AR-7288WnA / AR-7288WnB

Manual

09-2014 / v1.1

Edimax Technology Co., Ltd.
No.3, Wu-Chuan 3rd Road, Wu-Gu, New Taipei City 24891, Taiwan
Email: support@edimax.com.tw

Edimax Technology Europe B.V.
Fijenhof 2, 5652 AE Eindhoven, The Netherlands
Email: support@edimax.nl

Edimax Computer Company
3350 Scott Blvd., Bldg.15 Santa Clara, CA 95054, USA
Live Tech Support: 1(800) 652-6776
Email: support@edimax.com

COPYRIGHT

Edimax Technology Co., Ltd.
Add: No. 3, Wu-Chuan 3rd Rd., Wu-Ku Industrial Park, New Taipei City, Taiwan
Tel: +886-2-77396888
Email: sales@edimax.com.tw

Contents

Note: The images/screenshots used in this manual are for reference only – actual screens may vary according to firmware version. The contents of this manual are based on the most recent firmware version at the time of writing.

1. Product Introduction

1.1. Package Contents

Before you start using this product, please check if there is anything missing in the package and contact your dealer to claim the missing item(s):

- ADSL2+ router
- 12V power adapter
- RJ-45 Ethernet cable
- RJ-11 telephone line x 2
- Quick installation guide
- CD containing setup wizard, user manual
- ADSL Splitter
- 5dBi antenna

1.2. System Requirements

Recommended system requirements are as follows.

- A 10/100 base-T Ethernet card installed in your PC.
- A hub or Switch (connected to several PCs through one of the Ethernet interfaces on the device).
- Operating system: Windows 98 SE, Windows 2000, Windows ME, Windows XP, Windows 7, Windows 8/8.1.
- Internet Explorer V5.0 or higher, Netscape V4.0 or higher or Firefox 1.5 or higher.

1.3. Safety Precautions

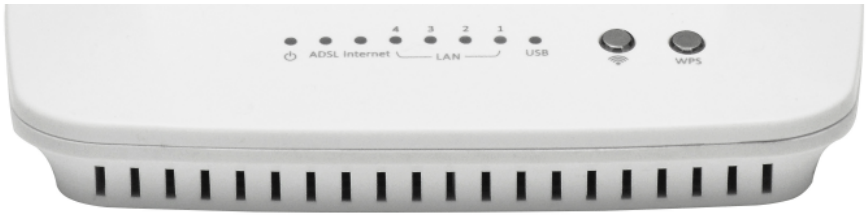
Follow the following instructions to prevent the device from risks and damage caused by fire or electric power:

- Use volume labels to mark the type of power.
- Use the power adapter included within the package contents.
- Pay attention to the power load of the outlet or prolonged lines. An overburdened power outlet or damaged lines and plugs may cause an electric shock or fire. Check the power cords regularly. If you find any damage, replace it at once.
- Proper space left for heat dissipation is necessary to avoid damage caused by overheating to the device. The long and thin holes on the device are designed for heat dissipation to ensure that the device works normally. Do not cover these heat dissipation holes.
- Do not put this device close to heat sources or high temperatures. Keep the device out of direct sunshine.

- Do not put this device close to a place where it is damp or wet. Do not spill any fluid on this device.
- Do not connect this device to any PCs or electronic products, other than those which you are instructed or recommended to do so in the product's documentation, by our customer engineers or by your broadband provider – connecting to incorrect devices may cause a fire risk.
- Place this device on a stable surface.

1.4. LED Status & Button Definitions

Front Panel



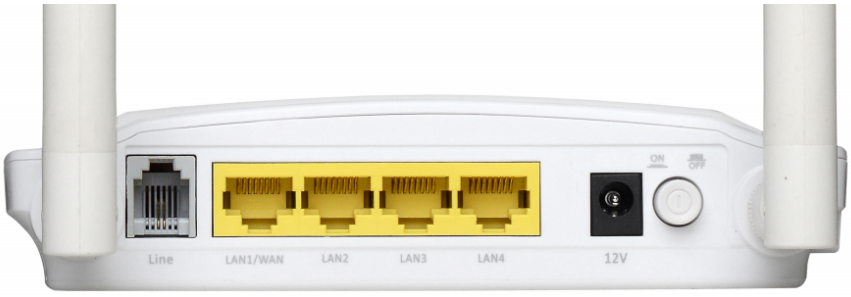
LED	Color	Status	Description
Power ⏻	**Green**	**On**	ADSL2+ router is on.
		Off	ADSL2+ router Is off.
	Red	**On**	ADSL broadband initial self-test failed or upgrading firmware.
ADSL	**Green**	**On**	ADSL line is synchronized and ready to use.
		Slow Flashing	ADSL synchronization failed (please refer to *Note i.* below)
		Quick Flashing	ADSL negotiation is in progress.
Internet	**Green**	**On**	Internet connected in router mode
		Flashing	Internet activity (transferring/receiving data) in router mode.
		Off	Device in bridged mode.
	Red	**On**	Internet not connected in router mode (Please refer to *Note ii.* below).
LAN1–4	**Green**	**On**	LAN port connected.
		Flashing	LAN activity (transferring/receiving data).
		Off	LAN port not connected.

WLAN	**Green**	**On**	Successful WLAN connection.
		Flashing	WLAN activity (transferring/receiving data).
		Off	WLAN connection failed.
WPS	**Green**	**Off**	WPS is disabled.
		Flashing	WPS is enabled and waiting for client to negotiate.

Note i. If the ADSL LED is off, please check your Internet connection. Refer to A. Hardware Installation for more information about how to connect the router correctly. If all connections are correct, please contact your ISP to check if there is a problem with your Internet service.

ii. If the Internet LED is red, please check your ADSL LED first. If the ADSL LED is off, refer to Note 1. If the green ADSL LED is ON, please check your Internet configuration. You may need to check with your ISP that your Internet is configured correctly.

Rear Panel



Item	Description
Power On/Off Button	Switches the router on or off.
Power	Power port for included 12V power adapter.
Wireless On/Off Button	Switch the wireless signal on or off.

Item	Description
WPS Button	Activate WPS (Wi-Fi Protected Setup)
LAN 1–4	RJ-45 Ethernet ports 1–4.
Reset Button	Hold for less than 5 seconds to restart the device, and hold for more than 10 seconds to reset the device to factory default settings.
Line	RJ-11 port for standard telephone line.

USB interface is used to connect a USB device, such as a USB flash disk or printer. Users can access and share the USB storage disk or use the printer device connecting to the router.

1.5. Features

The device supports the following features:

- Various line modes
- External PPPoE dial-up access
- Internal PPPoE/PPPoA dial-up access
- 1483Bridged/1483Routed with dynamic ip or static ip
- Multiple PVCs (8 PVCs supported)
- DHCP server/relay
- Static route
- Network Address Translation(NAT)
- DMZ
- Virtual Server
- Universal plug and play (UPnP)
- Dynamic Domain Name Server(DDNS)
- One-level password and username
- Network Time Protocol(NTP)
- Firmware upgrading through Web, TFTP, or FTP
- Resetting to factory defaults through Reset button or Web
- Diagnostic test
- Web interface
- Telnet CLI
- IP/MAC/URL Filter
- Application layer service
- QOS
- Port binding

2. Hardware Installation

1. Connect the ADSL line.

Connect the line port of the router of the device to the modem interface of a splitter using a telephone cable. Connect a telephone to the Phone interface of the splitter using a telephone cable. Connect the Line interface of the splitter to your existing, incoming line.

The splitter has three interfaces:

- Line: Connect to a wall phone jack (RJ-11 jack).
- Modem: Connect to the ADSL jack of the device.
- Phone: Connect to a telephone set.

2. Connect the router to your LAN network.

Connect the LAN interface of the router to your PC, hub or switch using an Ethernet cable.

3. Connect the power adapter to the router.

Plug one end of the power adapter into a wall outlet and connect the other end to the 12V interface of the device.

The following diagrams show how to correctly connect the router, PC, splitter and the telephone sets under two different configurations:

Configuration 1

0 shows the correct connection of the router, PC, splitter and the telephone sets, with no telephone set placed before the filter.

