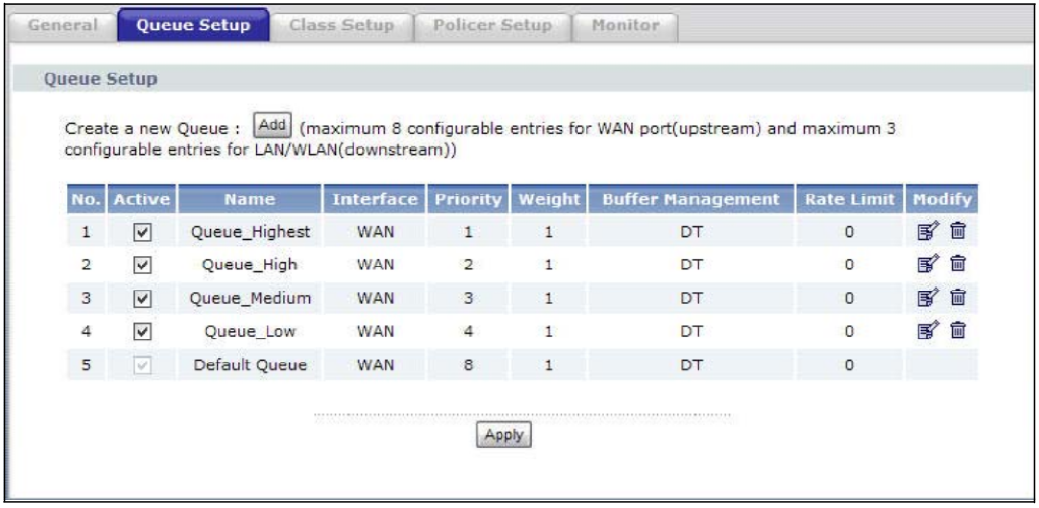
LABEL	DESCRIPTION
Enable QoS	Select the check box to turn on QoS to improve your network performance.
WAN Managed Upstream Bandwidth	Enter the amount of upstream bandwidth for the WAN interface that you want to allocate using QoS. The recommendation is to set this speed to match the interface's actual 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 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 Device to not use some of the interface's available bandwidth. If you leave this field blank, the 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 Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

15.4 The Queue Setup Screen

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

Use this screen to configure QoS queue assignment.

Figure 99 QoS Queue Setup



Create a new Queue : Add (maximum 8 configurable entries for WAN port(upstream) and maximum 3 configurable entries for LAN/WLAN(downstream))

No.	Active	Name	Interface	Priority	Weight	Buffer Management	Rate Limit	Modify
1	☑	Queue_Highest	WAN	1	1	DT	0	✎ 🗑
2	☑	Queue_High	WAN	2	1	DT	0	✎ 🗑
3	☑	Queue_Medium	WAN	3	1	DT	0	✎ 🗑
4	☑	Queue_Low	WAN	4	1	DT	0	✎ 🗑
5	☑	Default Queue	WAN	8	1	DT	0	

The following table describes the labels in this screen.

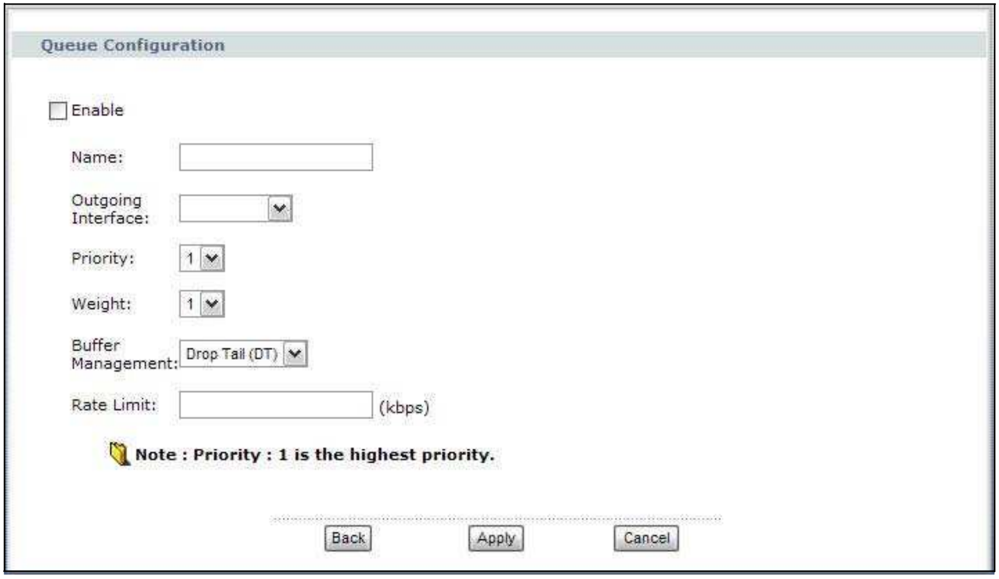
Table 61 QoS Queue Setup

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 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 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 Device.

15.4.1 Adding a QoS Queue

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

Figure 100 QoS Queue Setup: Add



Queue Configuration

□ Enable

Name:

Outgoing Interface:

Priority: 1

Weight: 1

Buffer Management: Drop Tail (DT)

Rate Limit: (kbps)

Note : Priority : 1 is the highest priority.

The following table describes the labels in this screen.

Table 62 QoS Queue Setup: Add

LABEL	DESCRIPTION
Enable	Select this to have the Device's QoS use this queue.
Name	Enter the descriptive name of this queue.

Table 62 QoS Queue Setup: Add

LABEL	DESCRIPTION
Outgoing Interface	Select the WAN interface to which this queue is applied.
Priority	Select the priority level (from 1 to 7) 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 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 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 Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

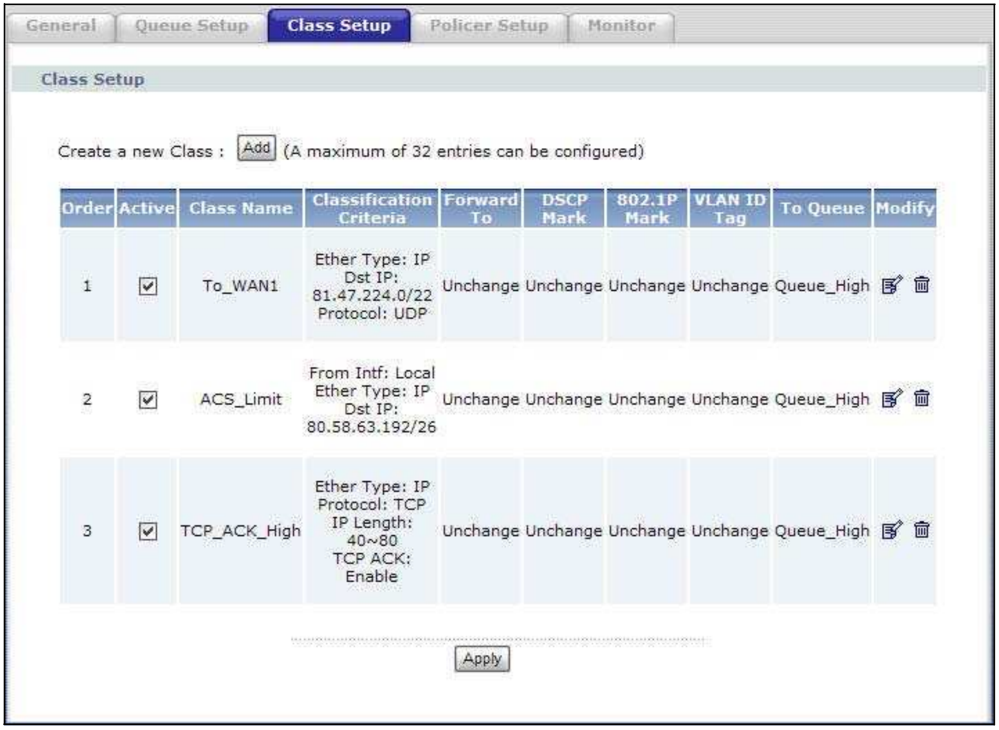
15.5 The Class Setup Screen

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 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 101 QoS Class Setup



Class Setup

Create a new Class : Add (A maximum of 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	☑	To_WAN1	Ether Type: IP Dst IP: 81.47.224.0/22 Protocol: UDP	Unchange	Unchange	Unchange	Unchange	Queue_High	✎ 🗑
2	☑	ACS_Limit	From Intf: Local Ether Type: IP Dst IP: 80.58.63.192/26	Unchange	Unchange	Unchange	Unchange	Queue_High	✎ 🗑
3	☑	TCP_ACK_High	Ether Type: IP Protocol: TCP IP Length: 40~80 TCP ACK: Enable	Unchange	Unchange	Unchange	Unchange	Queue_High	✎ 🗑

Apply

The following table describes the labels in this screen.

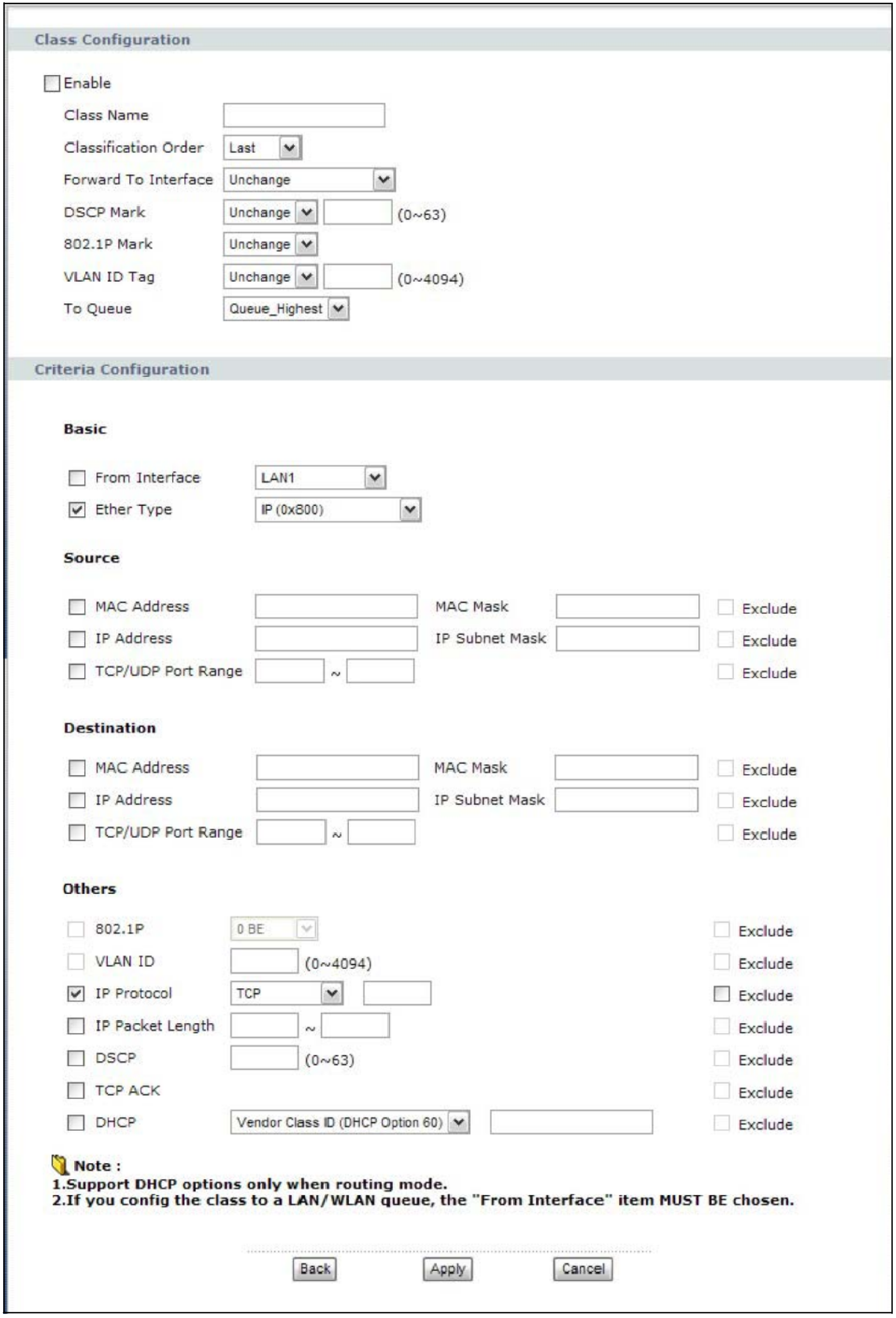
Table 63 QoS Class Setup

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.
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 Device.

15.5.1 QoS Class Edit

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

Figure 102 QoS Class Setup: Add



Class Configuration

☐ Enable

Class Name

Classification Order: Last

Forward To Interface: Unchange

DSCP Mark: Unchange (0~63)

802.1P Mark: Unchange

VLAN ID Tag: Unchange (0~4094)

To Queue: Queue_Highest

Criteria Configuration

Basic

☐ From Interface: LAN1

☑ 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 (0~4094) · ☐ Exclude

☑ IP Protocol: TCP · ☐ Exclude

☐ IP Packet Length ~ · ☐ Exclude

☐ DSCP (0~63) · ☐ Exclude

☐ TCP ACK · ☐ Exclude

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

Note :
1.Support DHCP options only when routing mode.
2.If you config the class to a LAN/WLAN queue, the "From Interface" item MUST BE chosen.

The following table describes the labels in this screen.

Table 64 QoS Class Configuration

LABEL	DESCRIPTION
Class Configuration	
Enable	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 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 Device replaces the DSCP field in the packets. If you select **Unchange**, the Device keep the DSCP field in the packets.
802.1p Mark	Select a priority level with which the Device replaces the IEEE 802.1p priority field in the packets. If you select **Unchange**, the 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 Device replaces the VLAN ID of the frames. If you select **Remove**, the Device deletes the VLAN ID of the frames before forwarding them out. If you select **Add**, the Device treat all matched traffic untagged and add a second VLAN ID. If you select **Unchange**, the 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.
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.

Table 64 QoS Class Configuration (continued)

LABEL	DESCRIPTION
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	
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.

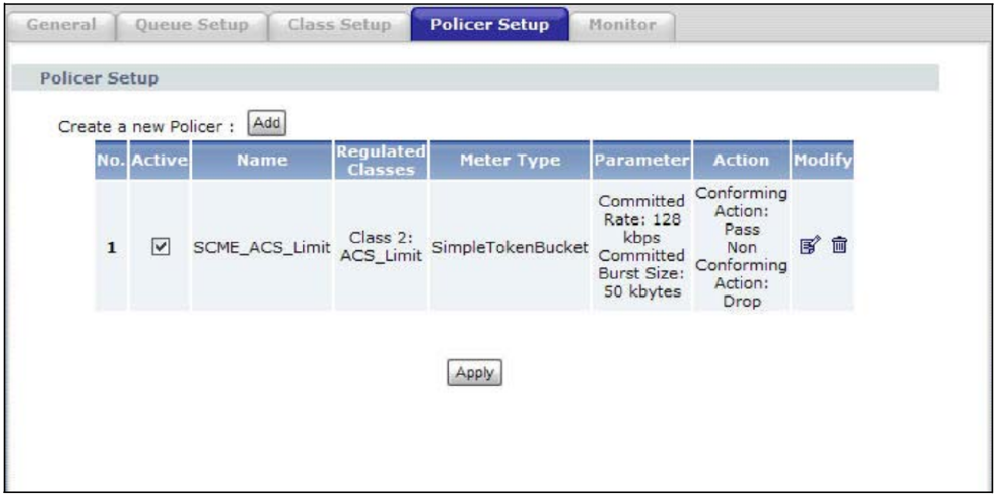
Table 64 QoS Class Configuration (continued)

LABEL	DESCRIPTION
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 Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

15.6 The Policer Setup Screen

Click **QoS > Policer Setup** to open the screen as shown next. Use this screen to configure QoS policers to limit the transmission rate of incoming traffic. This lets you prevent high priority packets from choking off all other traffic.

Figure 103 Policer Setup



Policer Setup

Create a new Policer : Add

No.	Active	Name	Regulated Classes	Meter Type	Parameter	Action	Modify
1	☑	SCME_ACS_Limit	Class 2: ACS_Limit	SimpleTokenBucket	Committed Rate: 128 kbps Committed Burst Size: 50 kbytes	Conforming Action: Pass Non Conforming Action: Drop	

The following table describes the labels in this screen.

Table 65 QoS Policer Setup

LABEL	DESCRIPTION
Add	Click this button to create a new entry.
No.	This is the index number of this entry.

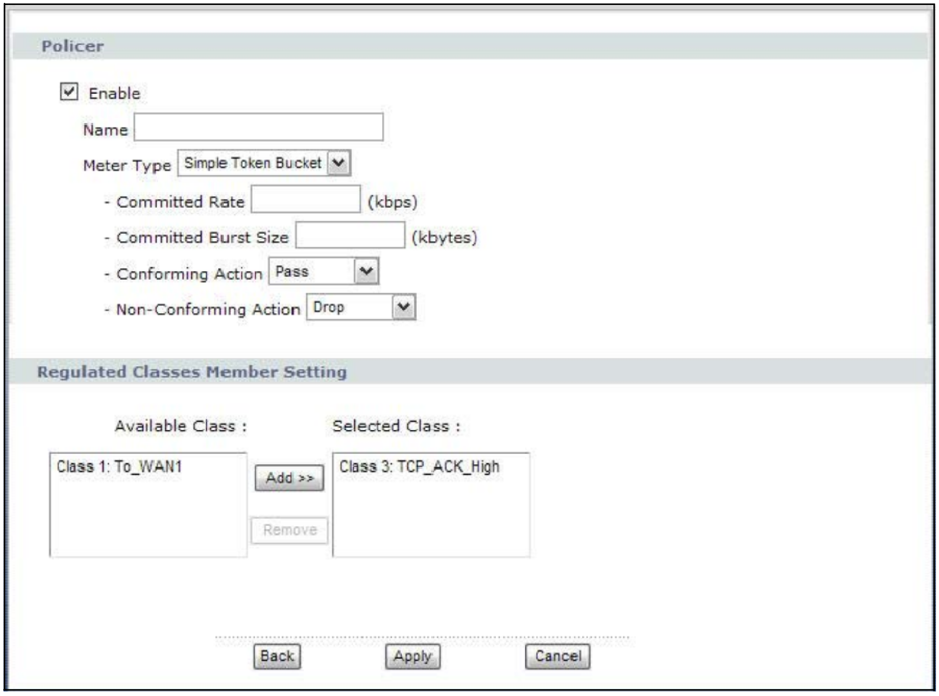
Table 65 QoS Policer Setup

LABEL	DESCRIPTION
Active	Select the check box to enable the policer.
Name	This shows the descriptive name of this queue.
Regulated Classes	These are the policer's member QoS classes (classifiers).
Meter Type	This shows which QoS metering algorithm the policer uses to shape traffic.
Parameter	These are the rates and burst sizes against which the policer checks the traffic of the member QoS classes.
Action	This shows the how the policer has the Device treat different types of traffic belonging to the policer's member QoS classes.
Modify	Click the **Edit** icon to go to the screen where you can edit the policer. 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 Device.

15.6.1 Adding a QoS Policer

Click the **Add** button or the **Edit** icon in the **Policer Setup** screen to configure a policer.

Figure 104 Policer Setup: Add



Policer

☑ Enable

Name

Meter Type: Simple Token Bucket

- Committed Rate (kbps)
- Committed Burst Size (kbytes)
- Conforming Action: Pass
- Non-Conforming Action: Drop

Regulated Classes Member Setting

Available Class : Class 1: To_WAN1

Selected Class : Class 3: TCP_ACK_High

The following table describes the labels in this screen.

Table 66 QoS Policer Setup: Add

LABEL	DESCRIPTION
Enable	Select this to turn on this policer.
Name	Enter the descriptive name of this policer.

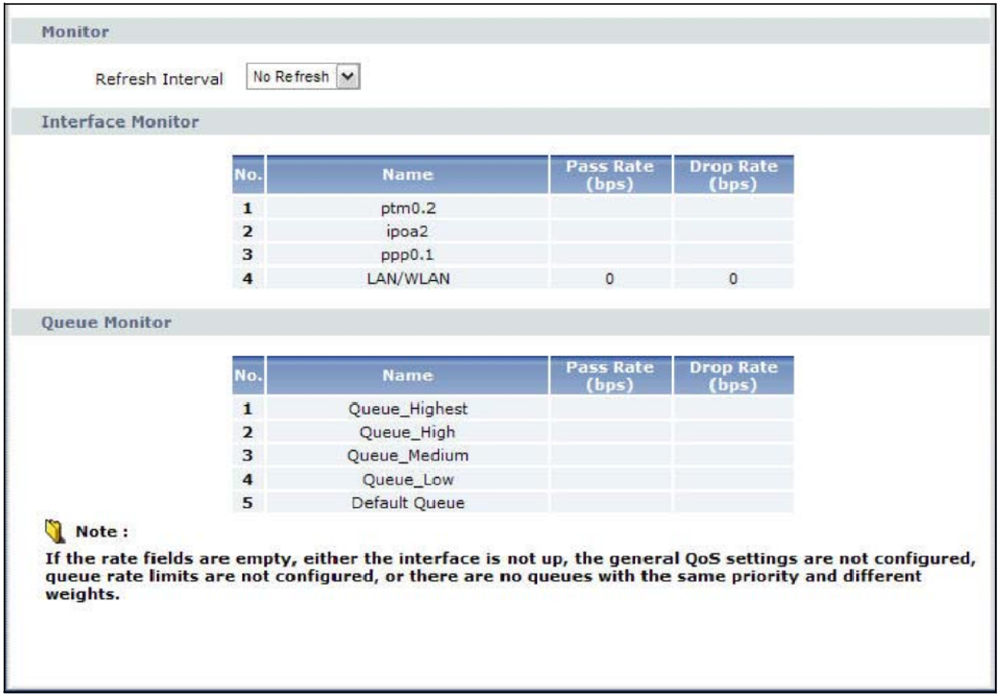
Table 66 QoS Policer Setup: Add

LABEL	DESCRIPTION
Meter Type	Select how the policer shapes the traffic of the member QoS classes. The **Simple Token Bucket** algorithm uses tokens in a bucket to control when traffic can be transmitted. Each token represents one byte. The algorithm allows bursts of up to *b* bytes which is also the bucket size.
Committed Rate	Specify the committed rate. When the incoming traffic rate of the member QoS classes is less than the committed rate, the device applies the conforming action to the traffic.
Committed Burst Size	Specify the committed burst size for packet bursts. This must be equal to or less than the peak burst size (two rate three color) or excess burst size (single rate three color) if it is also configured. This is the maximum size of the (first) token bucket in a traffic metering algorithm.
Conforming Action	Specify what the Device does for packets within the committed rate and burst size (green-marked packets). • **Pass**: Send the packets without modification. • **DSCP Mark**: Change the DSCP mark value of the packets. Enter the DSCP mark value to use.
Non-Conforming Action	Specify what the Device does for packets that exceed the excess burst size or peak rate and burst size (red-marked packets). • **Drop**: Discard the packets. • **DSCP Mark**: Change the DSCP mark value of the packets. Enter the DSCP mark value to use. The packets may be dropped if there is congestion on the network.
Regulated Classes Member Setting	
Available Class Selected Class	Select a QoS classifier to apply this QoS policer to traffic that matches the QoS classifier. Highlight a QoS classifier in the **Available Class** box and use the **Add >>** button to move it to the **Selected Class** box. To remove a QoS classifier from the **Selected Class** box, select it and use the **Remove** button.
Back	Click **Back** to return to the previous screen without saving.
Apply	Click **Apply** to save your changes back to the Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

15.7 The QoS Monitor Screen

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

Figure 105 QoS > Monitor



Monitor

Refresh Interval: No Refresh

Interface Monitor

No.	Name	Pass Rate (bps)	Drop Rate (bps)
1	ptm0.2		
2	ipoa2		
3	ppp0.1		
4	LAN/WLAN	0	0

Queue Monitor

No.	Name	Pass Rate (bps)	Drop Rate (bps)
1	Queue_Highest		
2	Queue_High		
3	Queue_Medium		
4	Queue_Low		
5	Default Queue		

Note :

If the rate fields are empty, either the interface is not up, the general QoS settings are not configured, queue rate limits are not configured, or there are no queues with the same priority and different weights.

The following table describes the labels in this screen.

Table 67 QoS > Monitor

LABEL	DESCRIPTION
Refresh Interval	Enter how often you want the 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 Device.
Pass Rate	This shows the transmission rate of packets which are forwarded to this interface and transmitted successfully.
Drop Rate	This shows the transmission rate of packets which are forwarded to this interface and dropped.
Queue Monitor	
No.	This is the index number of the entry.
Name	This shows the name of the queue.
Pass Rate	This shows the transmission rate of packets which are assigned to this queue and transmitted successfully.
Drop Rate	This shows the transmission rate of packets which are assigned to this queue and dropped.

15.8 Technical Reference

The following section contains additional technical information about the 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 68 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.

IP Precedence

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

Token Bucket

The token bucket algorithm uses tokens in a bucket to control when traffic can be transmitted. The bucket stores tokens, each of which represents one byte. The algorithm allows bursts of up to *b* bytes which is also the bucket size, so the bucket can hold up to *b* tokens. Tokens are generated and added into the bucket at a constant rate. The following shows how tokens work with packets:

- A packet can be transmitted if the number of tokens in the bucket is equal to or greater than the size of the packet (in bytes).
- After a packet is transmitted, a number of tokens corresponding to the packet size is removed from the bucket.
- If there are no tokens in the bucket, the Device stops transmitting until enough tokens are generated.
- If not enough tokens are available, the Device treats the packet in either one of the following ways:

  In traffic shaping:

  - Holds it in the queue until enough tokens are available in the bucket.

  In traffic policing:

  - Drops it.
  - Transmits it but adds a DSCP mark. The Device may drop these marked packets if the network is overloaded.

Configure the bucket size to be equal to or less than the amount of the bandwidth that the interface can support. It does not help if you set it to a bucket size over the interface’s capability. The smaller the bucket size, the lower the data transmission rate and that may cause outgoing packets to be dropped. A larger transmission rate requires a big bucket size. For example, use a bucket size of 10 kbytes to get the transmission rate up to 10 Mbps.

16

Dynamic DNS Setup

16.1 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.

16.1.1 What You Can Do in this Chapter

Use the **Dynamic DNS** screen (Section 16.3 on page 208) to enable DDNS and configure the DDNS settings on the Device.

16.2 What You Need To Know

DYNDNS Wildcard

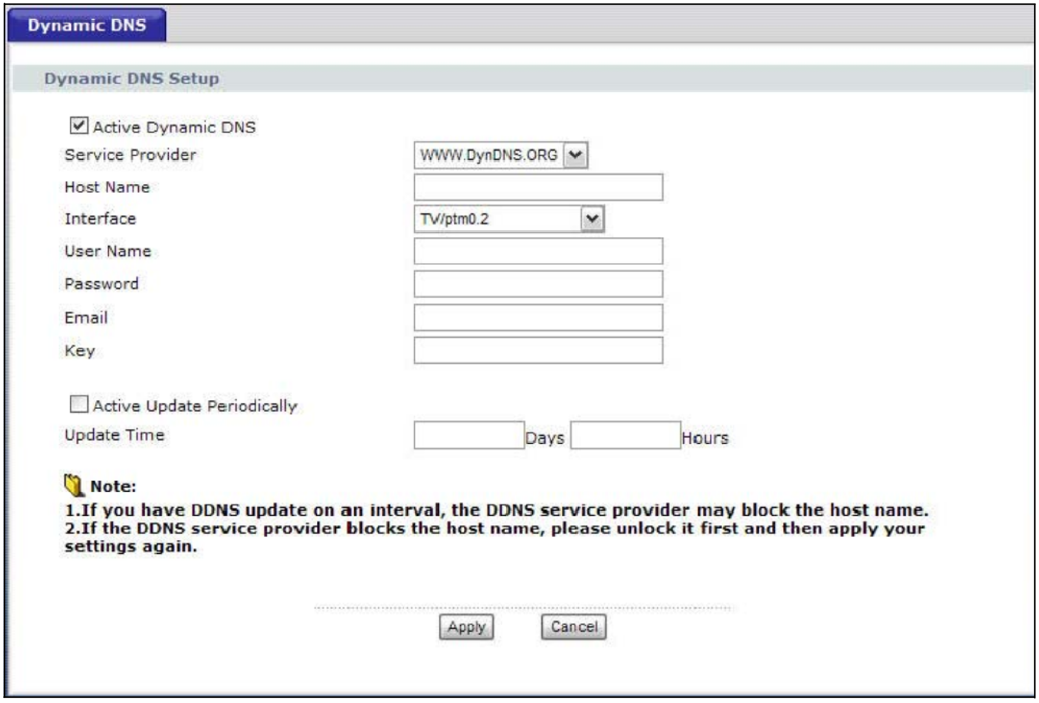
Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

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

16.3 The Dynamic DNS Screen

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

Figure 106 Advanced > Dynamic DNS



☑ Active Dynamic DNS

Service Provider: WWW.DynDNS.ORG

Host Name:

Interface: TV/ptm0.2

User Name:

Password:

Email:

Key:

□ Active Update Periodically

Update Time: Days Hours

Note:
1.If you have DDNS update on an interval, the DDNS service provider may block the host name.
2.If the DDNS service provider blocks the host name, please unlock it first and then apply your settings again.

The following table describes the fields in this screen.

Table 69 Advanced > Dynamic DNS

LABEL	DESCRIPTION
Active Dynamic DNS	Select this to have the Device use DDNS.
Service Provider	Select the name of your Dynamic DNS service provider.
Host Name	Type the domain name assigned to your 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.
Active Update Periodically	Select this to have the Device update the domain name on a regular interval. Bear in mind that some Dynamic DNS service providers will not appreciate the extra traffic and may block your host name.
Update Time	If you selected **Active Update Periodically**, enter a number of days and hours to set how often the Device updates the domain name.

Table 69 Advanced > Dynamic DNS (continued)

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

17

Remote Management

17.1 Overview

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

17.1.1 What You Can Do in this Chapter

- The **TR-069** screen lets you configure the Device's TR-069 auto-configuration settings (Section 17.2 on page 211).
- The **IP Address** screens let you configure from which IP address(es) users can use a service to manage the Device (Section 17.3 on page 213).

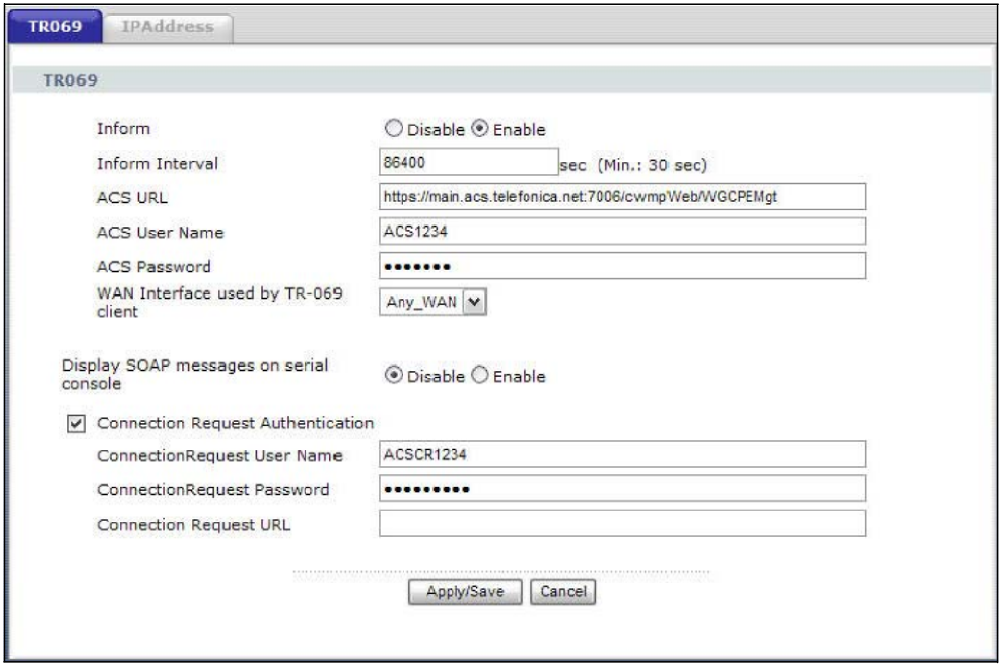
17.2 The TR-069 Screen

TR-069 defines how Customer Premise Equipment (CPE), for example your 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 Device, modify settings, perform firmware upgrades as well as monitor and diagnose the 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 107 TR-069



TR069

Inform ○ Disable ● Enable

Inform Interval 86400 sec (Min.: 30 sec)

ACS URL https://main.acs.telefonica.net:7006/cwmpWeb/WGCPEMgt

ACS User Name ACS1234

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 ACSCR1234

ConnectionRequest Password ••••••••••

Connection Request URL

The following table describes the fields in this screen.

Table 70 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 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 Device, this user name is used to authenticate the ACS.

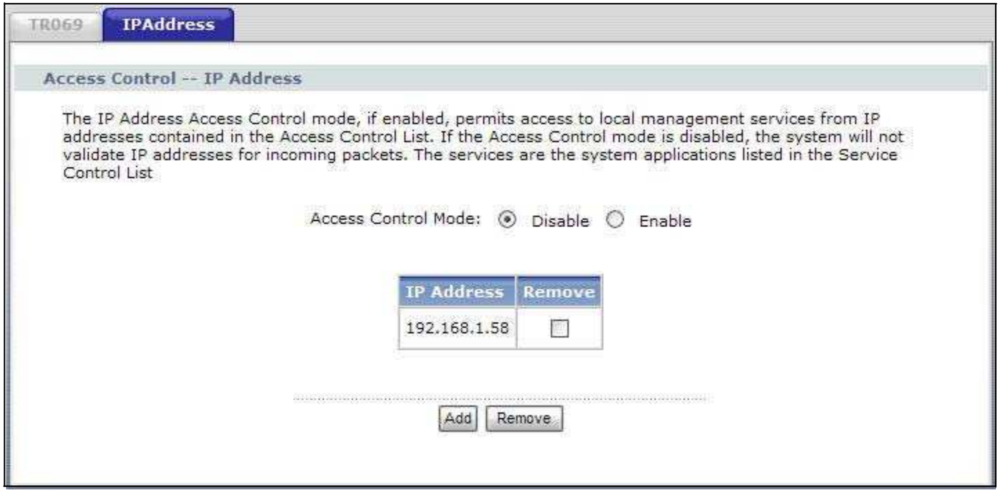
Table 70 TR-069 (continued)

LABEL	DESCRIPTION
Connection Request Password	Enter the connection request password. When the ACS makes a connection request to the 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 Device.
Apply/Save	Click this button to save your changes back to the Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

17.3 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 Device.

Figure 108 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
192.168.1.58	□

The following table describes the fields in this screen.

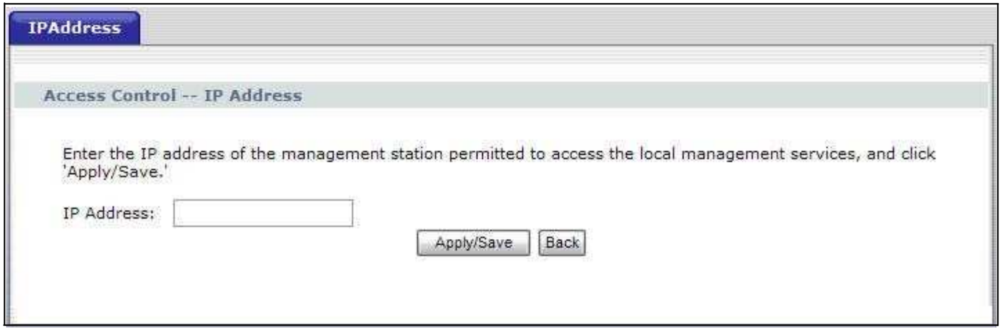
Table 71 IP Address

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 Device.
Remove	Select this check box and click the **Remove** button to delete this entry from the Device.
Add	Click this button to create a new entry.
Remove	Click this button to delete the selected entry.

17.3.1 Adding an IP Address

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

Figure 109 IP Address: Add



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 Device.
Apply/Save	Click this button to save your changes back to the Device.
Back	Click this button to return to the previous screen without saving.

18

Universal Plug-and-Play (UPnP)

18.1 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.

18.1.1 What You Can Do in this Chapter

The **UPnP** screen lets you enable UPnP on the Device (Section 18.3 on page 216).

18.2 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 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.

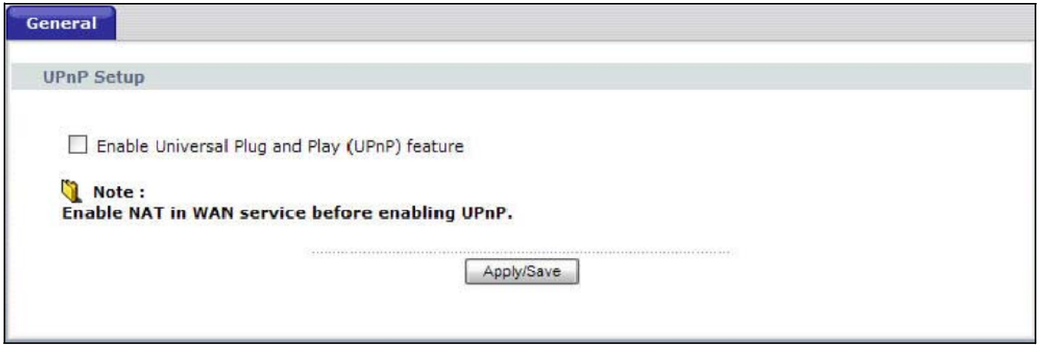
See the following sections for examples of installing and using UPnP.

18.3 The UPnP Screen

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

See Section 18.1 on page 215 for more information.

Figure 110 Advanced > UPnP



□ Enable Universal Plug and Play (UPnP) feature

Note :
Enable NAT in WAN service before enabling UPnP.

The following table describes the fields in this screen.

Table 73 Advanced > UPnP

LABEL	DESCRIPTION
Enable Universal Plug and Play (UPnP) feature	Select this check box to enable UPnP. Be aware that anyone could use a UPnP application to open the Web Configurator's login screen without entering the Device's IP address (although you must still enter the password to access the web configurator).
Apply/Save	Click this to save the setting to the Device.

18.4 Installing UPnP in Windows Example

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

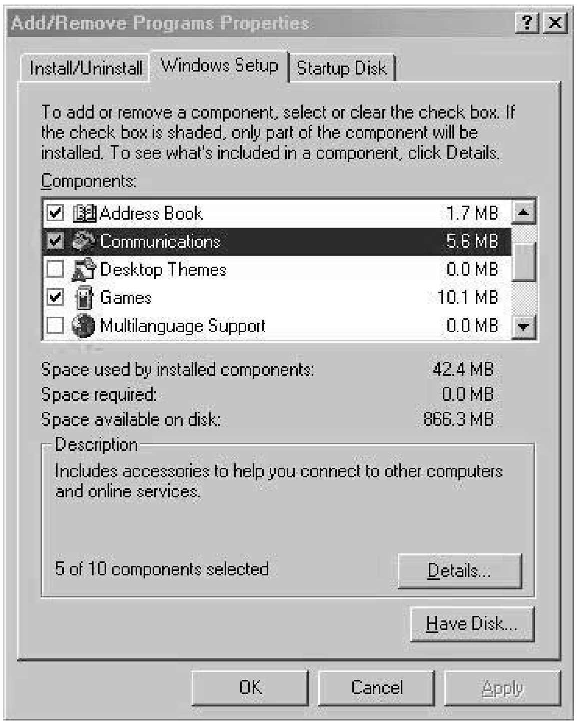
Installing UPnP in Windows Me

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

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

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

Figure 111 Add/Remove Programs: Windows Setup: Communication



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

Components:

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

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

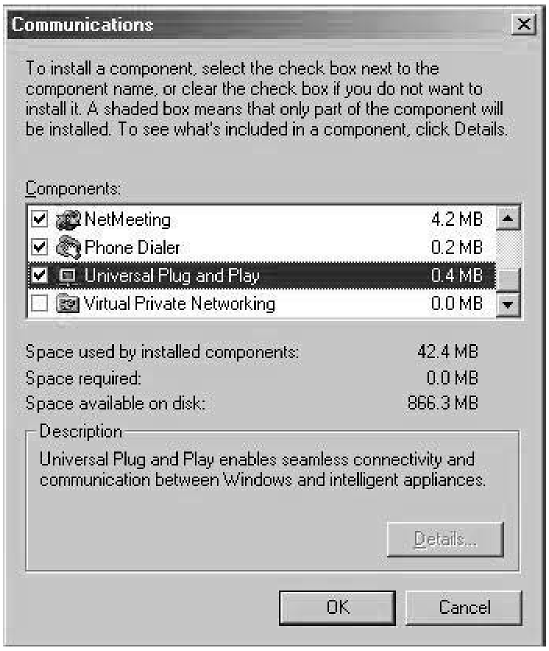
Description

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

5 of 10 components selected

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

Figure 112 Add/Remove Programs: Windows Setup: Communication: Components



Communications

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

Components:

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

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

Description

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

4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.