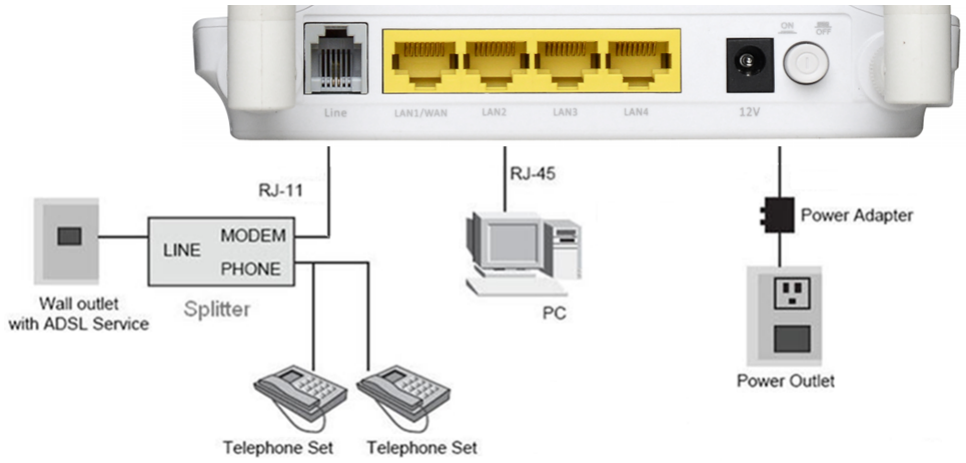


Figure 1 –Connection diagram
(Without connecting telephone sets before the filter)

Configuration 2

0 shows the correct connection when a telephone set is installed before the filter.

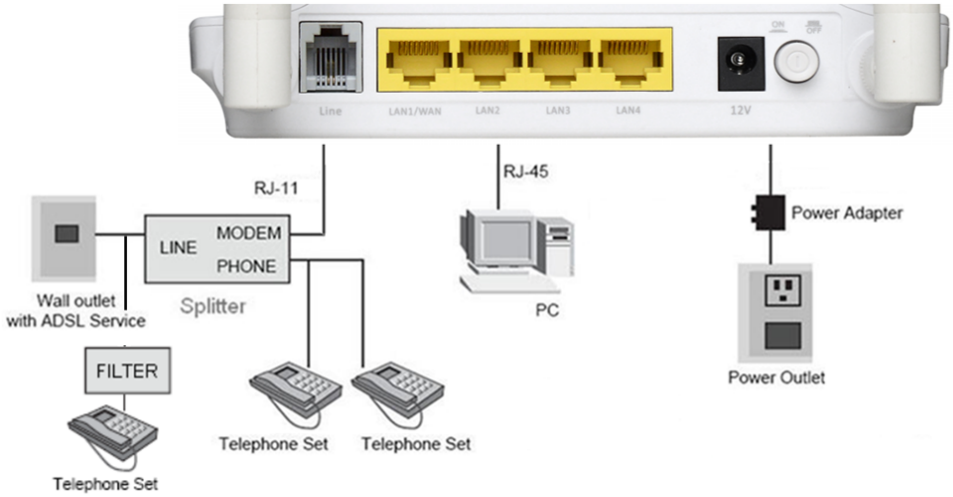


Figure 2 - Connection diagram
(Connecting a telephone set before the filter)

Note:
When **Configuration 2** is used, the filter must be installed close to the telephone cable. Do not use the splitter to replace the filter.

Installing a telephone directly before the splitter may lead to failure of connection between the device and the central office, or failure of Internet access, or slow connection speed. If you really need to add a telephone set before the splitter, you must add a micro filter before a telephone set. Do not connect several telephones before the splitter or connect several telephones with the micro filter.

4. Check the ADSL LED status.

Please check the ADSL LED on the front panel. This light indicates the status of your ADSL broadband through your telephone line. If the light is on, you can continue setup. However if the light is flashing, there is no broadband line detected. Please call your Internet Service Provider (ISP) and inform them about the flashing ADSL light to resolve the issue.

5. Firewall settings.

Please turn off all personal firewalls before you continue the setup – firewalls can block communication between your PC and router.

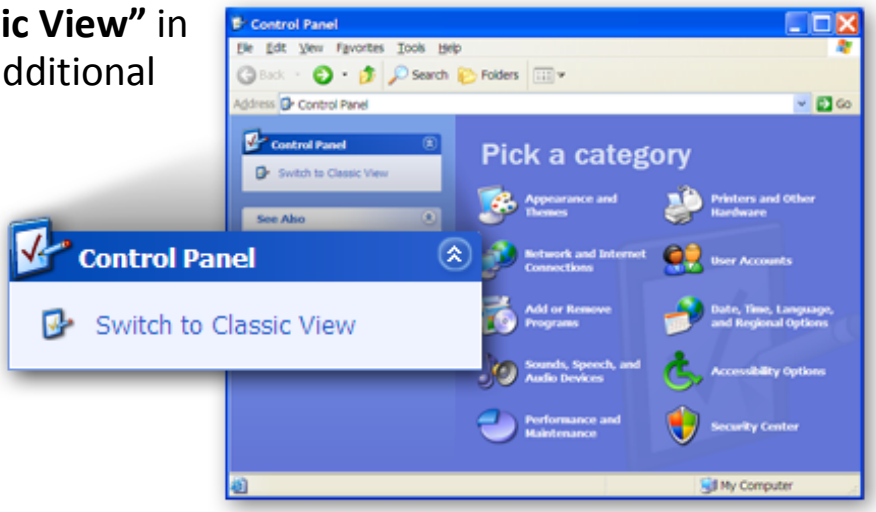
Note: You must use the power adapter included in the package with the router, do NOT attempt to use a third-party power adapter.

6. PC LAN IP configuration.

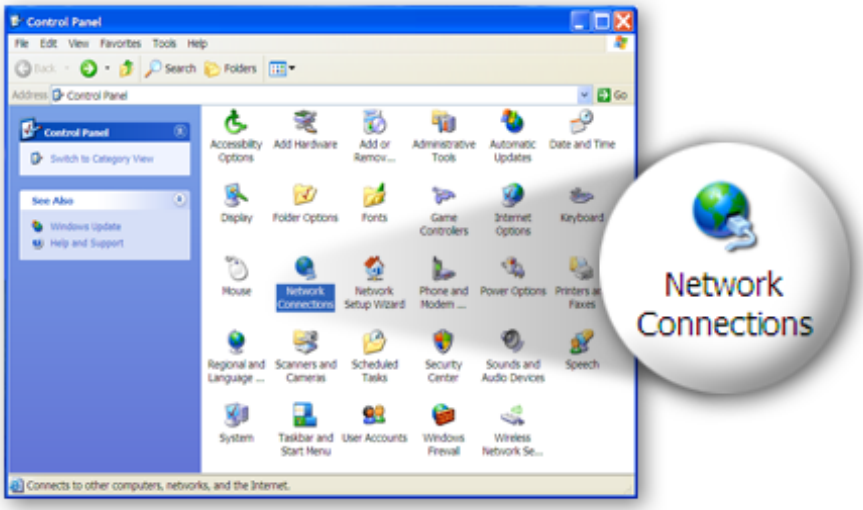
Configure your PC's LAN settings to automatically obtain an IP address from the router by following the steps below:

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

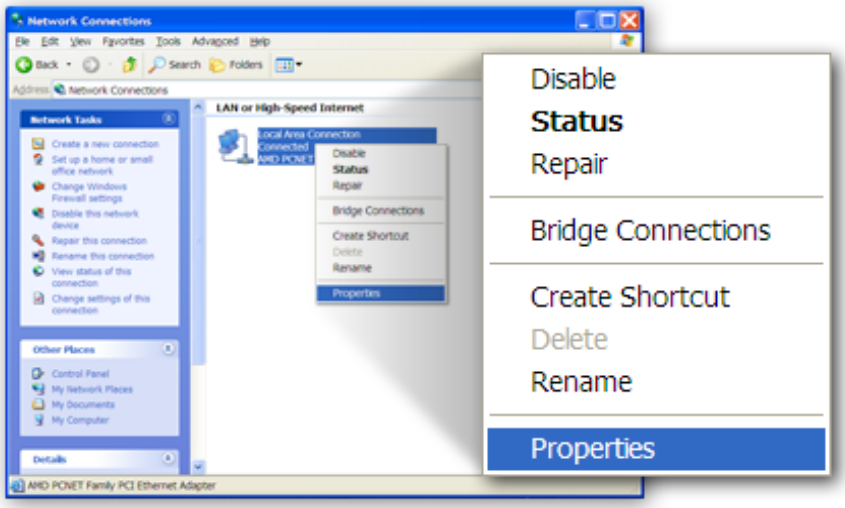
2. Click **"Switch to Classic View"** in the top left to show additional setting icons.