5 Restart the computer when prompted.

Installing UPnP in Windows XP

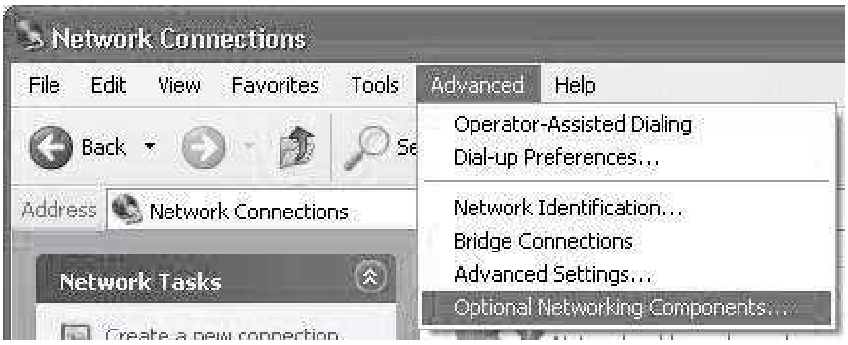
Follow the steps below to install the UPnP in Windows XP.

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

2 Double-click **Network Connections**.

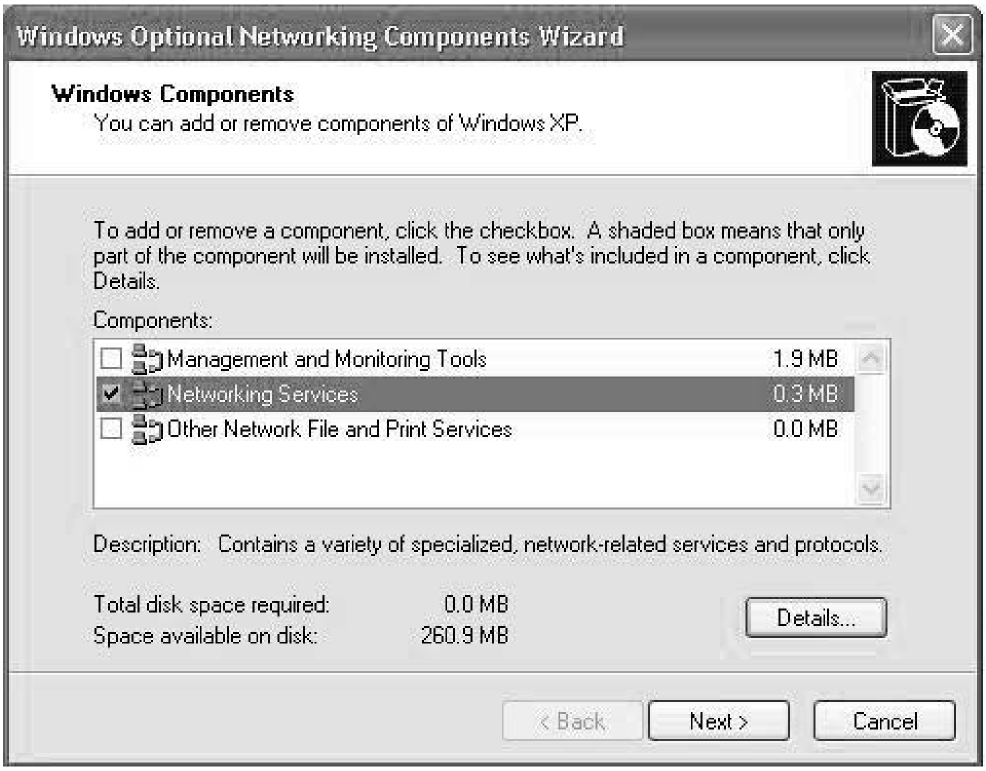
3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ...**.

Figure 113 Network Connections



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

Figure 114 Windows Optional Networking Components Wizard



Windows Optional Networking Components Wizard

Windows Components
You can add or remove components of Windows XP.

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

Components:

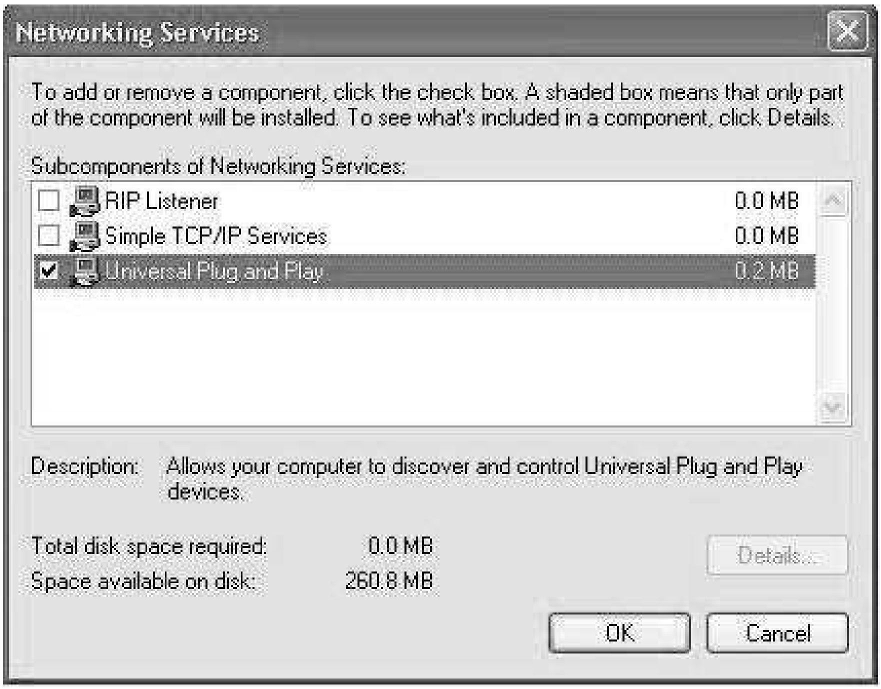
□	Management and Monitoring Tools	1.9 MB
☑	Networking Services	0.3 MB
□	Other Network File and Print Services	0.0 MB

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

Total disk space required: 0.0 MB
Space available on disk: 260.9 MB

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

Figure 115 Networking Services



Networking Services

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

Subcomponents of Networking Services:

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

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

Total disk space required: 0.0 MB
Space available on disk: 260.8 MB

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

18.5 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the Device.

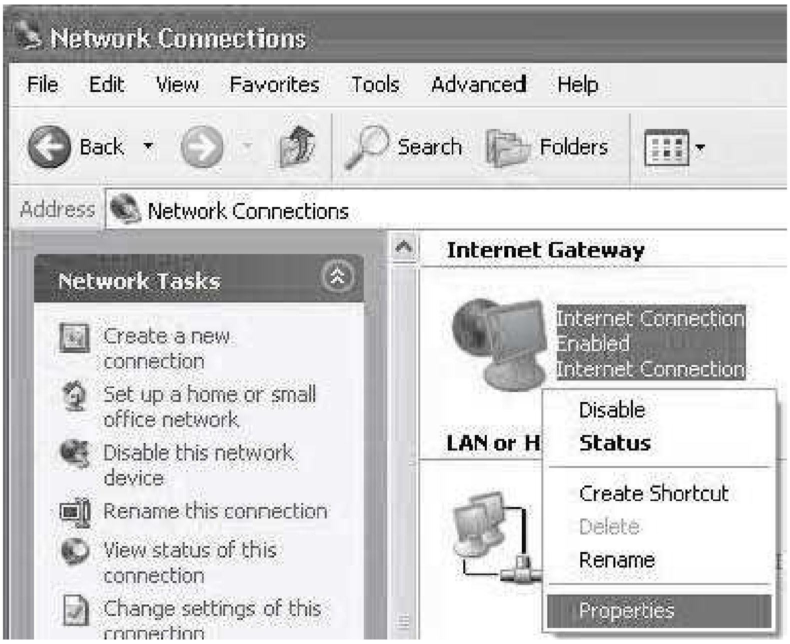
Make sure the computer is connected to a LAN port of the Device. Turn on your computer and the Device.

Auto-discover Your UPnP-enabled Network Device

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

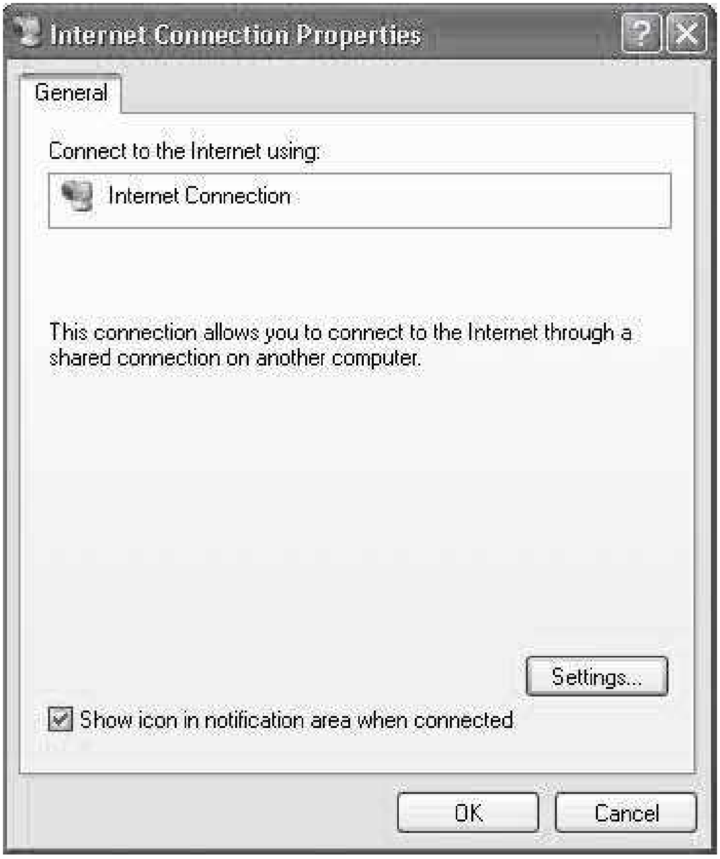
2 Right-click the icon and select **Properties**.

Figure 116 Network Connections



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

Figure 117 Internet Connection Properties



Connect to the Internet using:

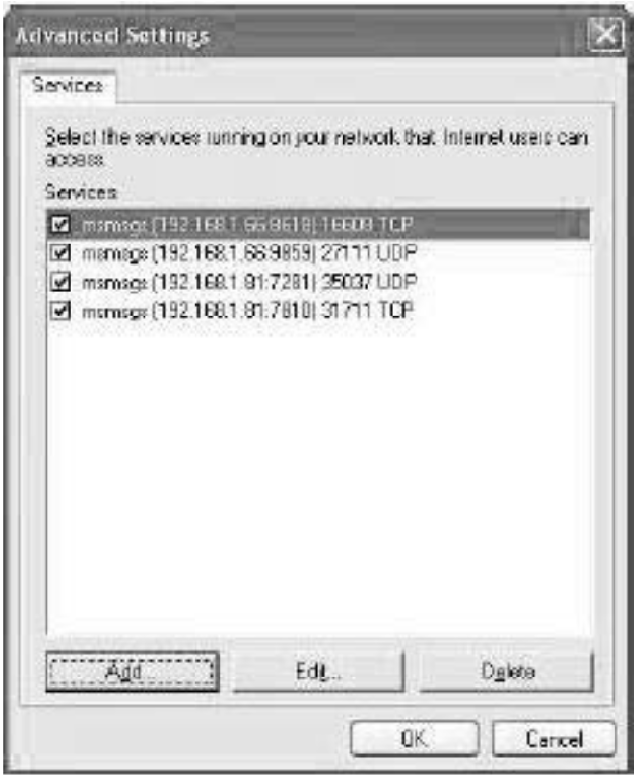
Internet Connection

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

☑ Show icon in notification area when connected

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

Figure 118 Internet Connection Properties: Advanced Settings

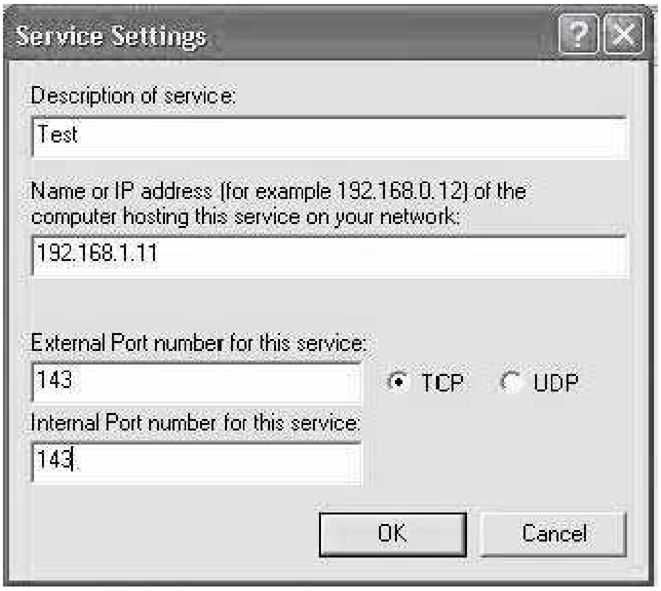


Select the services running on your network that Internet users can access.

Services

☑ msmsgs (192.168.1.66:8618) 16608 TCP
☑ msmsgs (192.168.1.66:9859) 27111 UDP
☑ msmsgs (192.168.1.81:7281) 35037 UDP
☑ msmsgs (192.168.1.81:7810) 31711 TCP

Figure 119 Internet Connection Properties: Advanced Settings: Add



Description of service:
Test

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

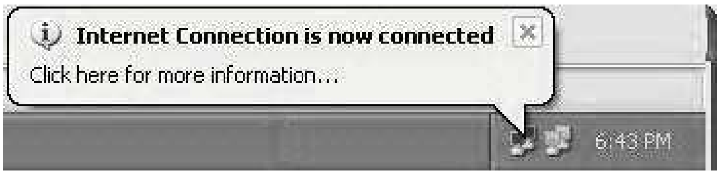
External Port number for this service:
143 ● TCP ○ UDP

Internal Port number for this service:
143

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

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

Figure 120 System Tray Icon

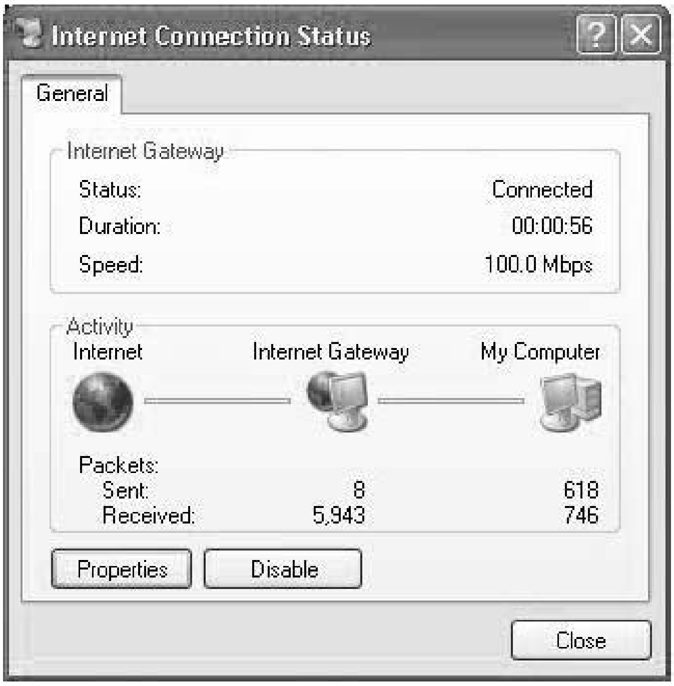


Internet Connection is now connected

Click here for more information...

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

Figure 121 Internet Connection Status



Status: Connected

Duration: 00:00:56

Speed: 100.0 Mbps

Packets:		
Sent:	8	618
Received:	5,943	746

Web Configurator Easy Access

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

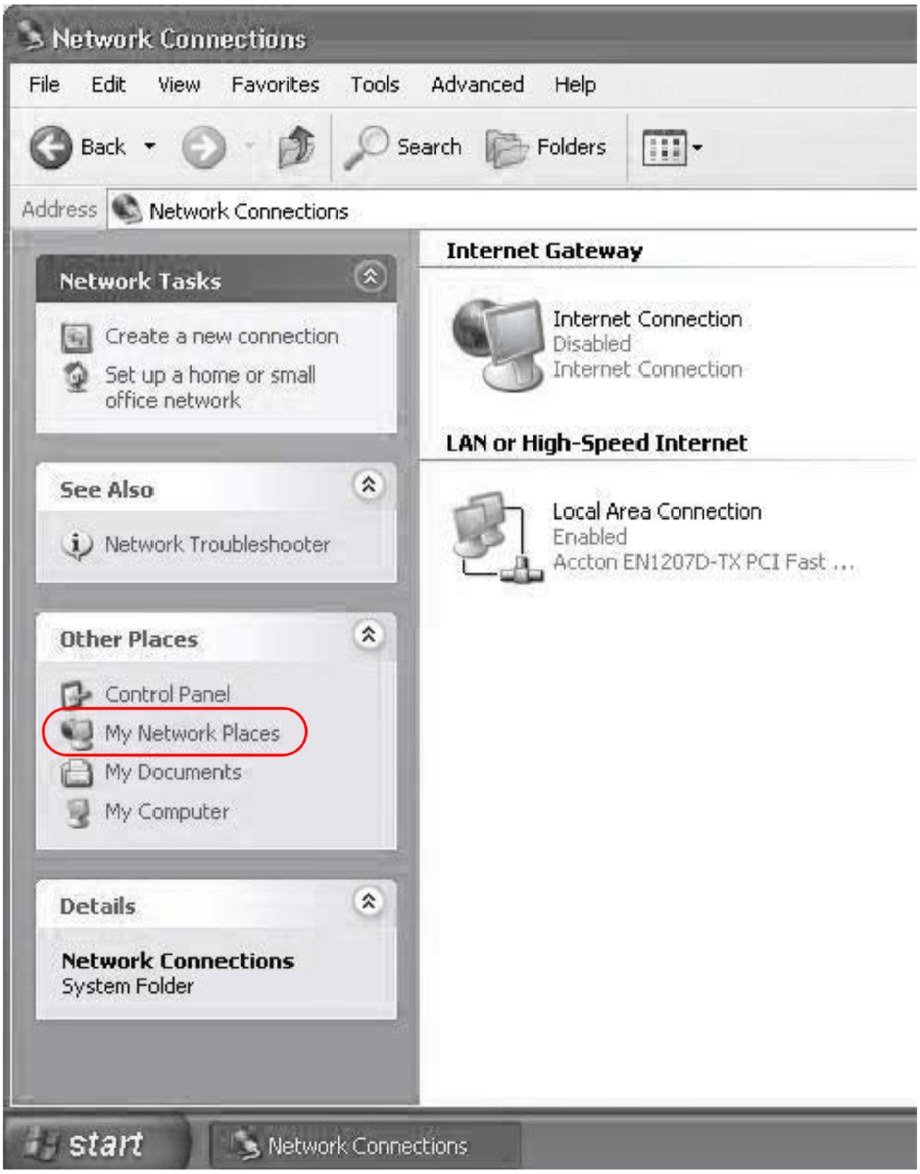
Follow the steps below to access the web configurator.

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

2 Double-click **Network Connections**.

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

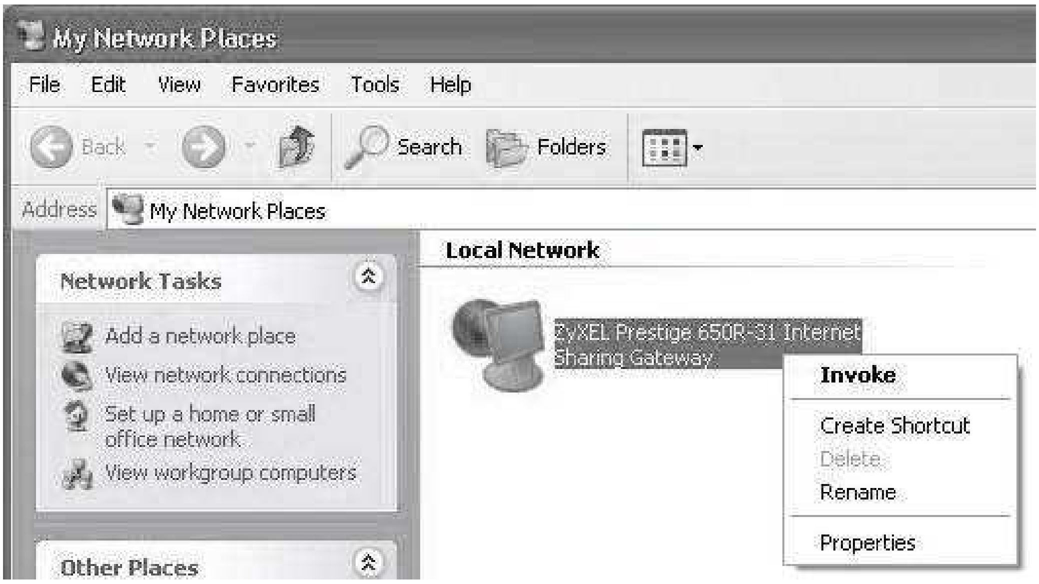
Figure 122 Network Connections



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

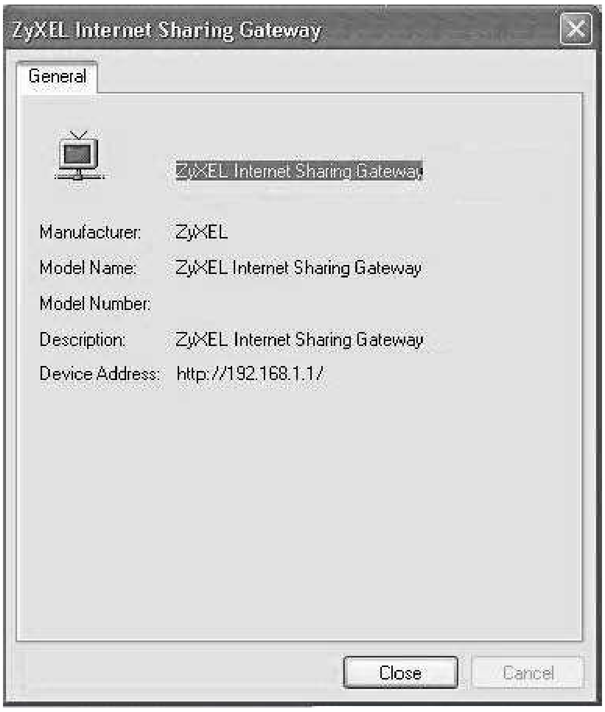
5 Right-click on the icon for your Device and select **Invoke**. The web configurator login screen displays.

Figure 123 Network Connections: My Network Places



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

Figure 124 Network Connections: My Network Places: Properties: Example



ZyXEL Internet Sharing Gateway

Manufacturer: ZyXEL

Model Name: ZyXEL Internet Sharing Gateway

Model Number:

Description: ZyXEL Internet Sharing Gateway

Device Address: http://192.168.1.1/

19

System Settings

19.1 Overview

This chapter shows you how to configure system related settings, such as system time, password, name, the domain name and the inactivity timeout interval.

19.1.1 What You Can Do in this Chapter

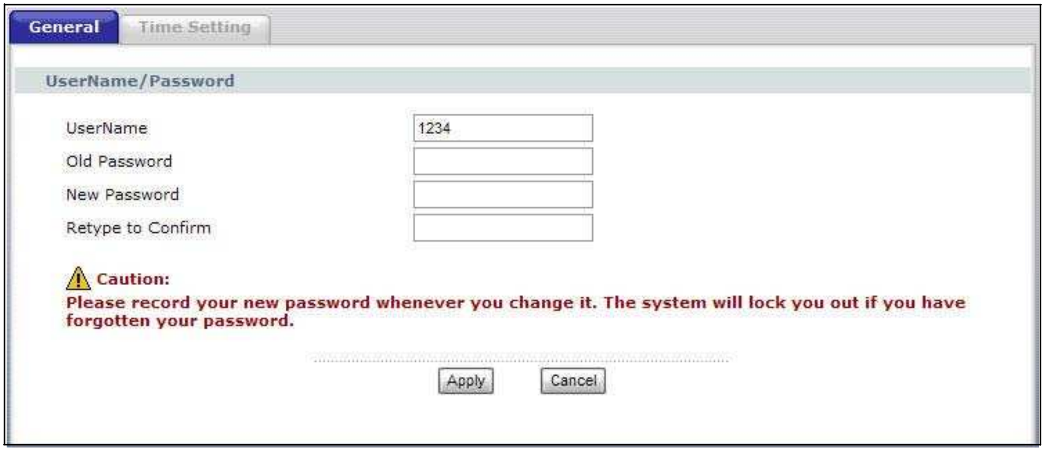
- The **General** screen lets you configure system settings (Section 19.2 on page 227).
- The **Time Setting** screen lets you set the system time (Section 19.3 on page 229).

19.2 The General Screen

Use the **General** screen to configure system settings such as the system password.

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

Figure 125 Maintenance > System > General



UserName/Password

UserName	1234
Old Password	
New Password	
Retype to Confirm	

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

The following table describes the labels in this screen.

Table 74 Maintenance > System > Genera

LABEL	DESCRIPTION
UserName	Type the user name you use to access the system.
Old Password	Type the default password or the existing password you use to access the system in this field.

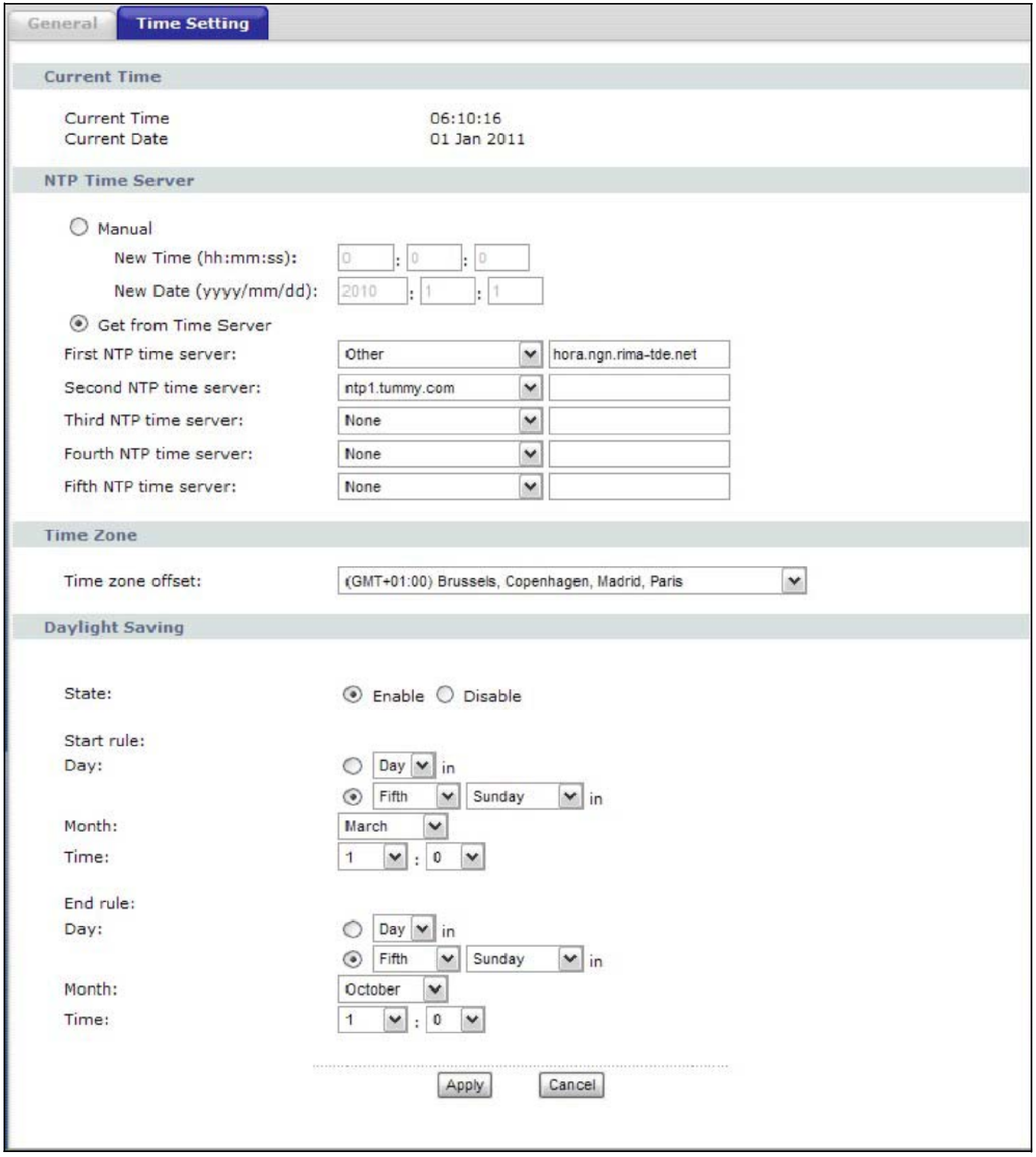
Table 74 Maintenance > System > Genera

LABEL	DESCRIPTION
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the Device.
Retype to Confirm	Type the new password again for confirmation.
Apply	Click **Apply** to save your changes back to the Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

19.3 The Time Setting Screen

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

Figure 126 Maintenance > System > Time Setting



Current Time

Current Time 06:10:16
Current Date 01 Jan 2011

NTP Time Server

○ Manual
New Time (hh:mm:ss): 0 : 0 : 0
New Date (yyyy/mm/dd): 2010 : 1 : 1
● Get from Time Server
First NTP time server: Other hora.ngn.rima-tde.net
Second NTP time server: ntp1.tummy.com
Third NTP time server: None
Fourth NTP time server: None
Fifth NTP time server: None

Time Zone

Time zone offset: (GMT+01:00) Brussels, Copenhagen, Madrid, Paris

Daylight Saving

State: ● Enable ○ Disable

Start rule:
Day: ○ Day in
● Fifth Sunday in
Month: March
Time: 1 : 0

End rule:
Day: ○ Day in
● Fifth Sunday in
Month: October
Time: 1 : 0

The following table describes the fields in this screen.

Table 75 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Current Time	
Current Time	This field displays the time of your Device. Each time you reload this page, the Device synchronizes the time with the time server.

Table 75 Maintenance > System > Time Setting (continued)

LABEL	DESCRIPTION
Current Date	This field displays the date of your Device. Each time you reload this page, the Device synchronizes the date with the time server.
Time and Date Setup	
Manual	Select this option to enter the time and date manually.
Get from Time Server	Select this option to have the Device get the time and date from the time server you specified below.
First NTP time server Second NTP time server Third NTP time server Fourth NTP time server Fifth NTP time server	Select an NTP time server from the drop-down list box. Otherwise, select **Other** and enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Select **None** if you don’t want to configure the time server. Check with your ISP/network administrator if you are unsure of this information.
Time zone offset	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
State	Daylight saving is a period from late spring to fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select **Enable** if you use Daylight Saving Time.
Start rule	Configure the day and time when Daylight Saving Time starts if you selected **Enable**. The **Time** hour field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select the second radio button, **Second**, **Sunday**, **March** and 2 in the **Time** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select the second radio button, **Last**, **Sunday**, **March**. The time you select in the **Time** field depends on your time zone. In Germany for instance, you would use 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End rule	Configure the day and time when Daylight Saving Time ends if you selected **Enable**. The **Time** hour field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and 2 in the **Time** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you select in the **Time** field depends on your time zone. In Germany for instance, you would use 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).

Table 75 Maintenance > System > Time Setting (continued)

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

20

Logs

20.1 Overview

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

The web configurator allows you to choose which categories of events and/or alerts to have the Device log and then display the logs or have the Device send them to a syslog server.

20.1.1 What You Can Do in this Chapter

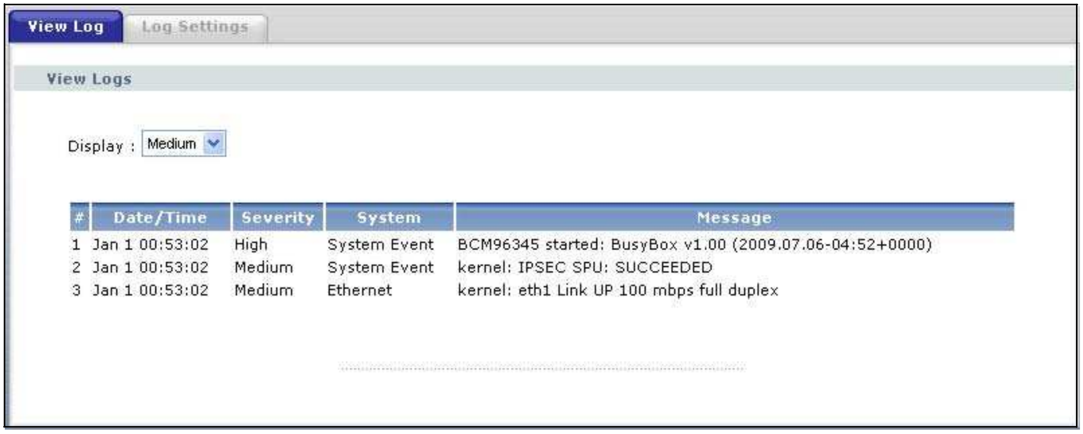
- The **View Log** screen lets you see the logs for the categories that you selected in the **Log Settings** screen (Section 20.2 on page 233).
- The **Log Settings** screen lets you configure to where the Device is to send logs and which logs and/or immediate alerts the Device is to record (Section 20.3 on page 234).

20.2 The View Log Screen

Click **Maintenance > Logs** to open the **View Log** screen. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see Section 20.3 on page 234).

The log wraps around and deletes the old entries after it fills.

Figure 127 Maintenance > Logs > View Log



Display : Medium

#	Date/Time	Severity	System	Message
1	Jan 1 00:53:02	High	System Event	BCM96345 started: BusyBox v1.00 (2009.07.06-04:52+0000)
2	Jan 1 00:53:02	Medium	System Event	kernel: IPSEC SPU: SUCCEEDED
3	Jan 1 00:53:02	Medium	Ethernet	kernel: eth1 Link UP 100 mbps full duplex

The following table describes the fields in this screen.

Table 76 Maintenance > Logs > View Log

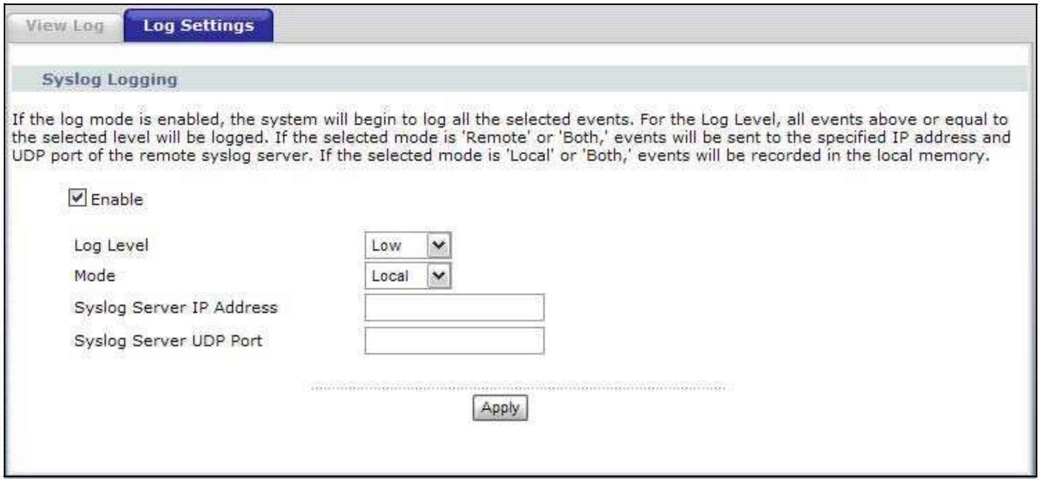
LABEL	DESCRIPTION
Display	Select a severity level of logs to view. The Device displays the logs with the severity level equal to or higher than what you selected.
#	This field is a sequential value and is not associated with a specific entry.
Date/Time	This field displays the time the log was recorded.
Severity	This field displays the severity level of the log.
System	This field displays the system module from which the logs come.
Message	This field states the reason for the log.

20.3 The Log Settings Screen

Use the **Log Settings** screen to configure to where the Device is to send logs and which logs and/or immediate alerts the Device is to record and display.

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

Figure 128 Maintenance > Logs > Log Settings



If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

☑ Enable

Log Level: Low

Mode: Local

Syslog Server IP Address:

Syslog Server UDP Port:

The following table describes the fields in this screen.

Table 77 Maintenance > Logs > Log Settings

LABEL	DESCRIPTION
Enable	Select this to turn on system logging.
Log Level	Select the severity level of the logs that you want the Device to display, record and send to the log server. The Device displays and records the logs with the severity level equal to or higher than what you selected.

Table 77 Maintenance > Logs > Log Settings

LABEL	DESCRIPTION
Mode	Select **Local** to record the logs and store them in the local memory of the Device only. Select **Remote** to send logs to the specified log server. Select **Both** to record the logs and store them in the local memory and also send logs to the log server.
Syslog Server IP Address	Enter the server name or the IP address of the log server.
Syslog Server UDP Port	Enter the UDP port of the log server.
Apply	Click **Apply** to save your customized settings.

21

Tools

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE your Device.

21.1 Overview

This chapter explains how to upload new firmware, manage configuration files and restart your Device.

Use the instructions in this chapter to change the device's configuration file or upgrade its firmware. After you configure your device, you can backup the configuration file to a computer. That way if you later misconfigure the device, you can upload the backed up configuration file to return to your previous settings. You can alternately upload the factory default configuration file if you want to return the device to the original default settings. The firmware determines the device's available features and functionality. You can download new firmware releases from your nearest ZyXEL FTP site (or www.zyxel.com) to use to upgrade your device's performance.