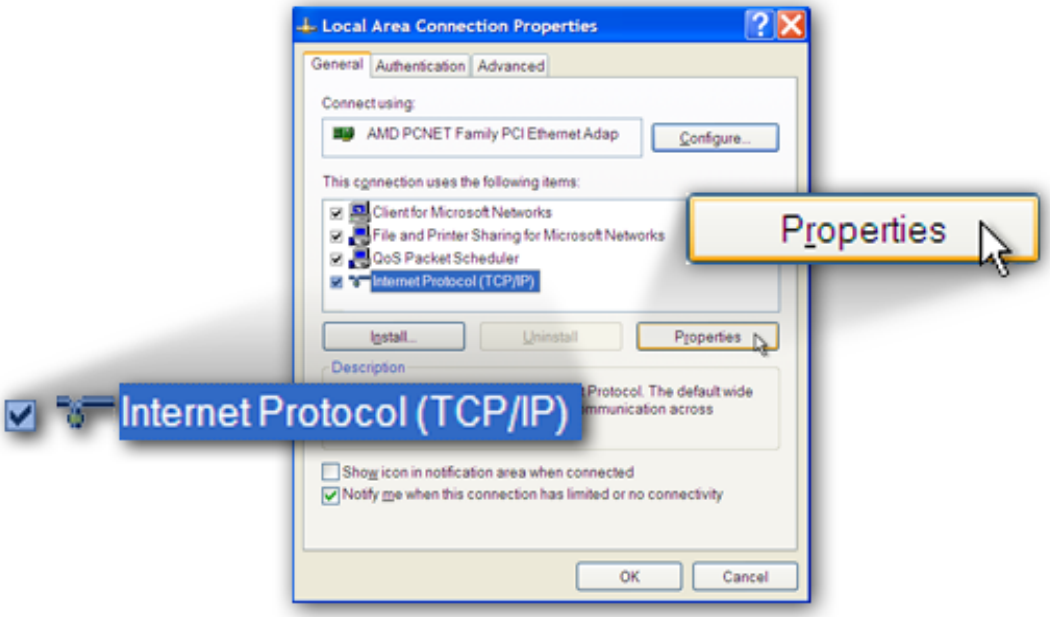
3. Locate the **"Network Connections"** icon and double-click to open network connection settings.



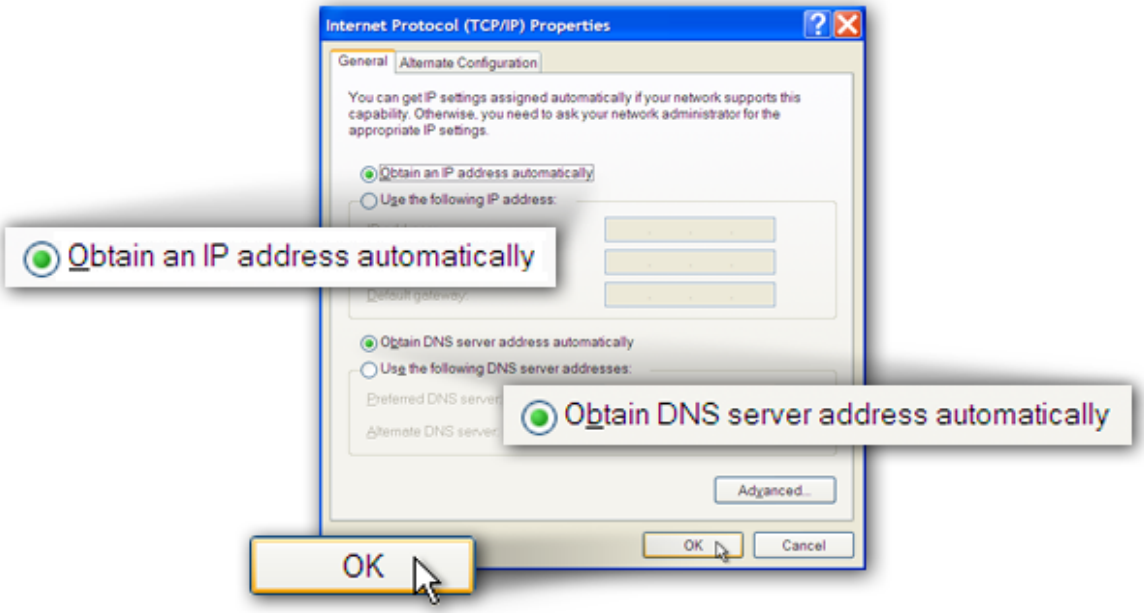
4. Select the **“Local Area Connection”** icon and right-click it to open the sub-menu, then select **“Properties”**.



5. Select **“Internet Protocol (TCP/IP)”** and then click **“Properties”**



6. Ensure that **“Obtain an IP address automatically”** and **“Obtain DNS server address automatically”** are selected and then press **“OK”**.



3. IP Address Setting

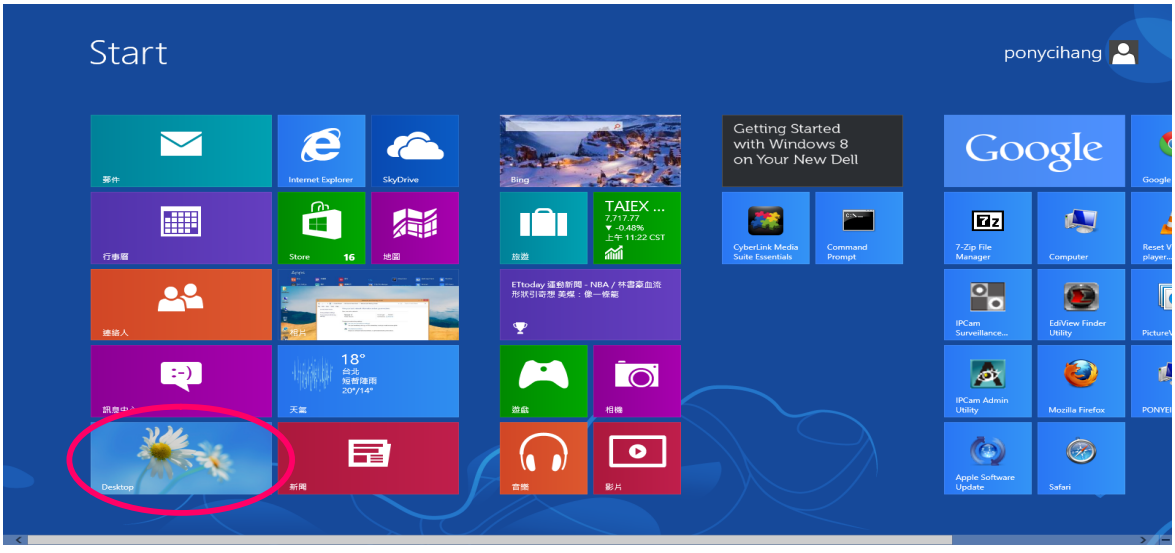
To use the router to access the Internet, the PCs in the network must have an Ethernet adapter installed and be connected to the router either directly or through a hub or switch. The TCP/IP protocol of each PC must be installed and the IP Address of each PC has to be set in the same subnet as the router.

The router's default IP Address is **192.168.2.1** and the subnet mask is **255.255.255.0**. PCs can be configured to obtain IP Address automatically through the DHCP Server of the router or a fixed IP Address in order to be in the same subnet as the router. By default, the DHCP Server of the router is enabled and will dispatch IP Address to PC from **192.168.2.100** to **192.168.2.199**. It is strongly recommended to set obtaining IP address automatically.

This section shows you how to configure your PC so that it can obtain an IP address automatically for either Windows 95/98/Me, 2000 or NT operating systems. For other operating systems (Macintosh, Sun, etc.), please follow the manual of the operating system. The following is a step-by-step illustration of how to configure your PC to obtain an IP address automatically for **Windows 8, Windows 7, Windows Vista and Windows XP.**