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

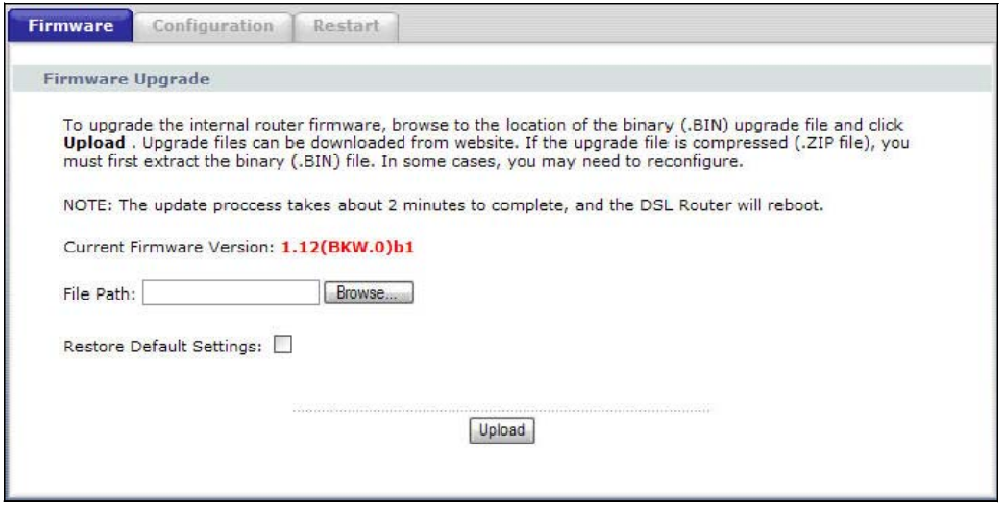
21.1.1 What You Can Do in this Chapter

- The **Firmware** screen lets you upload firmware to your device (Section 21.2 on page 237).
- The **Configuration** screen lets you backup and restore device configurations (Section 21.3 on page 239). You can also reset your device settings back to the factory default.
- The **Restart** screen lets you restart your Device (Section 21.4 on page 241).

21.2 The Firmware Screen

Click **Maintenance > Tools** to open the **Firmware** screen. Follow the instructions in this screen to upload firmware to your Device. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

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



Firmware Upgrade

To upgrade the internal router firmware, browse to the location of the binary (.BIN) upgrade file and click **Upload** . Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure.

NOTE: The update proccess takes about 2 minutes to complete, and the DSL Router will reboot.

Current Firmware Version: 1.12(BKW.0)b1

File Path: Browse...

Restore Default Settings: □

Upload

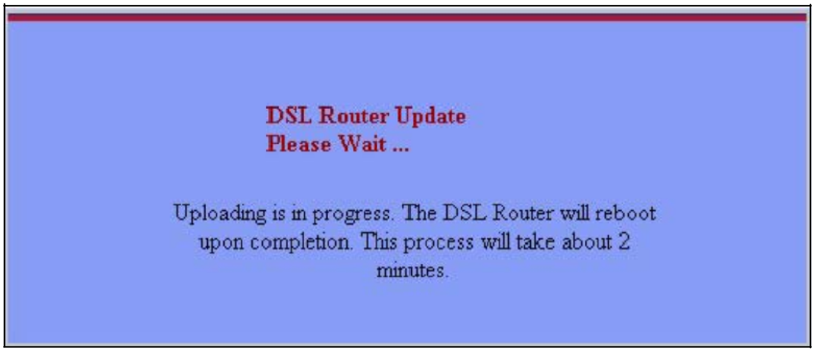
Figure 129 Maintenance > Tools > Firmware

The following table describes the labels in this screen.

Table 78 Maintenance > Tools > Firmware

LABEL	DESCRIPTION
Current Firmware Version	This is the present Firmware version and the date created.
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Restore Default Settings	Select this to also clear all user-entered configuration information and return the Device to its factory defaults.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

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



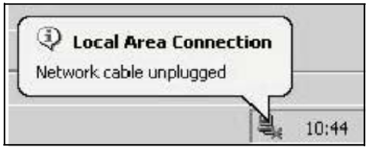
DSL Router Update
Please Wait ...

Uploading is in progress. The DSL Router will reboot upon completion. This process will take about 2 minutes.

Figure 130 Firmware Upload In Progress

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

Figure 131 Network Temporarily Disconnected

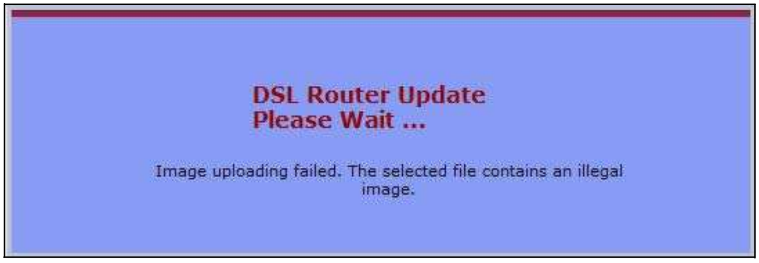


Local Area Connection
Network cable unplugged

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

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

Figure 132 Error Message



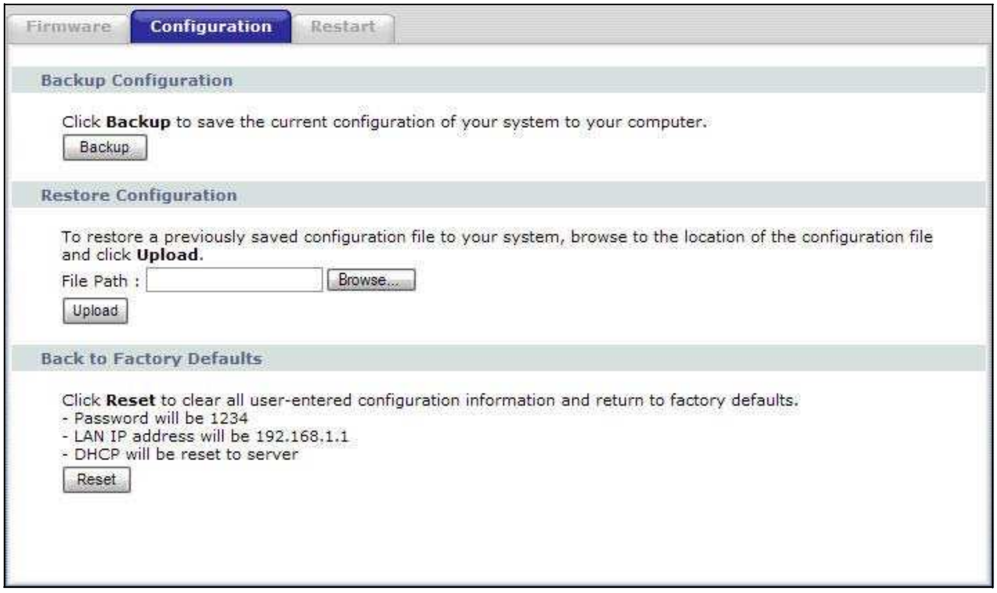
DSL Router Update
Please Wait ...

Image uploading failed. The selected file contains an illegal image.

21.3 The Configuration Screen

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

Figure 133 Maintenance > Tools > Configuration



Backup Configuration

Click **Backup** to save the current configuration of your system to your computer.

Restore Configuration

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click **Upload**.

File Path :

Back to Factory Defaults

Click **Reset** to clear all user-entered configuration information and return to factory defaults.
- Password will be 1234
- LAN IP address will be 192.168.1.1
- DHCP will be reset to server

Backup Configuration

Backup Configuration allows you to back up (save) the Device’s current configuration to a file on your computer. Once your Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the Device’s current configuration to your computer.

Restore Configuration

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

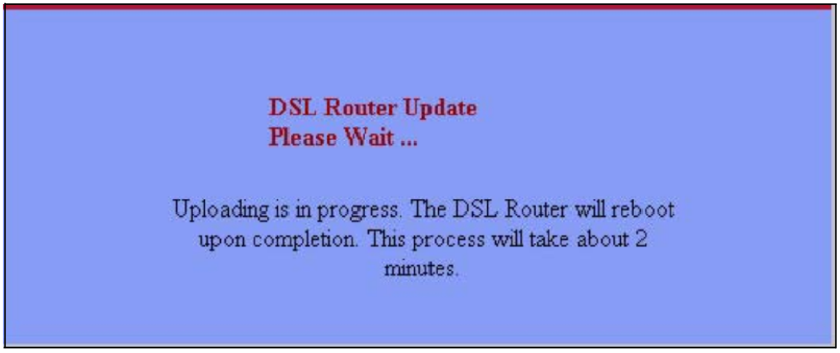
Table 79 Restore Configuration

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

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

After you see a “restore configuration successful” screen, you must then wait one minute before logging into the Device again.

Figure 134 Configuration Upload Successful

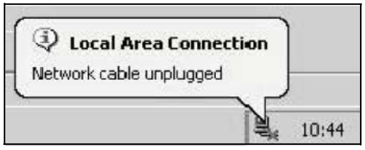


DSL Router Update
Please Wait ...

Uploading is in progress. The DSL Router will reboot upon completion. This process will take about 2 minutes.

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

Figure 135 Network Temporarily Disconnected

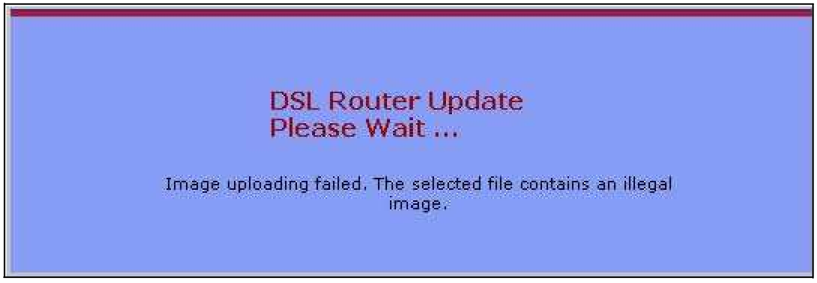


Local Area Connection
Network cable unplugged

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1).

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

Figure 136 Configuration Upload Error



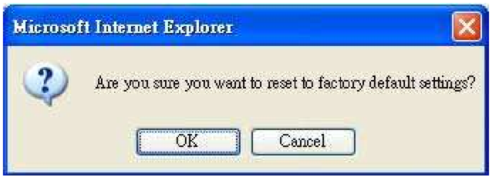
DSL Router Update
Please Wait ...

Image uploading failed. The selected file contains an illegal image.

Reset to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the Device to its factory defaults. The following warning screen appears.

Figure 137 Reset Warning Message



Microsoft Internet Explorer

Are you sure you want to reset to factory default settings?

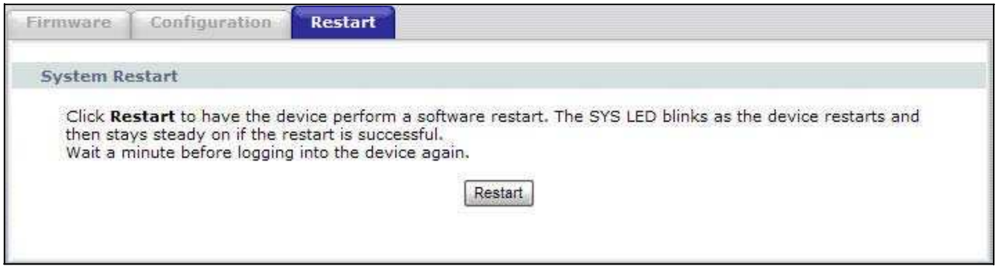
You can also press the **RESET** button on the rear panel to reset the factory defaults of your Device. Refer to Section 1.6 on page 22 for more information on the **RESET** button.

21.4 The Restart Screen

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

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

Figure 138 Maintenance > Tools >Restart



System Restart

Click **Restart** to have the device perform a software restart. The SYS LED blinks as the device restarts and then stays steady on if the restart is successful.
Wait a minute before logging into the device again.

22

Diagnostic

22.1 Overview

The **Diagnostic** screens display information to help you identify problems with the Device.

The route between a CO VDSL switch and one of its CPE may go through switches owned by independent organizations. A connectivity fault point generally takes time to discover and impacts subscriber's network access. In order to eliminate the management and maintenance efforts, IEEE 802.1ag is a Connectivity Fault Management (CFM) specification which allows network administrators to identify and manage connection faults. Through discovery and verification of the path, CFM can detect, analyze and isolate connectivity faults in bridged LANs.

22.1.1 What You Can Do in this Chapter

- The **General** screen lets you ping an IP address or trace the route packets take to a host (Section 22.4 on page 245).
- The **802.1ag** screen lets you perform CFM actions (Section 22.4 on page 245).
- The **OAM Ping Test** screen lets you send an ATM OAM (Operation, Administration and Maintenance) packet to verify the connectivity of a specific PVC. (Section 22.4 on page 245).

22.2 What You Need to Know

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

How CFM Works

A Maintenance Association (MA) defines a VLAN and associated Maintenance End Point (MEP) ports on the device under a Maintenance Domain (MD) level. An MEP port has the ability to send Connectivity Check Messages (CCMs) and get other MEP ports information from neighbor devices' CCMs within an MA.

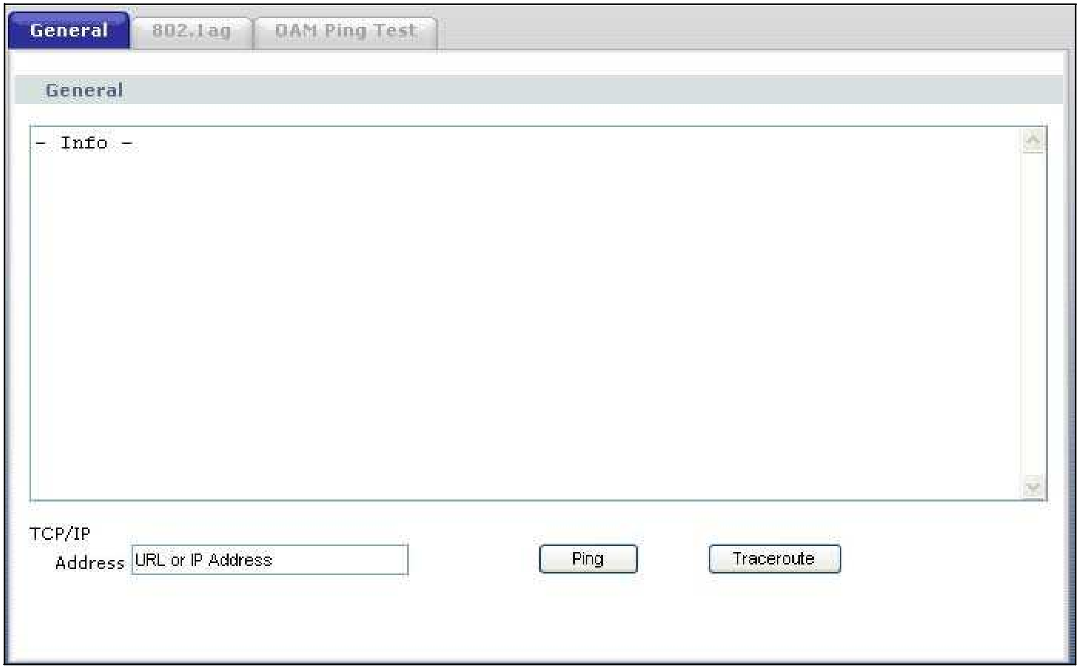
CFM provides two tests to discover connectivity faults.

- Loopback test - checks if the MEP port receives its Loop Back Response (LBR) from its target after it sends the Loop Back Message (LBM). If no response is received, there might be a connectivity fault between them.
- Link trace test - provides additional connectivity fault analysis to get more information on where the fault is. If an MEP port does not respond to the source MEP, this may indicate a fault. Administrators can take further action to check and resume services from the fault according to the line connectivity status report.

22.3 The General Diagnostic Screen

Click **Maintenance > Diagnostic** to open the screen shown next. Ping and traceroute help check availability of remote hosts and also help troubleshoot network or Internet connections.

Figure 139 Maintenance > Diagnostic > General



The following table describes the fields in this screen.

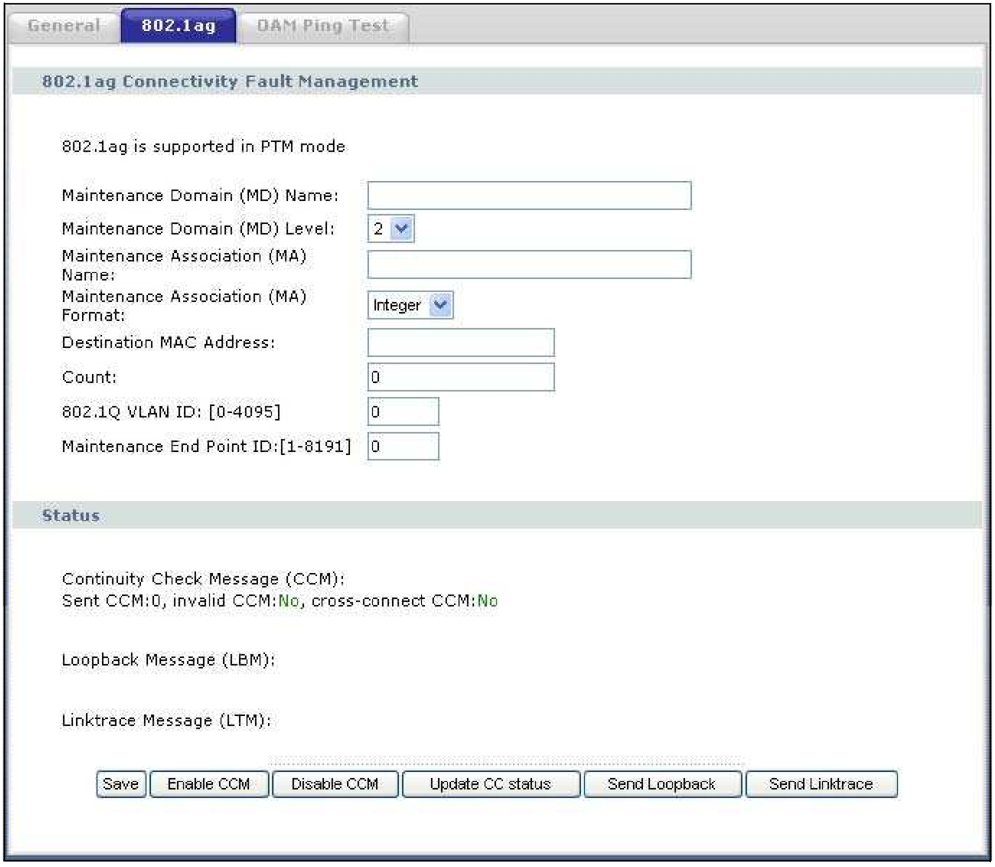
Table 80 Maintenance > Diagnostic > General

LABEL	DESCRIPTION
TCP/IP Address	Type the IP address of a computer that you want to ping in order to test a connection or trace the route packets take to.
Ping	Click this button to ping the IP address that you entered.
Traceoute	Click this button to perform the traceroute function. This determines the path a packet takes to the specified host.

22.4 The 802.1ag Screen

Click **Maintenance > Diagnostic** > **8.2.1ag** to open the following screen. Use this screen to perform CFM actions.

Figure 140 802.1ag



802.1ag Connectivity Fault Management

802.1ag is supported in PTM mode

Maintenance Domain (MD) Name:

Maintenance Domain (MD) Level: 2

Maintenance Association (MA) Name:

Maintenance Association (MA) Format: Integer

Destination MAC Address:

Count: 0

802.1Q VLAN ID: [0-4095] 0

Maintenance End Point ID:[1-8191] 0

Status

Continuity Check Message (CCM):
Sent CCM:0, invalid CCM:No, cross-connect CCM:No

Loopback Message (LBM):

Linktrace Message (LTM):

The following table describes the fields in this screen.

Table 81 Maintenance > Diagnostic > 802.1ag

LABEL	DESCRIPTION
802.1ag Connectivity Fault Management	
Maintenance Domain (MD) Name	Type a name of up to 39 printable English keyboard characters for this MD. The combined length of the MD Name and MA name must be less or equal to 44bytes.
Maintenance Domain (MD) Level	Select a level (0-7) under which you want to create an MA.
Maintenance Association (MA) Name	Type a name of up to 39 printable English keyboard characters for this MA. The combined length of the MD Name and MA name must be less or equal to 44bytes.

Table 81 Maintenance > Diagnostic > 802.1ag (continued)

LABEL	DESCRIPTION
Maintenance Association (MA) Format	Select the format which the Device uses to send this MA information in the domain (MD). Options are **VID**, **String** and **Integer**. If you select **VID** or **Integer**, the Device adds the VLAN ID you specified for an MA in the CCM. If you select **String**, the Device adds the MA name you specified above in the CCM. Note: The MEPs in the same MA should use the same MA format.
Destination MAC Address	Enter the target device's MAC address to which the Device performs a CFM loopback test.
Count	Set how many times the Device send loopback messages (LBMs).
802.1Q VLAN ID	Type a VLAN ID (0-4095) for this MA.
Maintenance End Point ID	Enter an ID number (1-8191) for this MEP port. Each MEP port needs a unique ID number within an MD. The MEP ID is to identify an MEP port used when you perform a CFM action
Status	
Continuity Check Message (CCM)	This shows how many Connectivity Check Messages (CCMs) are sent and if there is any invalid CCM or cross-connect CCM.
Loopback Message (LBM)	This shows how many Loop Back Messages (LBMs) are sent and if there is any inorder or outorder Loop Back Response (LBR) received from a remote MEP.
Linktrace Message (LTM)	This shows the destination MAC address in the Link Trace Response (LTR).
Save	Click this to save your changes back to the Device.
Enable CCM	Click this button to have the selected MEP send Connectivity Check Messages (CCMs) to other MEPs.
Disable CCM	Click this button to disallow the selected MEP to send Connectivity Check Messages (CCMs) to other MEPs.
Update CC status	Click this button to reload the test result.
Send Loopback	Click this button to have the selected MEP send the LBM (Loop Back Message) to a specified remote end point.
Send Linktrace	Click this button to have the selected MEP send the LTMs (Link Trace Messages) to a specified remote end point.

22.5 The OAM Ping Test Screen

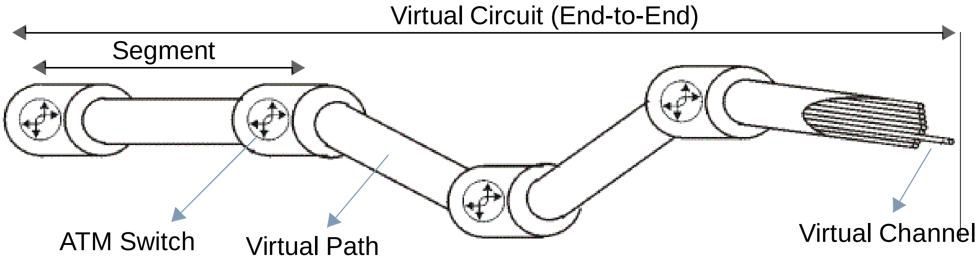
Click **Maintenance > Diagnostic > OAM Ping Test** to open the screen shown next. Use this screen to perform an OAM (Operation, Administration and Maintenance) F4 or F5 loopback test on a

PVC. The Device sends an OAM F4 or F5 packet to the DSLAM or ATM switch and then returns it to the Device. The test result then displays in the text box.

ATM sets up virtual circuits over which end systems communicate. The terminology for virtual circuits is as follows:

• Virtual Channel (VC)	Logical connections between ATM devices
• Virtual Path (VP)	A bundle of virtual channels
• Virtual Circuits	A series of virtual paths between circuit end points

Figure 141 Virtual Circuit Topology



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

F4 cells operate at the virtual path (VP) level, while F5 cells operate at the virtual channel (VC) level. F4 cells use the same VPI as the user data cells on VP connections, but use different predefined VCI values. F5 cells use the same VPI and VCI as the user data cells on the VC connections, and are distinguished from data cells by a predefinded Payload Type Identifier (PTI) in the cell header. Both F4 flows and F5 flows are bidirectional and have two types.

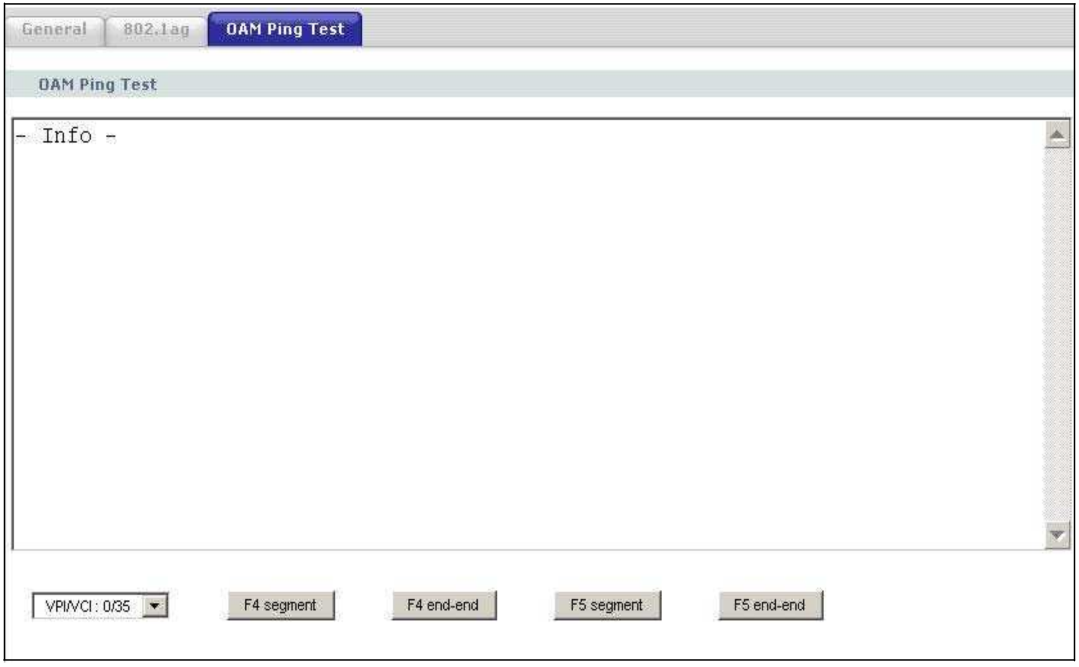
- segment F4 flows (VCI=3)
- end-to-end F4 flows (VCI=4)
- segment F5 flows (PTI=100)
- end-to-end F5 flows (PTI=101)

OAM F4 or F5 tests are used to check virtual path or virtual channel availability between two DSL devices. Segment flows are terminated at the connecting point which terminates a VP or VC segment. End-to-end flows are terminated at the end point of a VP or VC connection, where an ATM link is terminated. Segment loopback tests allow you to verify integrity of a PVC to the nearest neighboring ATM device. End-to-end loopback tests allow you to verify integrity of an end-to-end PVC.

Note: The DSLAM to which the Device is connected must also support ATM F4 and/or F5 to use this test.

Note: This screen is available only when you configure an ATM layer-2 interface.

Figure 142 Maintenance > Diagnostic > OAM Ping Test



The following table describes the fields in this screen.

Table 82 Maintenance > Diagnostic > OAM Ping Test

LABEL	DESCRIPTION
	Select a PVC on which you want to perform the loopback test.
F4 segment	Press this to perform an OAM F4 segment loopback test.
F4 end-end	Press this to perform an OAM F4 end-to-end loopback test.
F5 segment	Press this to perform an OAM F5 segment loopback test.
F5 end-end	Press this to perform an OAM F5 end-to-end loopback test.

23

Troubleshooting

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

- Power, Hardware Connections, and LEDs
- Device Access and Login
- Internet Access
- Wireless LAN Troubleshooting

23.1 Power, Hardware Connections, and LEDs

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

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

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.7 on page 23.
2. Check the hardware connections.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Turn the Device off and on.
5. If the problem continues, contact the vendor.

23.2 Device Access and Login

I forgot the IP address for the Device.

1 The default IP address is **192.168.1.1**.

2 If you changed the IP address and have forgotten it, you might get the IP address of the Device by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the Device (it depends on the network), so enter this IP address in your Internet browser.

3 If this does not work, you have to reset the device to its factory defaults. See Section 1.6 on page 22.

I forgot the password.

1 The default password can be found on the cover of this User's Guide.

2 If this does not work, you have to reset the device to its factory defaults. See Section 1.6 on page 22.

I cannot see or access the **Login** screen in the web configurator.

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.1.1.
- If you changed the IP address (Section on page 122), use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the Device.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.

3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See Appendix A on page 261.

4 Reset the device to its factory defaults, and try to access the Device with the default IP address. See Section 1.6 on page 22.

5 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- If your computer is connected wirelessly, use a computer that is connected to a **ETHERNET** port.

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

1 Make sure you have entered the user name and password correctly. The default user name and password can be found on the cover of this User's Guide. These fields are case-sensitive, so make sure [Caps Lock] is not on.

2 Turn the Device off and on.

3 If this does not work, you have to reset the device to its factory defaults. See Section 23.1 on page 249.

23.3 Internet Access

I cannot access the Internet.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.7 on page 23.

2 Make sure you entered your ISP account information correctly in the WAN screens. These fields are case-sensitive, so make sure [Caps Lock] is not on.

3 If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.

4 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.

5 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the Device), but my Internet connection is not available anymore.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.7 on page 23.

2 Turn the Device off and on.

3 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1 There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.7 on page 23. If the Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

2 Check the signal strength. If the signal strength is low, try moving your computer closer to the Device if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).

3 Turn the Device off and on.

4 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Check the settings for QoS. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.

I cannot connect to the Internet using a second DSL connection.

ADSL and VDSL connections cannot work at the same time. You can only use one type of DSL connection, either ADSL or VDSL connection at one time.

I cannot create multiple connections of the same type.

Your layer-2 interface must be in VLAN MUX Mode to create multiple WAN services for each connection.

23.4 Wireless LAN Troubleshooting

I cannot access the Device or ping any computer from the WLAN (wireless AP or router).

1 Make sure the wireless LAN is enabled on the Device.

2 Make sure the wireless adapter on the wireless station is working properly.

3 Make sure the wireless adapter installed on your computer is IEEE 802.11 compatible and supports the same wireless standard as the Device.

4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the Device.

5 Check that both the Device and your wireless station are using the same wireless and wireless security settings.

6 Make sure traffic between the WLAN and the LAN is not blocked by the firewall on the Device.

7 Make sure you allow the Device to be remotely accessed through the WLAN interface. Check your remote management settings.

- See Chapter 7 Wireless LAN in the User's Guide for more information.

8 Check if MAC Filter is configured to deny wireless access to certain MAC addresses to the Device.

Product Specifications

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

24.1 Hardware Specifications

Table 83 Hardware Specifications

Dimensions	231(W) x 147(D) x 57(H) mm
Weight	950g
Power Specification	12 V DC 1.5 A
Built-in Switch	Four auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports
RESET Button	Restores factory defaults
Antenna	Two external dipole 2dBi antennas
WPS Button	3 seconds: turn on or off WLAN 8 seconds: enable WPS (Wi-Fi Protected Setup)
Operation Temperature	0º C ~ 40º C
Storage Temperature	-20º ~ 60º C
Operation Humidity	20% ~ 85% RH
Storage Humidity	20% ~ 90% RH

24.2 Firmware Specifications

Table 84 Firmware Specifications

Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default User Name	1234
Default Password	1234
DHCP Server IP Pool	192.168.1.33 to 192.168.1.199
Static Routes	16
Device Management	Use the web configurator to easily configure the rich range of features on the Device.

Table 84 Firmware Specifications (continued)

Wireless Functionality (wireless devices only)	Allow the IEEE 802.11b, IEEE 802.11g and/or IEEE 802.11n wireless clients to connect to the Device wirelessly. Enable wireless security (WEP, WPA(2), WPA(2)-PSK) and/or MAC filtering to protect your wireless network.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator to put it on the Device. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the Device’s configuration. You can put it back on the Device later if you decide to revert back to an earlier configuration.
Port Forwarding	If you have a server (mail or web server for example) on your network, you can use this feature to let people access it from the Internet.
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the Device assign IP addresses, an IP default gateway and DNS servers to computers on your network. Your device can also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients.
DHCPv6	Use this feature to have the ZyXEL Device assign IPv6 addresses, an IPv6 default gateway and IPv6 DNS servers to computers on your network.
Dynamic DNS Support	With Dynamic DNS (Domain Name System) support, you can use a fixed URL, www.zyxel.com for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.
IP Multicast	IP multicast is used to send traffic to a specific group of computers. The Device supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).
Time and Date	Get the current time and date from an external server when you turn on your Device. You can also set the time manually. These dates and times are then used in logs.
Logs	Use logs for troubleshooting. You can send logs from the Device to an external syslog server.
Universal Plug and Play (UPnP)	A UPnP-enabled device can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.
QoS (Quality of Service)	You can efficiently manage traffic on your network by reserving bandwidth and giving priority to certain types of traffic and/or to particular computers.
Remote Management	This allows you to decide whether a service (HTTP or FTP traffic for example) from a computer on a network (LAN or WAN for example) can access the Device.
PPPoE Support (RFC2516)	PPPoE (Point-to-Point Protocol over Ethernet) emulates a dial-up connection. It allows your ISP to use their existing network configuration with newer broadband technologies such as ADSL. The PPPoE driver on your device is transparent to the computers on the LAN, which see only Ethernet and are not aware of PPPoE thus saving you from having to manage PPPoE clients on individual computers.
Other PPPoE Features	PPPoE idle time out PPPoE dial on demand
IP Alias	IP alias allows you to partition a physical network into logical networks over the same Ethernet interface. Your device supports three logical LAN interfaces via its single physical Ethernet interface with the your device itself as the gateway for each LAN network.
Packet Filters	Your device’s packet filtering function allows added network security and management.

Table 84 Firmware Specifications (continued)

VDSL Standards	VDSL line coding: ITU-T G.993.2 DMT modulation DSL handshake procedure protocol: ITU-T G.994.1 DSL physical layer management protocol: ITU-T G.997.1 VDSL band plan: 997 and 998 Support U0 band VDSL profiles: 8a, 8b, 8c, 8d, 12a, 12b, 17a VDSL speed: up to 100/50 Mbps@ 700 feet Support Annex A, Annex B and 5-band VDSL2 Rate adaptation OLR: Bit Swapping/ SRA (Seamless Rate Adaption) Upstream power back-off (UPBO) VDSL OAM communication channels: Indicator bits (IB) channel, VDSL embedded operations channel (EOC) and VDSL overhead control channel (VOC) PTM Transmission Convergence (PTM-TC) Dual-latency xDSL framing (fast and interleaved) Trellis coding INP capability: At least two symbols protection (INP_MIN = 2), up to 16 symbols (INP_MIN = 16) ATM and PTM (dual-priority) ADSL/ADSL2/ADSL2+ fall back
ADSL Standards	Multi-Mode standard (ANSI T1.413,Issue 2; G.dmt(G.992.1); G.lite(G992.2)), Annex A ADSL2 G.dmt.bis (G.992.3), Annex A and M ADSL2+ (G.992.5), Annex A and M Reach-Extended ADSL (RE ADSL) SRA (Seamless Rate Adaptation) Auto-negotiating rate adaptation ADSL physical connection ATM AAL5 (ATM Adaptation Layer type 5) Multi-protocol over AAL5 (RFC2684/1483) PPP over ATM AAL5 (RFC 2364) PPP over Ethernet (RFC 2516) VC-based and LLC-based multiplexing Up to 8 PVCs (Permanent Virtual Circuits) in VLAN Mux Mode ATM traffic shaping (CBR, VBR-rt/nrt, UBR) ITU-T I.610 F4/F5 OAM

Table 84 Firmware Specifications (continued)

Other Protocol Support	PPP (Point-to-Point Protocol) link layer protocol Transparent bridging for unsupported network layer protocols RIP I/RIP II ICMP IP Multicasting IGMP v1 and v2 IGMP Proxy
Management	Embedded Web Configurator Remote Firmware Upgrade Syslog TR-069

24.3 Wireless Features

Table 85 Wireless Features

External Antenna	The Device is equipped with an attached antenna to provide a clear radio signal between the wireless stations and the access points.
Wireless LAN MAC Address Filtering	Your device can check the MAC addresses of wireless stations against a list of allowed or denied MAC addresses.
WEP Encryption	WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network to help keep network communications private.
Wi-Fi Protected Access	Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security standard. Key differences between WPA and WEP are user authentication and improved data encryption.

Table 85 Wireless Features

WPA2	WPA 2 is a wireless security standard that defines stronger encryption, authentication and key management than WPA.
Other Wireless Features	IEEE 802.11n Compliance Frequency Range: 2.4 GHz ISM Band Advanced Orthogonal Frequency Division Multiplexing (OFDM) Data Rates: 54Mbps, 11Mbps, 5.5Mbps, 2Mbps, and 1 Mbps Auto Fallback WPA2 WMM IEEE 802.11i IEEE 802.11e Wired Equivalent Privacy (WEP) Data Encryption 64/128 bit WLAN bridge to LAN Up to 32 MAC Address filters IEEE 802.1x Store up to 32 built-in user profiles using EAP-MD5 (Local User Database) External RADIUS server using EAP-MD5, TLS, TTLS

The following list, which is not exhaustive, illustrates the standards supported in the Device.

Table 86 Standards Supported

STANDARD	DESCRIPTION
RFC 1058	RIP-1 (Routing Information Protocol)
RFC 1112	IGMP v1
RFC 1631	IP Network Address Translator (NAT)
RFC 1661	The Point-to-Point Protocol (PPP)
RFC 1723	RIP-2 (Routing Information Protocol)
RFC 1981	Path MTU Discovery for IPv6
RFC 2236	Internet Group Management Protocol, Version 2.
RFC 2364	PPP over AAL5 (PPP over ATM over ADSL)
RFC 2408	Internet Security Association and Key Management Protocol (ISAKMP)
RFC 2460	IPv6 Specification
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2684	Multiprotocol Encapsulation over ATM Adaptation Layer 5.
RFC 2766	Network Address Translation - Protocol
RFC 3484	Default Address Selection for IPv6
RFC 4291	IPv6 Addressing Architecture
RFC 4443	ICMPv6
RFC 4861	Neighbor Discovery for IPv6
RFC 4862	IPv6 Stateless Address Autoconfiguration

Table 86 Standards Supported (continued)

STANDARD	DESCRIPTION
IEEE 802.11	Also known by the brand Wi-Fi, denotes a set of Wireless LAN/WLAN standards developed by working group 11 of the IEEE LAN/MAN Standards Committee (IEEE 802).
IEEE 802.11b	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11g	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11n	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11d	Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges
IEEE 802.11x	Port Based Network Access Control.
IEEE 802.11e QoS	IEEE 802.11 e Wireless LAN for Quality of Service
ITU-T G.993.2 (VDSL2)	ITU standard that defines VDSL2.
TR-069	DSL Forum Standard for CPE Wan Management.
TR-064	DSL Forum LAN-Side DSL CPE Configuration

Pop-up Windows, JavaScripts and Java Permissions

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

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

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

Internet Explorer Pop-up Blockers

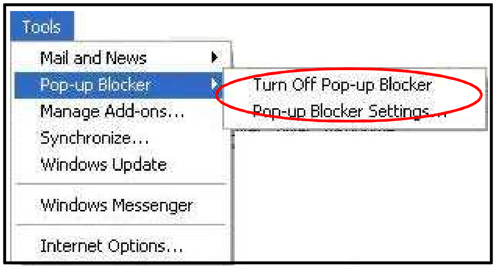
You may have to disable pop-up blocking to log into your device.