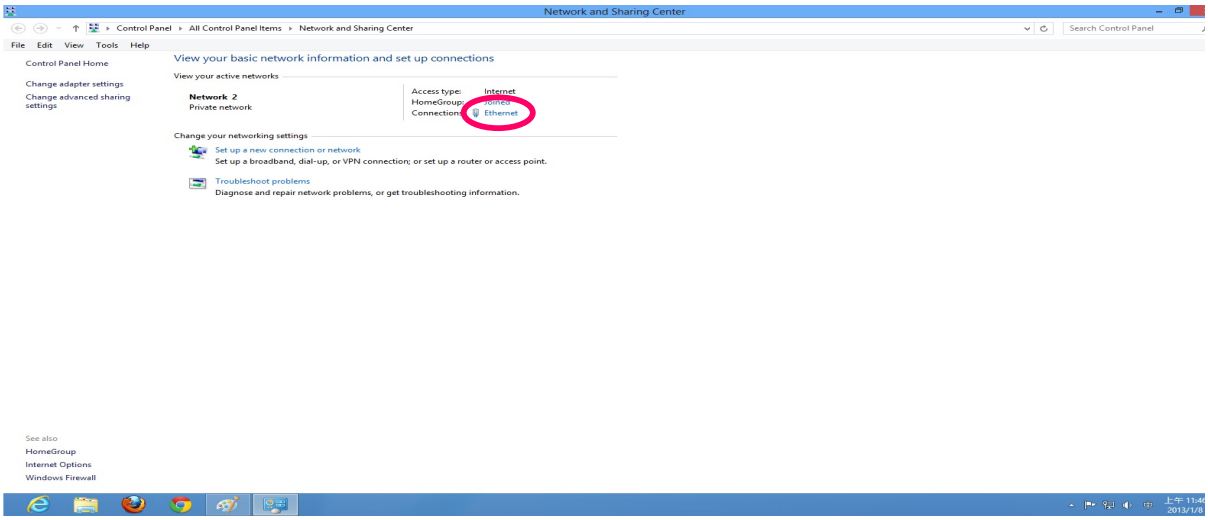
3.1. Windows 8

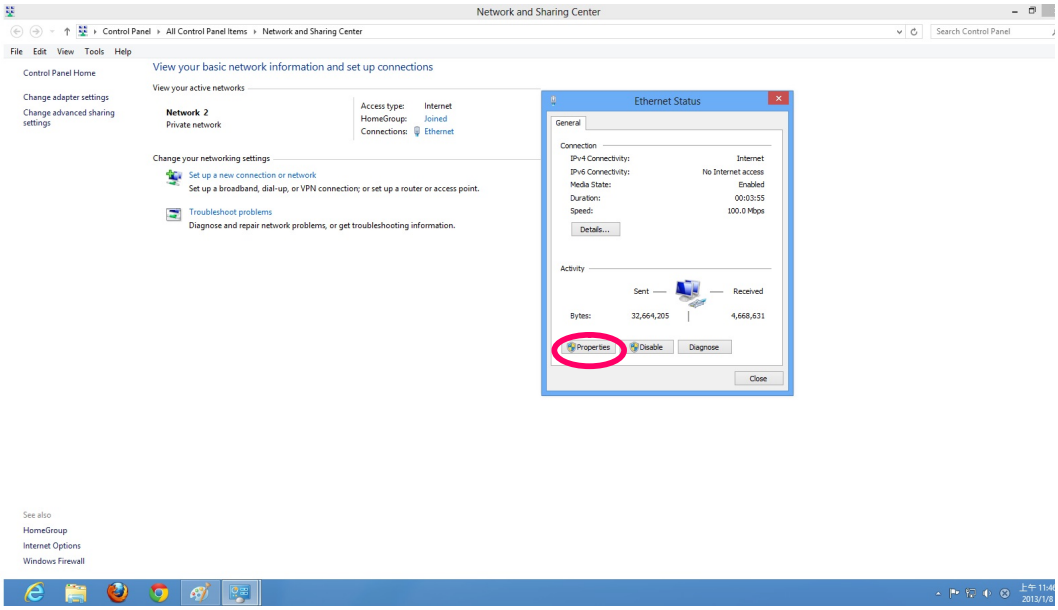
1. From the Windows 8 Start screen, you need to switch to desktop mode. Click the Desktop icon in the bottom left of the screen.



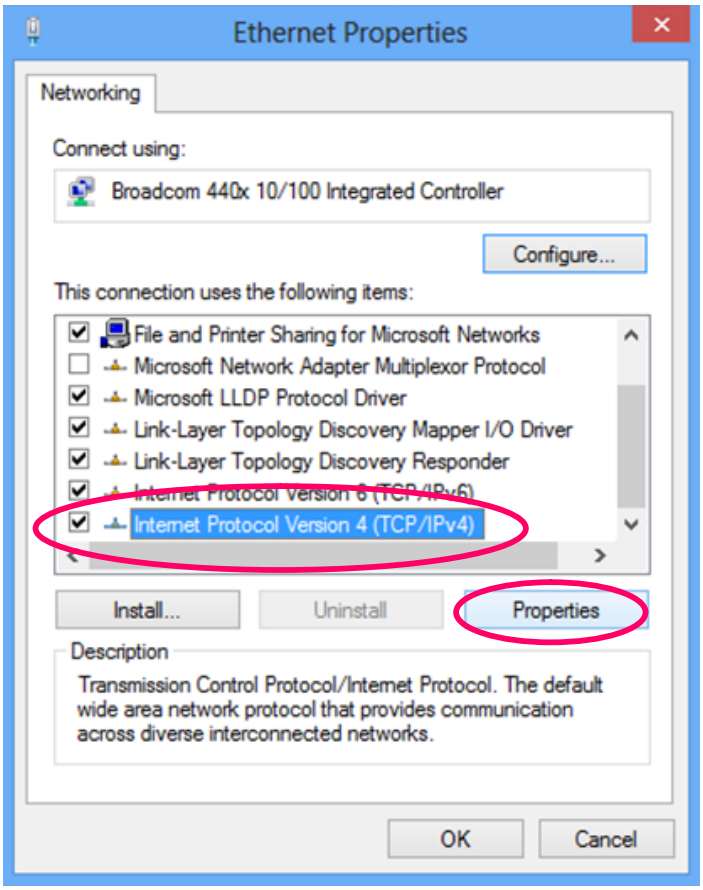
2. Click the Network icon and then select Open Network and Sharing Center to open the Network and Sharing Center window.

3. Click Ethernet to open the Ethernet Status window, and then select Properties. The Local Area Connection window will appear.

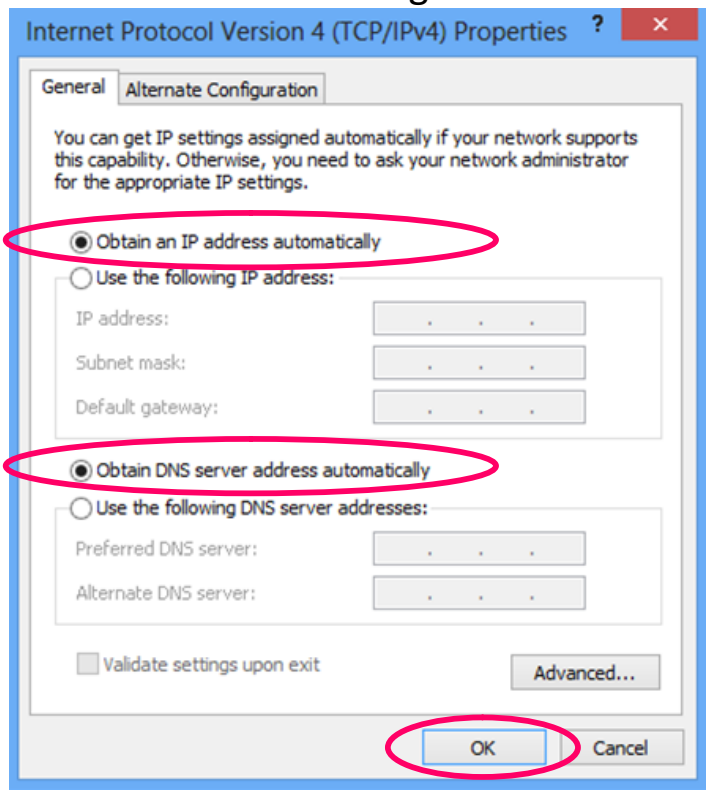




4. Check your list of Network Components. Select Internet Protocol Version 4 (TCP/IPv4) and click the Properties button.



5. In the Internet Protocol Version 4 (TCP/IPv4) Properties window, select Obtain an IP address automatically and Obtain DNS server address automatically as shown on the following screen.



6. Click OK (shown above) to confirm the setting. Your PC will now obtain an IP address automatically from your router's DHCP server.

Note: Please make sure that the router's DHCP server is the only DHCP server available on your LAN.

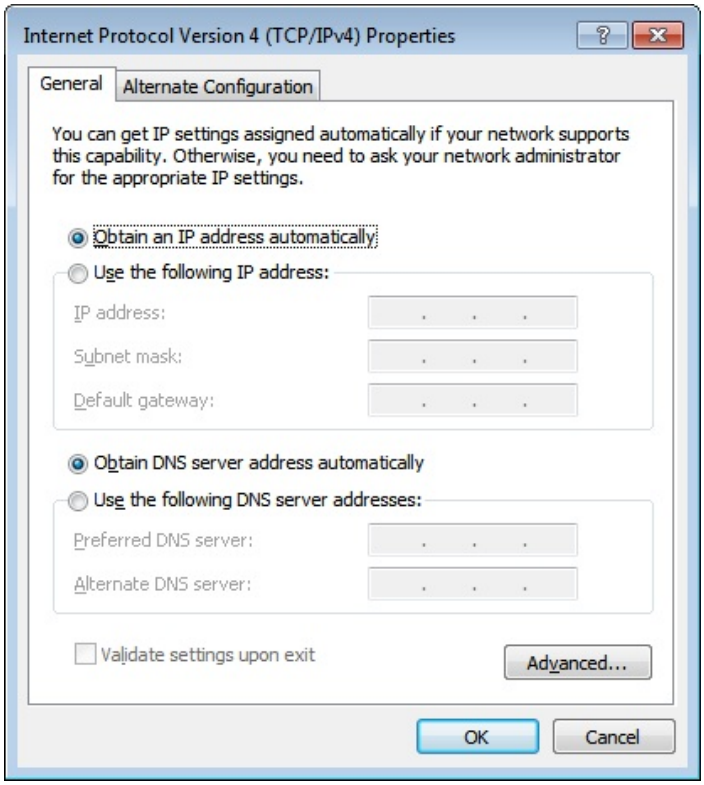
3.2. Windows 7

1. Click the Start button and select Control Panel. Double click Network and Internet and click Network and Sharing Center, the Network and Sharing Center window will appear.