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

Disable Pop-up Blockers

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

Figure 143 Pop-up Blocker

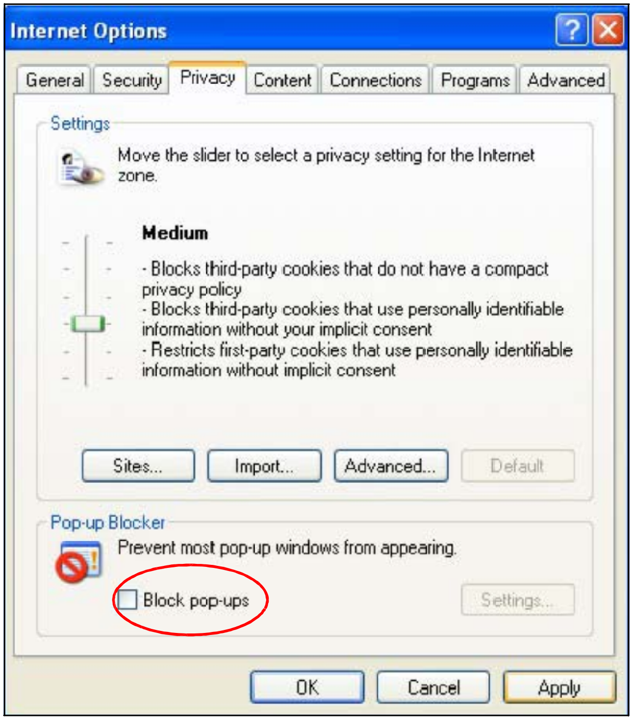


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 144 Internet Options: Privacy



Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

Prevent most pop-up windows from appearing.

□ Block pop-ups

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

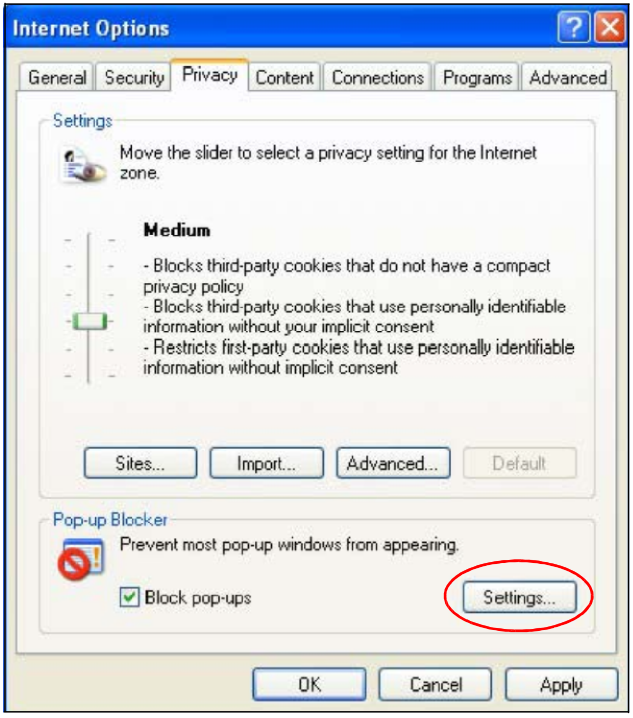
Enable Pop-up Blockers with Exceptions

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

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings...**to open the **Pop-up Blocker Settings** screen.

Figure 145 Internet Options: Privacy



Settings

Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

Pop-up Blocker

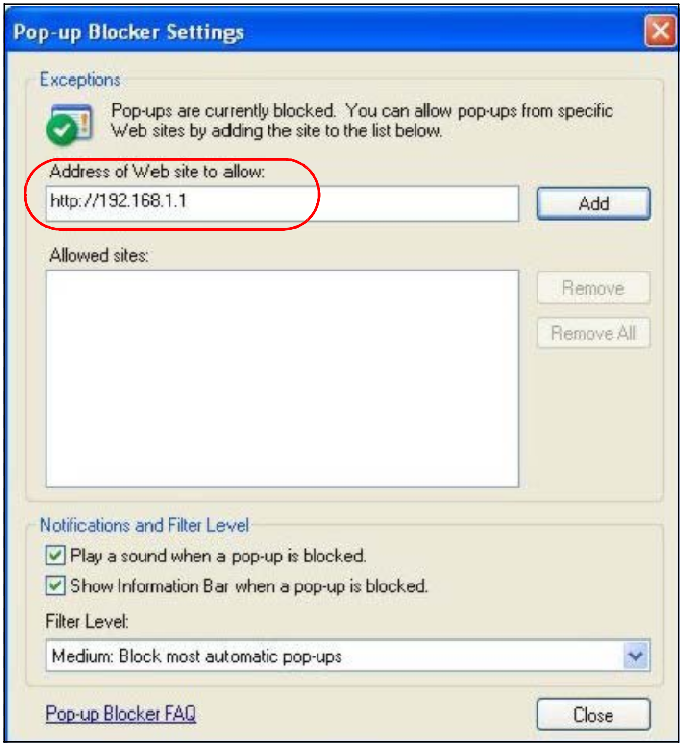
Prevent most pop-up windows from appearing.

☑ Block pop-ups

3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.167.1.

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

Figure 146 Pop-up Blocker Settings



Address of Web site to allow: http://192.168.1.1

☑ Play a sound when a pop-up is blocked.

☑ Show Information Bar when a pop-up is blocked.

Filter Level: Medium: Block most automatic pop-ups

Pop-up Blocker Settings
Exceptions
Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.
Add
Allowed sites:
Remove
Remove All
Notifications and Filter Level
Pop-up Blocker FAQ
Close

5 Click **Close** to return to the **Privacy** screen.

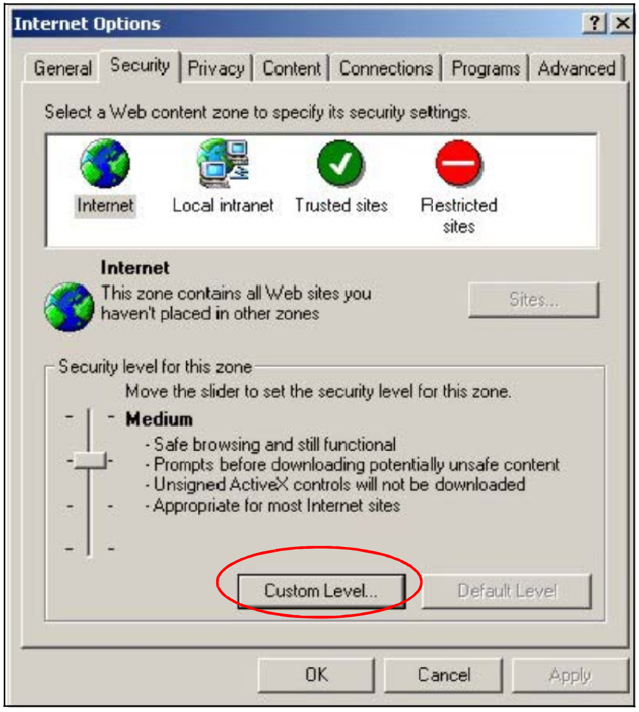
6 Click **Apply** to save this setting.

JavaScripts

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

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

Figure 147 Internet Options: Security



Select a Web content zone to specify its security settings.

Internet

This zone contains all Web sites you haven't placed in other zones

Move the slider to set the security level for this zone.

Medium

- Safe browsing and still functional
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded
- Appropriate for most Internet sites

2 Click the **Custom Level...** button.

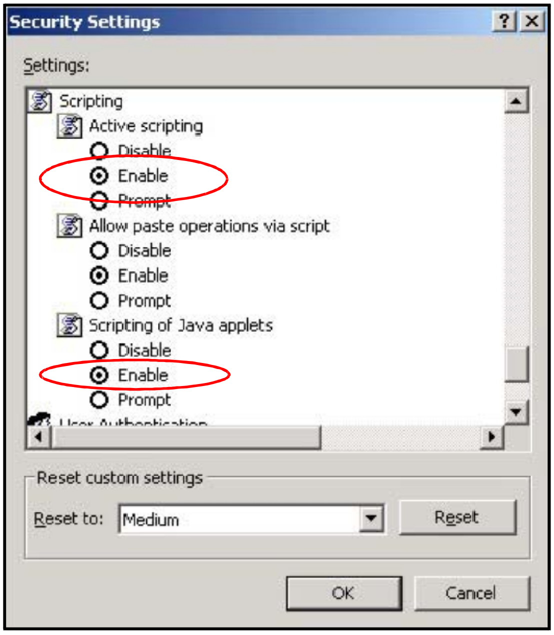
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 148 Security Settings - Java Scripting



Security Settings

Settings:

Scripting

Active scripting

○ Disable

● Enable

○ Prompt

Allow paste operations via script

○ Disable

● Enable

○ Prompt

Scripting of Java applets

○ Disable

● Enable

○ Prompt

User Authentication

Reset custom settings

Reset to: Medium

Java Permissions

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

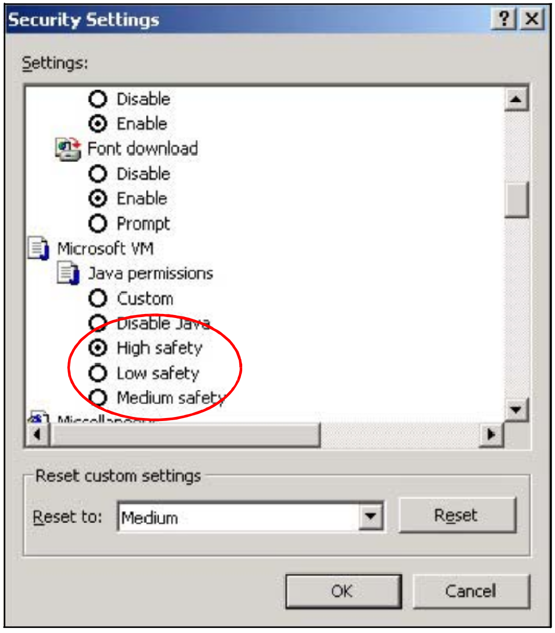
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

Figure 149 Security Settings - Java



Security Settings

Settings:

○ Disable
● Enable
Font download
○ Disable
● Enable
○ Prompt
Microsoft VM
Java permissions
○ Custom
○ Disable Java
● High safety
○ Low safety
○ Medium safety

Reset custom settings

Reset to: Medium

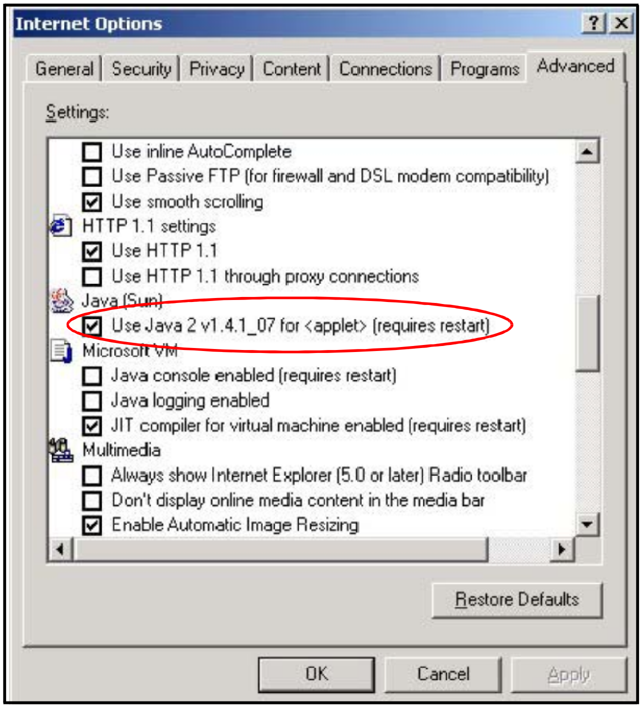
JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 150 Java (Sun)



- ☐ Use inline AutoComplete
- ☐ Use Passive FTP (for firewall and DSL modem compatibility)
- ☑ Use smooth scrolling

HTTP 1.1 settings

- ☑ Use HTTP 1.1
- ☐ Use HTTP 1.1 through proxy connections

Java (Sun)

- ☑ Use Java 2 v1.4.1_07 for <applet> (requires restart)

Microsoft VM

- ☐ Java console enabled (requires restart)
- ☐ Java logging enabled
- ☑ JIT compiler for virtual machine enabled (requires restart)

Multimedia

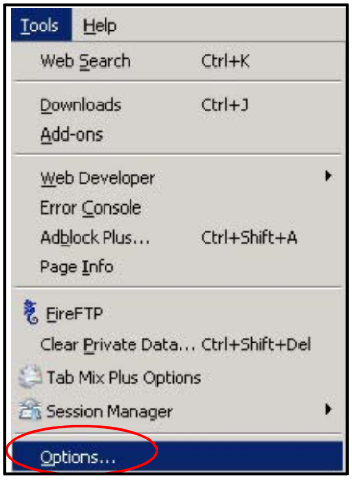
- ☐ Always show Internet Explorer (5.0 or later) Radio toolbar
- ☐ Don't display online media content in the media bar
- ☑ Enable Automatic Image Resizing

Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary.

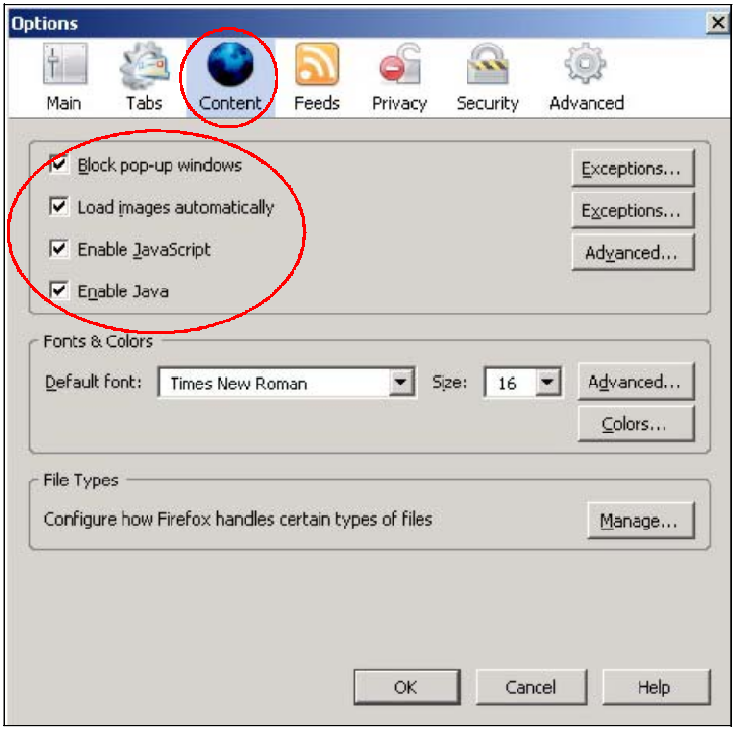
You can enable Java, Javascripts and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

Figure 151 Mozilla Firefox: Tools > Options



Click **Content**.to show the screen below. Select the check boxes as shown in the following screen.

Figure 152 Mozilla Firefox Content Security



☑ Block pop-up windows

☑ Load images automatically

☑ Enable JavaScript

☑ Enable Java

Fonts & Colors

Default font: Times New Roman Size: 16

File Types

Configure how Firefox handles certain types of files

B

IPv6

Overview

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 x 10^{38} IP addresses.

IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as "/x" where x is a number. For example,

```
2001:db8:1a2b:15::1a2f:0/32
```

means that the first 32 bits (`2001:db8`) is the subnet prefix.

Link-local Address

A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a "private IP address" in IPv4. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of fe80::/10. The link-local unicast address format is as follows.

Table 87 Link-local Unicast Address Format

1111 1110 10	0	Interface ID
10 bits	54 bits	64 bits

Global Address

A global address uniquely identifies a device on the Internet. It is similar to a "public IP address" in IPv4. A global unicast address starts with a 2 or 3.

Unspecified Address

An unspecified address (0:0:0:0:0:0:0:0 or ::) is used as the source address when a device does not have its own address. It is similar to "0.0.0.0" in IPv4.

Loopback Address

A loopback address (0:0:0:0:0:0:0:1 or ::1) allows a host to send packets to itself. It is similar to "127.0.0.1" in IPv4.

Multicast Address

In IPv6, multicast addresses provide the same functionality as IPv4 broadcast addresses. Broadcasting is not supported in IPv6. A multicast address allows a host to send packets to all hosts in a multicast group.

Multicast scope allows you to determine the size of the multicast group. A multicast address has a predefined prefix of ff00::/8. The following table describes some of the predefined multicast addresses.

Table 88 Predefined Multicast Address

MULTICAST ADDRESS	DESCRIPTION
FF01:0:0:0:0:0:0:1	All hosts on a local node.
FF01:0:0:0:0:0:0:2	All routers on a local node.
FF02:0:0:0:0:0:0:1	All hosts on a local connected link.
FF02:0:0:0:0:0:0:2	All routers on a local connected link.
FF05:0:0:0:0:0:0:2	All routers on a local site.
FF05:0:0:0:0:0:1:3	All DHCP severs on a local site.

The following table describes the multicast addresses which are reserved and can not be assigned to a multicast group.

Table 89 Reserved Multicast Address

MULTICAST ADDRESS
FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0

Table 89 Reserved Multicast Address (continued)

MULTICAST ADDRESS
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

Subnet Masking

Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block's 16 bits are then represented by four hexadecimal characters. For example, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

Interface ID

In IPv6, an interface ID is a 64-bit identifier. It identifies a physical interface (for example, an Ethernet port) or a virtual interface (for example, the management IP address for a VLAN). One interface should have a unique interface ID.

EUI-64

The EUI-64 (Extended Unique Identifier) defined by the IEEE (Institute of Electrical and Electronics Engineers) is an interface ID format designed to adapt with IPv6. It is derived from the 48-bit (6-byte) Ethernet MAC address as shown next. EUI-64 inserts the hex digits fffe between the third and fourth bytes of the MAC address and complements the seventh bit of the first byte of the MAC address. See the following example.

MAC	00	:	13	:	49	:	12	:	34	:	56				
EUI-64	02	:	13	:	49	:	FF	:	FE	:	12	:	34	:	56

Stateless Autoconfiguration

With stateless autoconfiguration in IPv6, addresses can be uniquely and automatically generated. Unlike DHCPv6 (Dynamic Host Configuration Protocol version six) which is used in IPv6 stateful autoconfiguration, the owner and status of addresses don't need to be maintained by a DHCP server. Every IPv6 device is able to generate its own and unique IP address automatically when IPv6 is initiated on its interface. It combines the prefix and the interface ID (generated from its own Ethernet MAC address, see Interface ID and EUI-64) to form a complete IPv6 address.

When IPv6 is enabled on a device, its interface automatically generates a link-local address (beginning with fe80).

When the interface is connected to a network with a router and the Device is set to automatically obtain an IPv6 network prefix from the router for the interface, it generates [3]another address which combines its interface ID and global and subnet information advertised from the router. This is a routable global IP address.

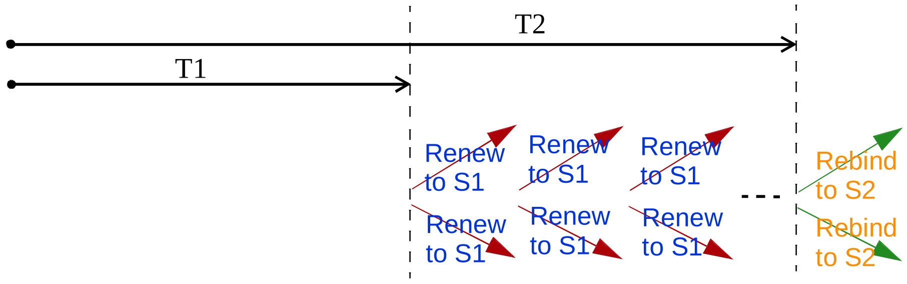
DHCPv6

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6, RFC 3315) is a server-client protocol that allows a DHCP server to assign and pass IPv6 network addresses, prefixes and other configuration information to DHCP clients. DHCPv6 servers and clients exchange DHCP messages using UDP.

Each DHCP client and server has a unique DHCP Unique IDentifier (DUID), which is used for identification when they are exchanging DHCPv6 messages. The DUID is generated from the MAC address, time, vendor assigned ID and/or the vendor's private enterprise number registered with the IANA. It should not change over time even after you reboot the device.

Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface. The DHCP client uses the IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information.
The IA type is the type of address in the IA. Each IA holds one type of address. IA_NA means an identity association for non-temporary addresses and IA_TA is an identity association for temporary addresses. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire. After T1, the client sends the server (**S1**) (from which the addresses in the IA_NA were obtained) a Renew message. If the time T2 is reached and the server does not respond, the client sends a Rebind message to any available server (**S2**). For an IA_TA, the client may send a Renew or Rebind message at the client's discretion.