2. Click Change adapter settings and right click on the Local Area Connection icon and select Properties. The Local Area Connection window will appear.

3. Check your list of Network Components. You should see Internet Protocol Version 4 (TCP/IPv4) on your list. Select it and click the Properties button.

4. In the Internet Protocol Version 4 (TCP/IPv4) Properties window, select Obtain an IP address automatically and Obtain DNS server address automatically as shown on the following screen.



5. Click OK to confirm the setting. Your PC will now obtain an IP address automatically from your router's DHCP server.

Note: Please make sure that the router's DHCP server is the only DHCP server available on your LAN.

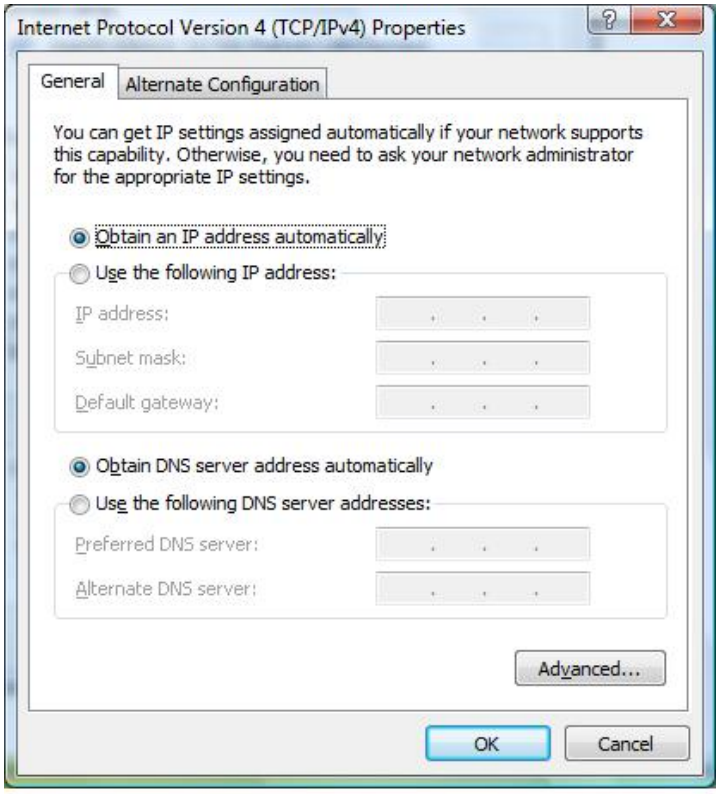
3.3. Windows Vista

1. Click the Start button and select Settings and then select Control Panel. Double click Network and Sharing Center, the Network and Sharing Center window will appear.

2. Click Manage network connections and right click on the Local Area Connection icon and select Properties. The Local Area Connection window will appear.

3. Check your list of Network Components. You should see Internet Protocol Version 4 (TCP/IPv4) on your list. Select it and click the Properties button.

4. In the Internet Protocol Version 4 (TCP/IPv4) Properties window, select Obtain an IP address automatically and Obtain DNS server address automatically as shown on the following screen.



5. Click OK to confirm the setting. Your PC will now obtain an IP address automatically from your router's DHCP server.

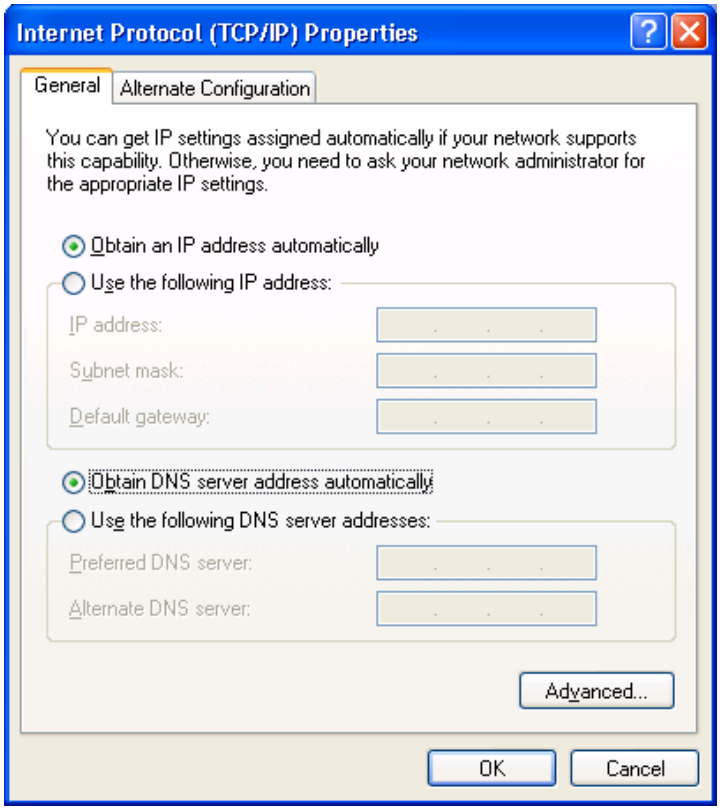
Note: Please make sure that the router's DHCP server is the only DHCP server available on your LAN.

3.4. Windows XP

1. Click the Start button and select Control Panel and then double click Network Connections. The Network Connections window will appear.

2. Right click on the Local Area Connection icon and select Properties. The Local Area Connection window will appear.
3. Check your list of Network Components. You should see Internet Protocol [TCP/IP] on your list. Select it and click the Properties button.

4. In the Internet Protocol (TCP/IP) Properties window, select Obtain an IP address automatically and Obtain DNS server address automatically as shown on the following screen.



5. Click OK to confirm the setting. Your PC will now obtain an IP address automatically from your router's DHCP server.

Note: Please make sure that the router's DHCP server is the only DHCP server available on your LAN.

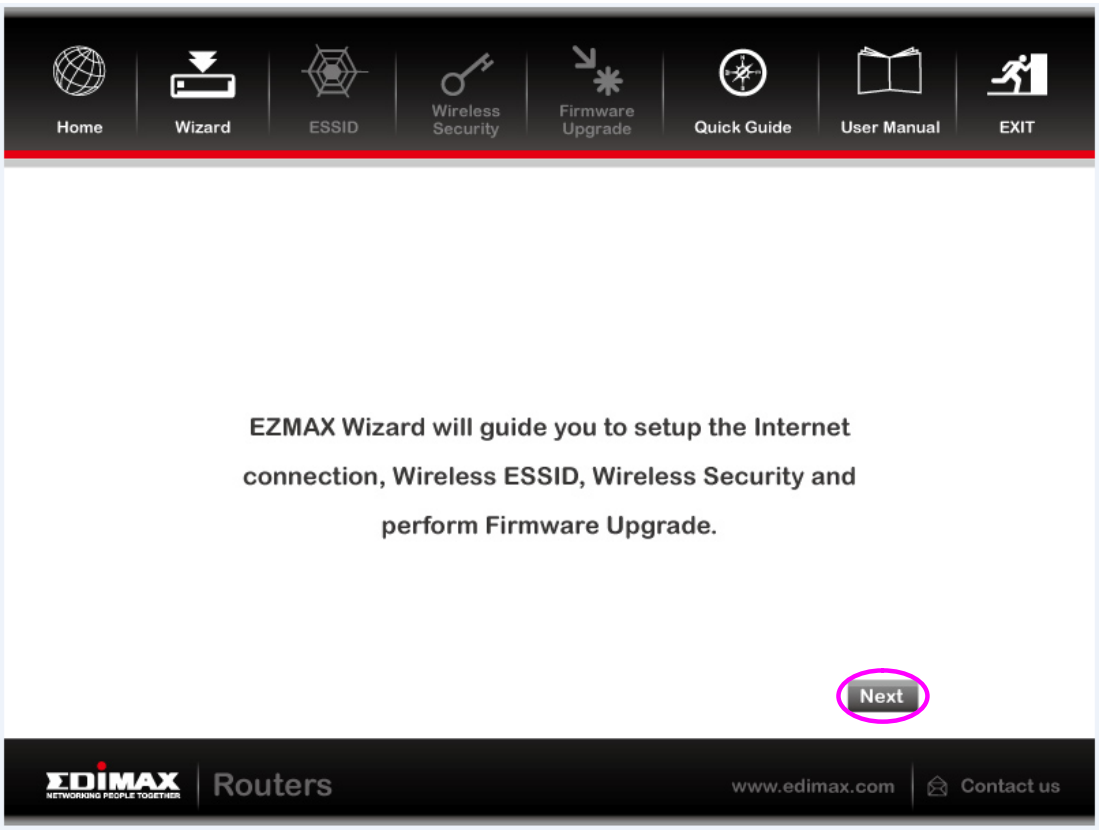
4. EZmax Setup Wizard

You can configure the router by running the setup wizard on the CD-ROM included in the package contents. The wizard enables you to configure your Internet connection, upgrade the firmware and change the router's password. Please follow the instructions below.

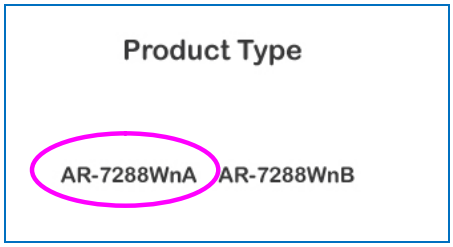
Alternatively, if you lose the CD-ROM or prefer a web based setup, you can login to the ADSL router using Internet Explorer, and configure the router from there using the web-based interface. Instructions for how to do so can be found in **5. Web Configuration.**

4.1. Setup Wizard

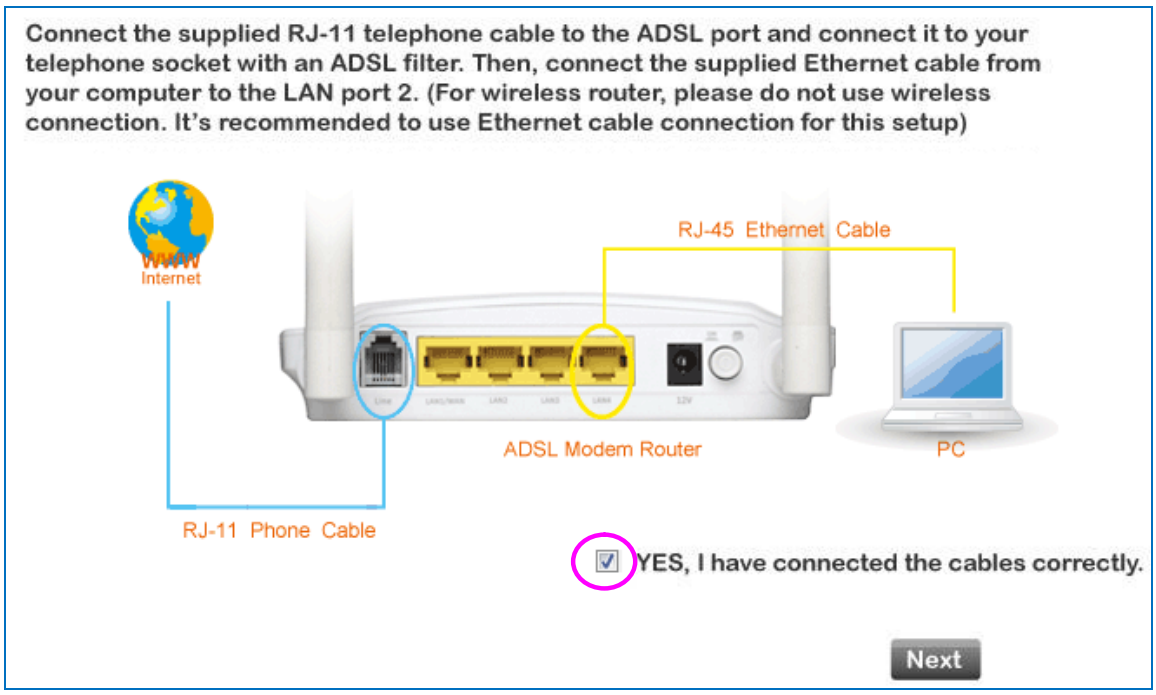
1. When you start the setup wizard, you will see the following screen. Please follow the on screen instructions.



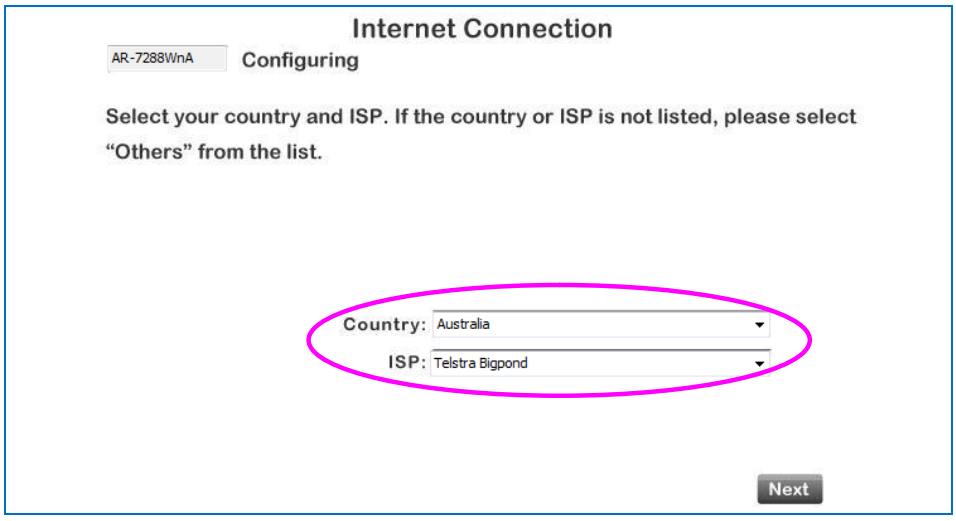
2. Please select your product.



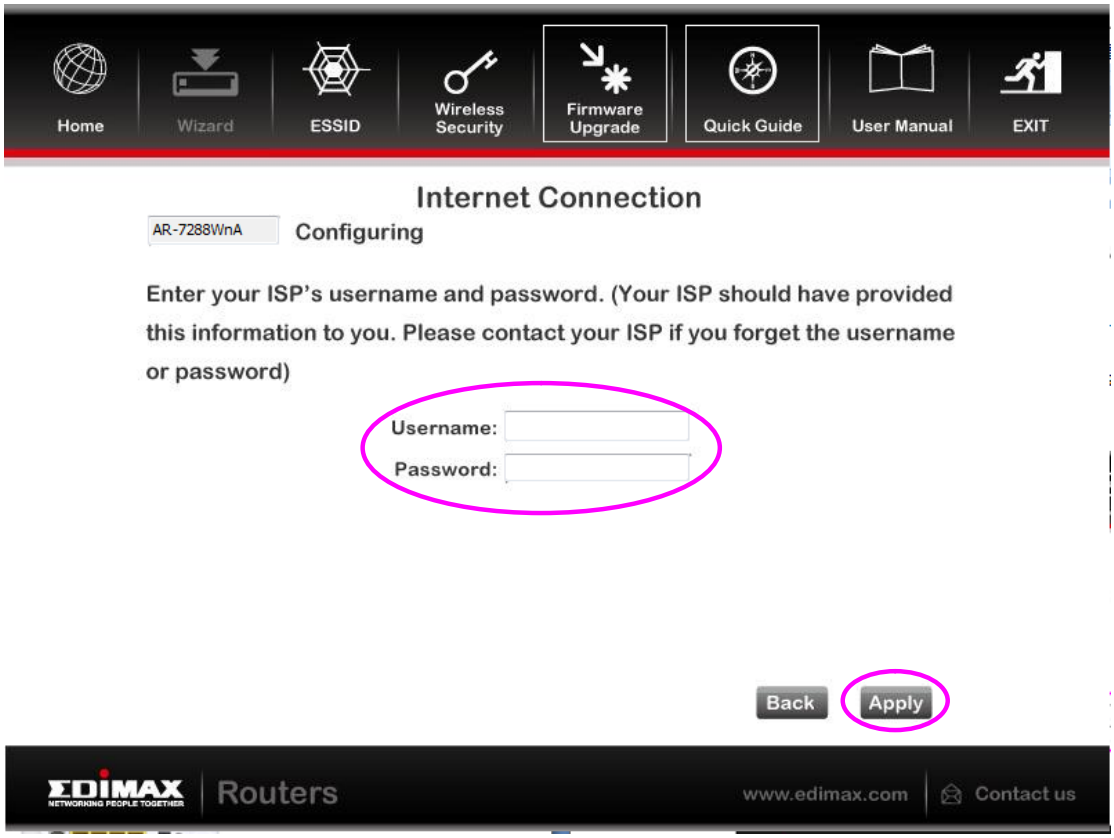
3. Please ensure all hardware is correctly installed. Check the box and click “Next”.