DHCP Relay Agent

A DHCP relay agent is on the same network as the DHCP clients and helps forward messages between the DHCP server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCP server on its network, it then needs a DHCP relay agent to send a message to a DHCP server that is not attached to the same network.

The DHCP relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string,

[3] In IPv6, all network interfaces can be associated with several addresses.

such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCP server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

Prefix Delegation

Prefix delegation enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The Device uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by multicast, the Device passes the IPv6 prefix information to its LAN hosts. The hosts then can use the prefix to generate their IPv6 addresses.

ICMPv6

Internet Control Message Protocol for IPv6 (ICMPv6 or ICMP for IPv6) is defined in RFC 4443. ICMPv6 has a preceding Next Header value of 58, which is different from the value used to identify ICMP for IPv4. ICMPv6 is an integral part of IPv6. IPv6 nodes use ICMPv6 to report errors encountered in packet processing and perform other diagnostic functions, such as "ping".

Multicast Listener Discovery

The Multicast Listener Discovery (MLD) protocol (defined in RFC 2710) is derived from IPv4's Internet Group Management Protocol version 2 (IGMPv2). MLD uses ICMPv6 message types, rather than IGMP message types. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3.

MLD allows an IPv6 switch or router to discover the presence of MLD listeners who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.

MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.

MLD filtering controls which multicast groups a port can join.

MLD Messages

A multicast router or switch periodically sends general queries to MLD hosts to update the multicast forwarding table. When an MLD host wants to join a multicast group, it sends an MLD Report message for that address.

An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

Transition Techniques

IPv6 Over IPv4 Tunnelling

To route traffic between two IPv6 networks over an IPv4 network, an IPv6 over IPv4 tunnel has to be used.

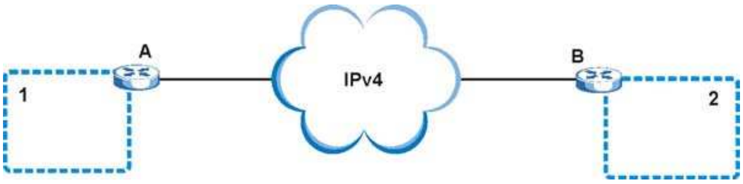
On the ZyXEL Device, you can either set up a configured tunnel or an automatic 6to4 tunnel. The following describes each method.

Configured Tunnel

A configured tunnel is a point-to-point tunnelling mechanism that encapsulates an IPv6 address with an IPv4 address. Routers (**A** and **B**) on both IPv6 networks (**1** and **2**) each must have an interface that connects to the IPv4 network (with an IPv4 address). This allows the router to send and receive IPv6 data over the IPv4 network.

In this case, you must specify **B**'s public IPv4 address on **A** (similarly, specify **A**'s public IPv4 address on **B**) in order for packets to arrive at the intended destination through the IPv4 network.

Figure 153 Configured Tunnel Example

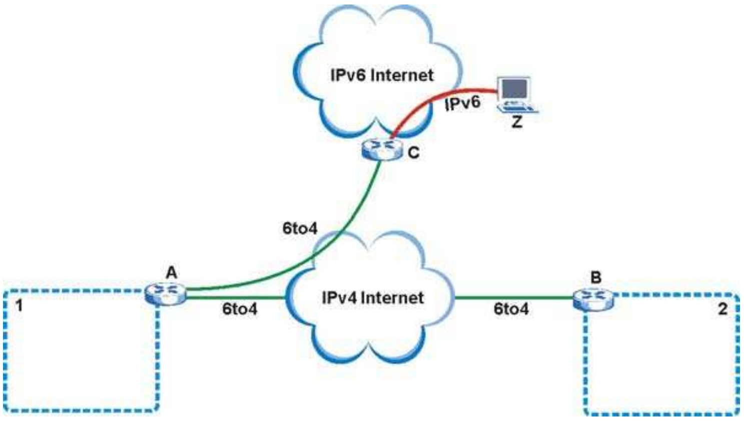


6to4 Tunnel

A 6to4 tunnel is an automatic tunnelling mechanism that provides connection between IPv6 networks across an IPv4 network. To transmit IPv6 packets over an IPv4 network, the IPv6 packets are encapsulated inside IPv4 packets.

The following figure shows a network example.

Figure 154 6to4 Relay Router Network Example



In a 6to4 tunnel, 6to4 routers (**A** and **B** in the example network) forward these packets between IPv6 networks (**1** and **2**) over the IPv4 Internet. A 6to4 relay router (**C**) connects to both an IPv6 and IPv4 network. A 6to4 relay router is used to forward packets between 6to4 routers in an IPv4 Internet and an IPv6 device (**Z**) on the IPv6 Internet.

To transmit packets, a 6to4 address is used with a special IPv6 prefix of `2002::` to encode a given IPv4 address. A 6to4 address has the following format:

2002:IPv4 address:subnet ID:host ID/64

For example, if you have an IPv4 address of 192.168.1.1 (first converted to binary notation and then to the colon hexadecimal representation of `c0a8:0101`), then the 6to4 addresses is `2002:c0a8:0101::1/64`.

Example - Enabling IPv6 on Windows XP/2003/Vista

By default, Windows XP and Windows 2003 support IPv6. This example shows you how to use the `ipv6 install` command on Windows XP/2003 to enable IPv6. This also displays how to use the `ipconfig` command to see auto-generated IP addresses.

```
C:\>ipv6 install
Installing...
Succeeded.

C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.1.1.46
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : fe80::2d0:59ff:feb8:103c%4
        Default Gateway . . . . . . . . . : 10.1.1.254
```

IPv6 is installed and enabled by default in Windows Vista. Use the `ipconfig` command to check your automatic configured IPv6 address as well. You should see at least one IPv6 address available for the interface on your computer.

Example - Enabling DHCPv6 on Windows XP

Windows XP does not support DHCPv6. If your network uses DHCPv6 for IP address assignment, you have to additionally install a DHCPv6 client software on your Windows XP. (Note: If you use static IP addresses or Router Advertisement for IPv6 address assignment in your network, ignore this section.)

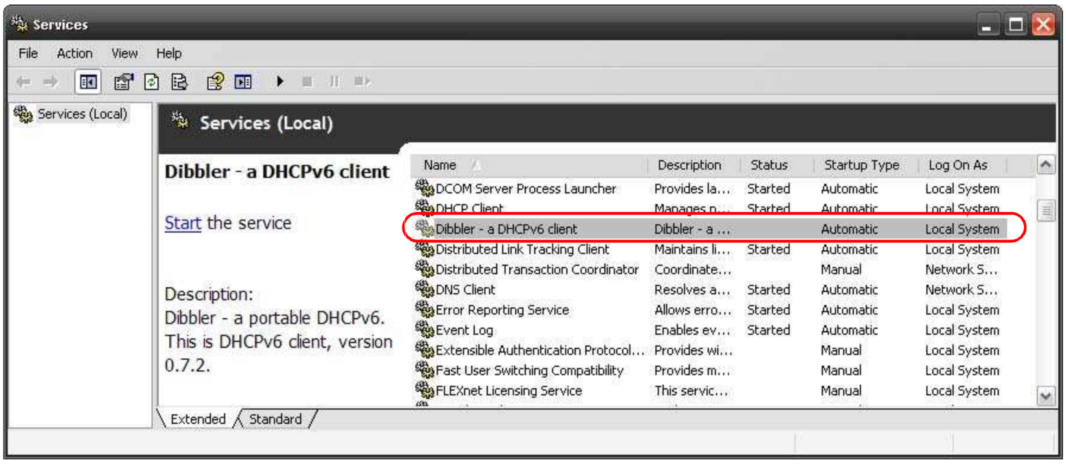
This example uses Dibbler as the DHCPv6 client. To enable DHCPv6 client on your computer:

1 Install Dibbler and select the DHCPv6 client option on your computer.

2 After the installation is complete, select **Start** > **All Programs** > **Dibbler-DHCPv6** > **Client Install as service**.

3 Select **Start** > **Control Panel** > **Administrative Tools** > **Services**.

4 Double click **Dibbler - a DHCPv6 client**.



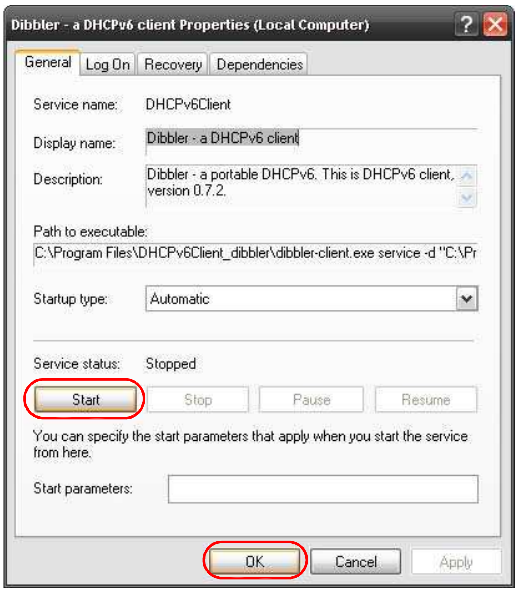
Dibbler - a DHCPv6 client

Start the service

Description:
Dibbler - a portable DHCPv6. This is DHCPv6 client, version 0.7.2.

Name	Description	Status	Startup Type	Log On As
DCOM Server Process Launcher	Provides la...	Started	Automatic	Local System
DHCP Client	Manages n...	Started	Automatic	Local System
Dibbler - a DHCPv6 client	Dibbler - a ...		Automatic	Local System
Distributed Link Tracking Client	Maintains li...	Started	Automatic	Local System
Distributed Transaction Coordinator	Coordinate...		Manual	Network S...
DNS Client	Resolves a...	Started	Automatic	Network S...
Error Reporting Service	Allows erro...	Started	Automatic	Local System
Event Log	Enables ev...	Started	Automatic	Local System
Extensible Authentication Protocol...	Provides wi...		Manual	Local System
Fast User Switching Compatibility	Provides m...		Manual	Local System
FLEXnet Licensing Service	This servic...		Manual	Local System

5 Click **Start** and then **OK**.



Service name: DHCPv6Client

Display name: Dibbler - a DHCPv6 client

Description: Dibbler - a portable DHCPv6. This is DHCPv6 client, version 0.7.2.

Path to executable:
C:\Program Files\DHCPv6Client_dibbler\dibbler-client.exe service -d "C:\Pr

Startup type: Automatic

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

6 Now your computer can obtain an IPv6 address from a DHCPv6 server.

Example - Enabling IPv6 on Windows 7

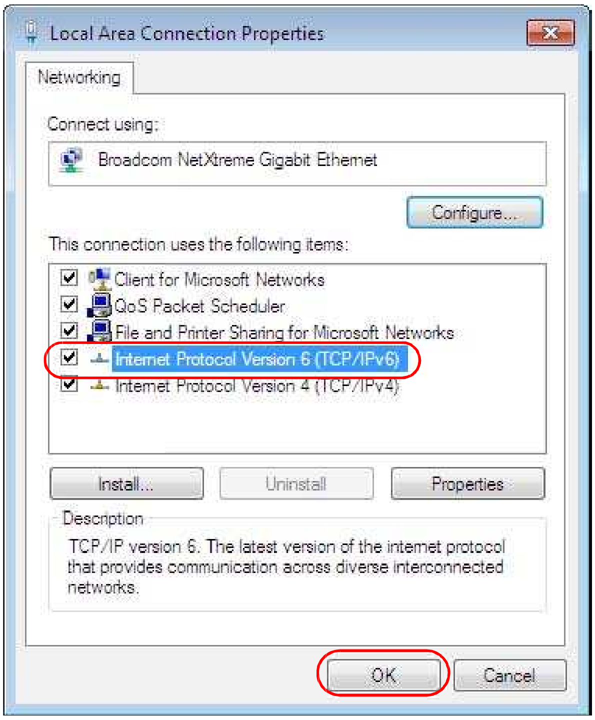
Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

To enable IPv6 in Windows 7:

1 Select **Control Panel** > **Network and Sharing Center** > **Local Area Connection**.

2 Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.

3 Click **OK** to save the change.



Connect using:

Broadcom NetXtreme Gigabit Ethernet

This connection uses the following items:

☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)

Description

TCP/IP version 6. The latest version of the internet protocol that provides communication across diverse interconnected networks.

4 Click **Close** to exit the **Local Area Connection Status** screen.

5 Select **Start** > **All Programs** > **Accessories** > **Command Prompt**.

6 Use the `ipconfig` command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:b021:2d::1000
   Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
   IPv4 Address. . . . . . . . . . . : 172.16.100.61
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::213:49ff:feaa:7125%11
                                       172.16.100.254
```

C

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s**) is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
    - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
    - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 90 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.

Table 90 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/ server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/ server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.

Table 90 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

D

Open Software Announcements

End-User License Agreement for “P-870HNU-51b”

WARNING: ZyXEL Communications Corp. IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED OR ZyXEL, AND YOUR MONEY WILL BE REFUNDED. HOWEVER, CERTAIN ZYXEL'S PRODUCTS MAY CONTAIN-IN PART-SOME THIRD PARTY'S FREE AND OPEN SOFTWARE PROGRAMS WHICH ALLOW YOU TO FREELY COPY, RUN, DISTRIBUTE, MODIFY AND IMPROVE THE SOFTWARE UNDER THE APPLICABLE TERMS OF SUCH THRID PARTY'S LICENSES ("OPEN-SOURCED COMPONENTS"). THE OPEN-SOURCED COMPONENTS ARE LISTED IN THE NOTICE OR APPENDIX BELOW. ZYXEL MAY HAVE DISTRIBUTED TO YOU HARDWARE AND/OR SOFTWARE, OR MADE AVAILABLE FOR ELECTRONIC DOWNLOADS THESE FREE SOFTWARE PROGRAMS OF THRID PARTIES AND YOU ARE LICENSED TO FREELY COPY, MODIFY AND REDISTIBUTE THAT SOFTWARE UNDER THE APPLICABLE LICENSE TERMS OF SUCH THIRD PARTY. NONE OF THE STATEMENTS OR DOCUMENTATION FROM ZYXEL INCLUDING ANY RESTRICTIONS OR CONDITIONS STATED IN THIS END USER LICENSE AGREEMENT SHALL RESTRICT ANY RIGHTS AND LICENSES YOU MAY HAVE WITH RESPECT TO THE OPEN-SOURCED COMPONENTS UNDER THE APPLICABLE LICENSE TERMS OF SUCH THIRD PARTY.

1.Grant of License for Personal Use

ZyXEL Communications Corp. ("ZyXEL") grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the Software ("Documentation"), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

2.Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

3.Copyright

The Software and Documentation contain material that is protected by international copyright law, trade secret law, international treaty provisions, and the applicable national laws of each respective country. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation.

4.Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. ZyXEL is not obligated to provide any maintenance, technical or other support for the resultant modified Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. Except as and only to the extent expressly permitted in this License, you may not market, co-brand, and private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing. Portions of the Software utilize or include third party software and other copyright material. Acknowledgements, licensing terms and disclaimers for such material are contained in the License Notice as below for the third party software, and your use of such material is exclusively governed by their respective terms. ZyXEL has provided, as part of the Software package, access to certain third party software as a convenience. To the extent that the Software contains third party software, ZyXEL has no express or implied obligation to provide any technical or other support for such software other than compliance with the applicable license terms of such third party, and makes no warranty (express, implied or statutory) whatsoever with respect thereto. Please contact the appropriate software vendor or manufacturer directly for technical support and customer service related to its software and products.

5.Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms and conditions of this License Agreement to those persons employed by you who come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

6.No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF

THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

7.Limitation of Liability

IN NO EVENT WILL ZyXEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE OR PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyXEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyXEL's TOTAL AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED THE PRODUCT'S PRICE. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

8.Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyXEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

9.Audit Rights

ZyXEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

10.Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyXEL all copies of the Software and Documentation in your possession or under your control. ZyXEL may terminate this License Agreement for any reason, including, but not limited to, if ZyXEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyXEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

11.General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in ROC, Taiwan if the parties agree to a binding arbitration. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyXEL. Any waiver or modification of this License

Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.

NOTE: Some components of this product incorporate free software programs covered under the open source code licenses which allows you to freely copy, modify and redistribute the software. For at least three (3) years from the date of distribution of the applicable product or software, we will give to anyone who contacts us at the ZyXEL Technical Support (support@zyxel.com.tw), for a charge of no more than our cost of physically performing source code distribution, a complete machine-readable copy of the complete corresponding source code for the version of the Programs that we distributed to you if we are in possession of such.

Notice

Information herein is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, except the express written permission of ZyXEL Communications Corporation.

This Product includes MIPS Linux kernel , Bridge-Utils, BusyBox, ebtables, bftpd, iproute2, iptables, udhcp, wput, Dnsmasq and zebra software under GPL 2.0 license.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the

scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

This Product includes ppp software under below license

This directory contains source code and precompiled binaries for ppp-2.4, a package which implements the Point-to-Point Protocol (PPP) to provide Internet connections over serial lines. ppp-2.4 currently supports Linux and Solaris.

All of the code here can be freely used and redistributed. Theindividual source files each have their own copyright and permission

notice; some have a BSD-style notice and some are under the GPL.

This Product includes Ssh server: dropbear software under MIT-style license

The MIT License

Copyright (c) <year> <copyright holders>

Permission is hereby granted, free of charge, to any person obtaining a copy

This Product includes openssl: openSSL library software under openSSL license

This is a copy of the current LICENSE file inside the CVS repository.

LICENSE ISSUES

==============

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of
the OpenSSL License and the original SSLeay license apply to the toolkit.
See below for the actual license texts. Actually both licenses are BSD-style
Open Source licenses. In case of any license issues related to OpenSSL
please contact openssl-core@openssl.org.

OpenSSL License

```
  ---------------

/*
=============================================================
=======
 * Copyright (c) 1998-2008 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
```

```
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
*
=============================================================
=======
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
```

```
*/

Original SSLeay License
-----------------------
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
```

* 1. Redistributions of source code must retain the copyright
*   notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*   notice, this list of conditions and the following disclaimer in the
*   documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*   must display the following acknowledgement:
*   "This product includes cryptographic software written by
*   Eric Young (eay@cryptsoft.com)"
*   The word 'cryptographic' can be left out if the rouines from the library
*   being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
*   the apps directory (application code) you must include an acknowledgement:
*   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or

This Product includes Dhcpv6 software under BSD license

BSD

This Product includes radvd software under following license

binary forms, with or without modification, of the software and documentation
provided that the following conditions are met:

0. If you receive a version of the software that is specifically labelled
   as not being for redistribution (check the version message and/or README),
   you are not permitted to redistribute that version of the software in any
   way or form.
1. All terms of all other applicable copyrights and licenses must be
   followed.
2. Redistributions of source code must retain the authors' copyright
   notice(s), this list of conditions, and the following disclaimer.
3. Redistributions in binary form must reproduce the authors' copyright
   notice(s), this list of conditions, and the following disclaimer in the
   documentation and/or other materials provided with the distribution.
4. All advertising materials mentioning features or use of this software
   must display the following acknowledgement with the name(s) of the
   authors as specified in the copyright notice(s) substituted where
   indicated:

This product includes software developed by the authors which are mentioned at the start of the source files and other contributors.

5. Neither the name(s) of the author(s) nor the names of its contributors
   may be used to endorse or promote products derived from this software
   without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY ITS AUTHORS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED

WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Legal Information

Copyright

Disclaimer

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

Trademarks

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

Certifications

Federal Communications Commission (FCC) Interference Statement

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

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

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

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

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

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- For operation within 5.15 ~ 5.25GHz frequency range, it is restricted to indoor environment.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

注意 ！

依據　低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用
者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現
有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍
受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。
減少電磁波影響，請妥適使用。

Notices

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

This device has been designed for the WLAN 2.4 GHz and 5 GHz networks throughout the EC region and Switzerland, with restrictions in France.

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

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

Viewing Certifications

1 Go to http://www.zyxel.com.

2 Select your product on the ZyXEL home page to go to that product's page.

3 Select the certification you wish to view from this page.

ZyXEL Limited Warranty

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

Note

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

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

Index