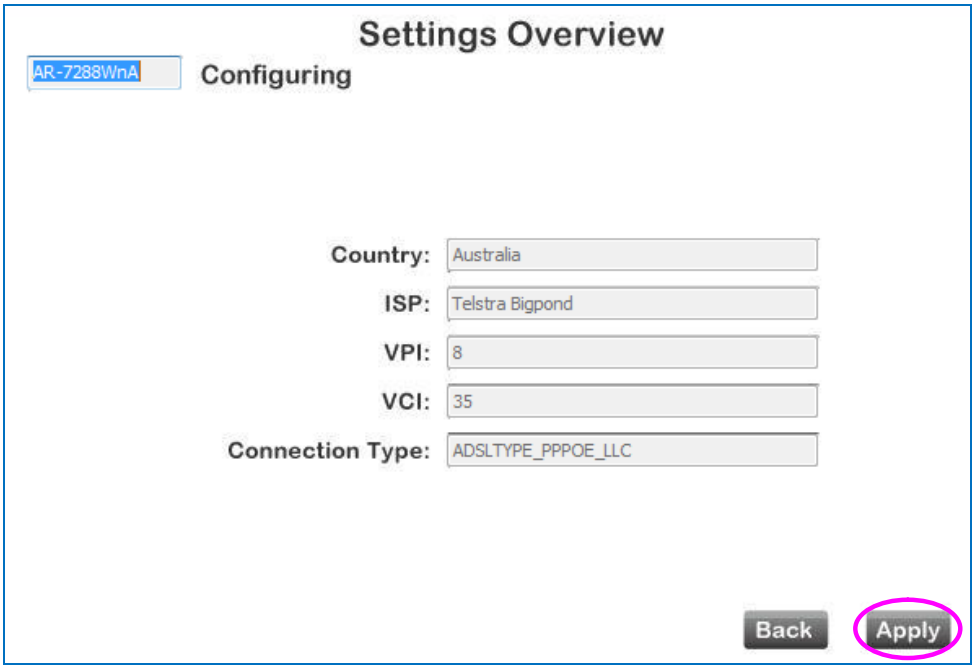


4. Select your country and ISP. If your ISP is not listed, select “Other” from the list and refer to **4.2. Internet Connection Type.**

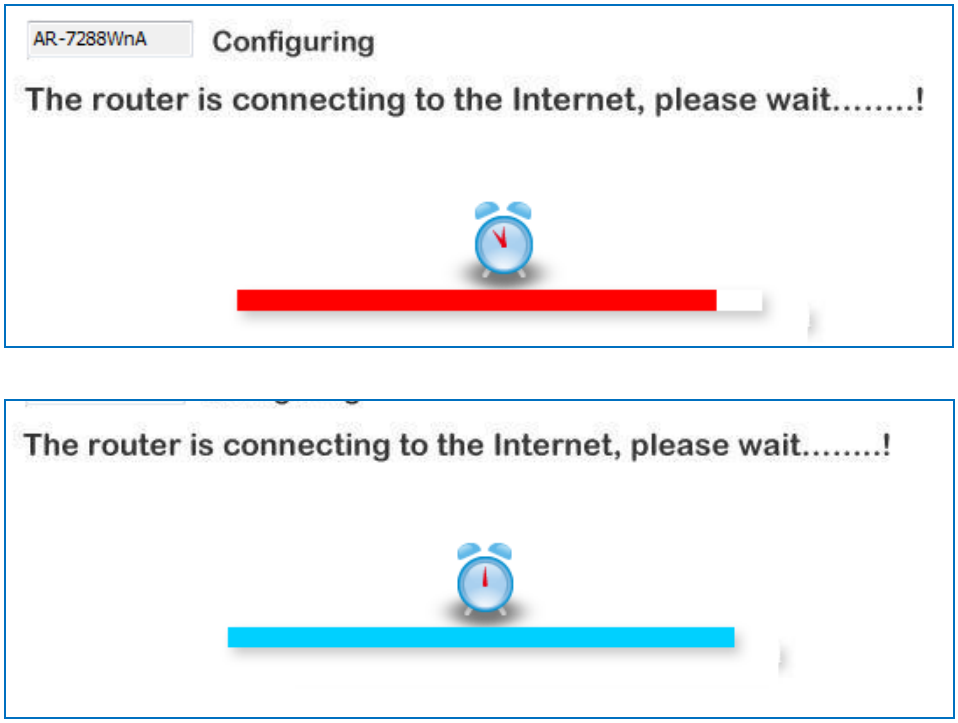


5. Enter your ISP's username and password and click "Apply". On the next screen, click "Apply" again.



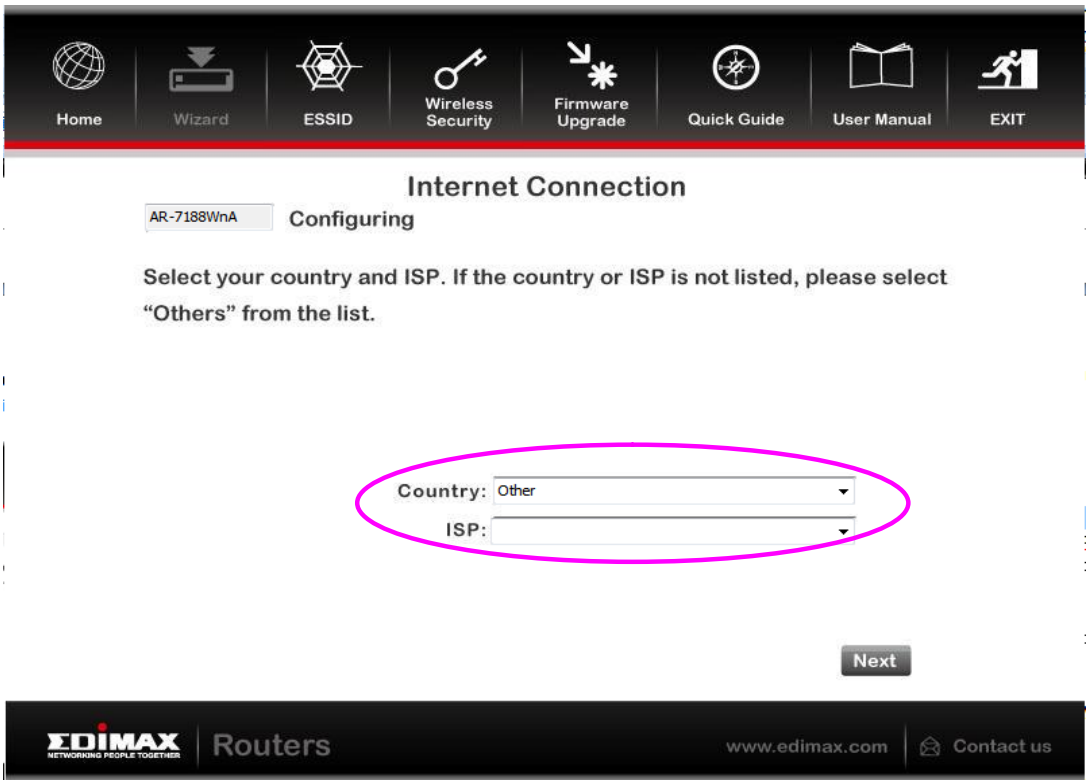


6. Please wait while the router connects to the Internet. When the router is connected successfully, you will see the screen below.

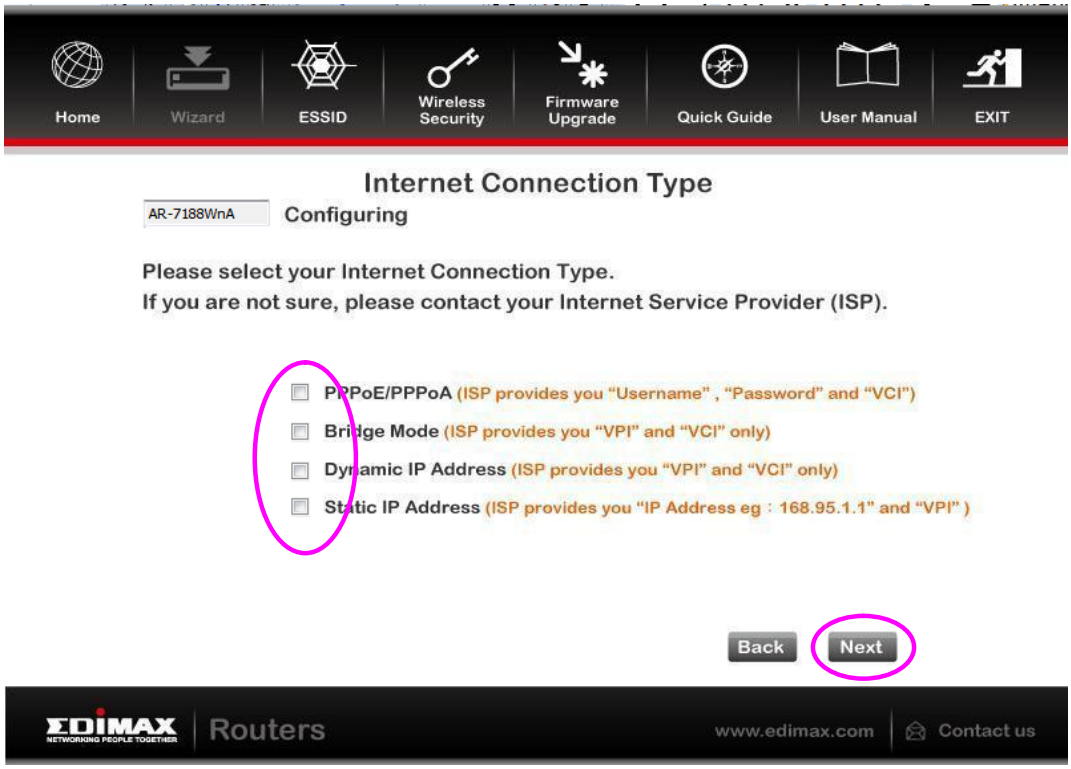


4.2. Internet Connection Type

If your country or ISP is not listed, please select “Other” from the list.



Then select your Internet connection type and click “Next”. If you are not sure, please contact your Internet Service Provider (ISP).



Depending on your selection, please refer to the appropriate chapter:

4.2.1. PPPoE/PPPoA

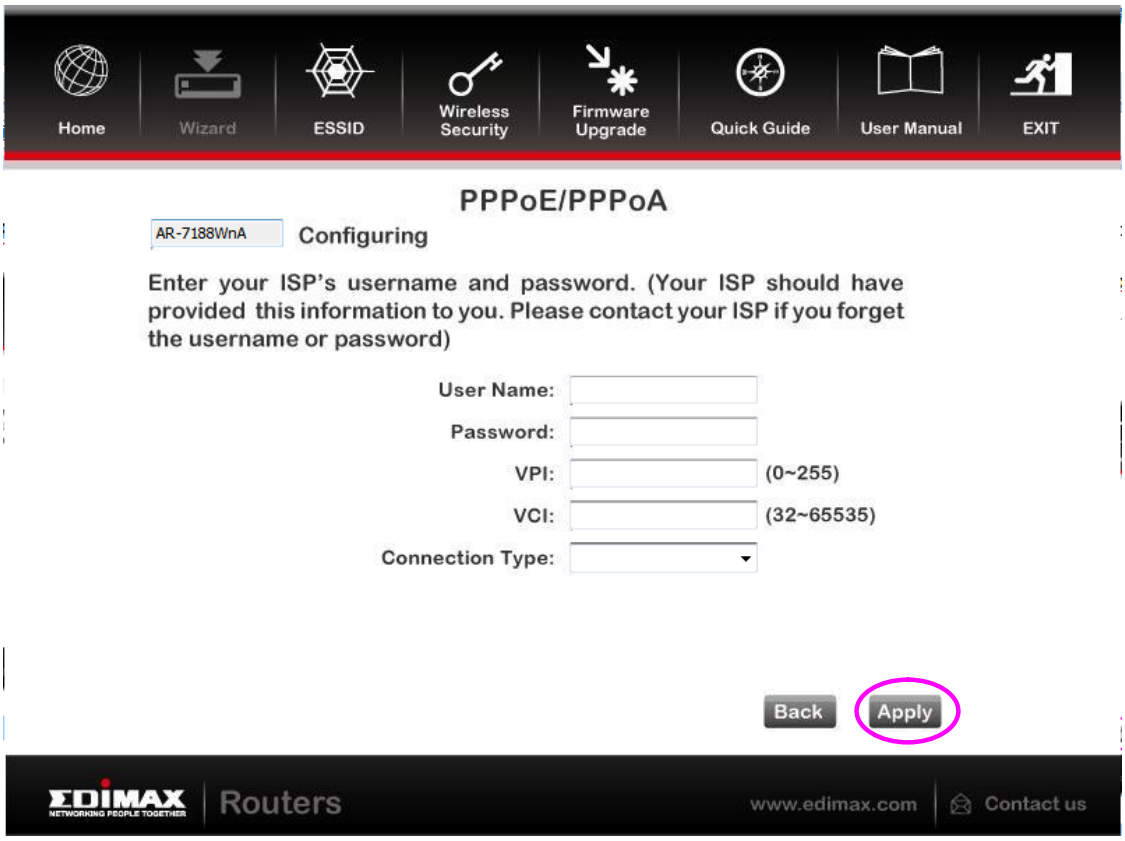
4.2.2. Bridge Mode

4.2.3. Dynamic IP Address

4.2.4. Static IP

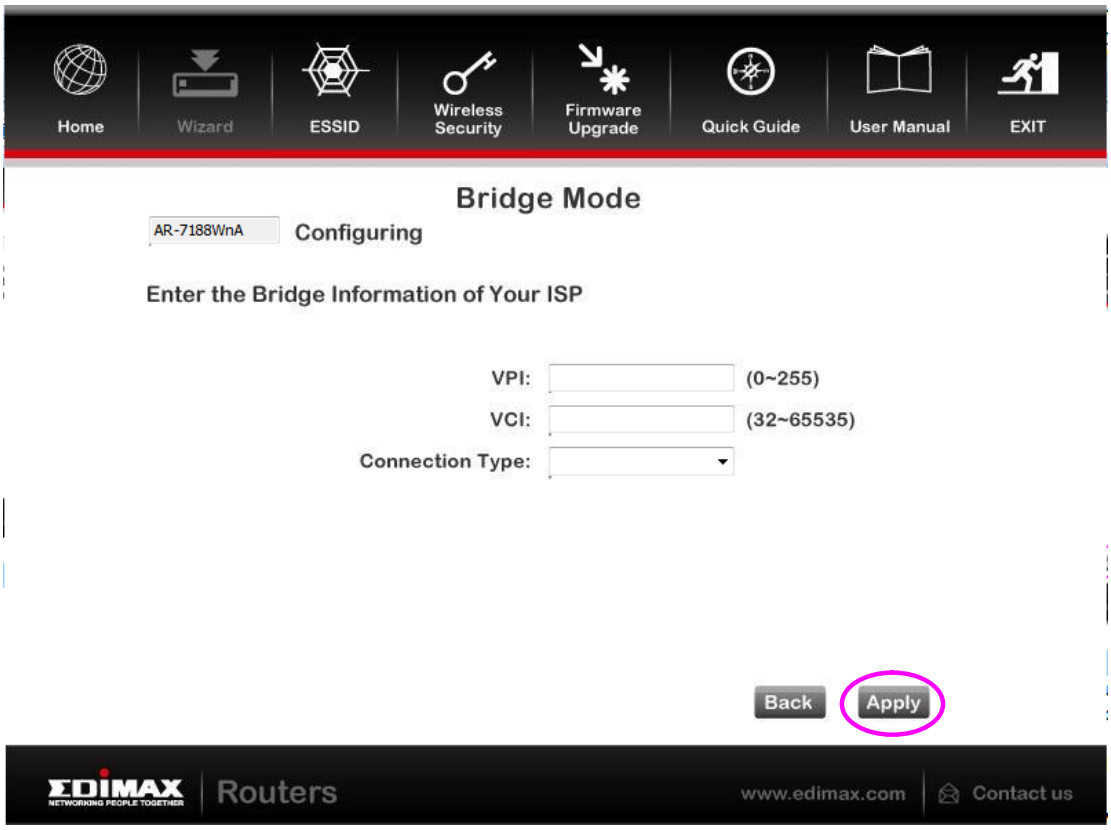
Parameter	Description
PPPoE/PPPoA	PPPoE (PPP over Ethernet) and PPPoA (PPP over ATM) are common connection methods used for xDSL.
Bridge Mode	Bridge Mode is a common connection method used for xDSL modems.
Dynamic IP Address	Obtain an IP address automatically from your service provider.
Static IP Address	Uses a static IP address. Your service provider gives a static IP address to access Internet services.

4.2.1. PPoE/PPPoA



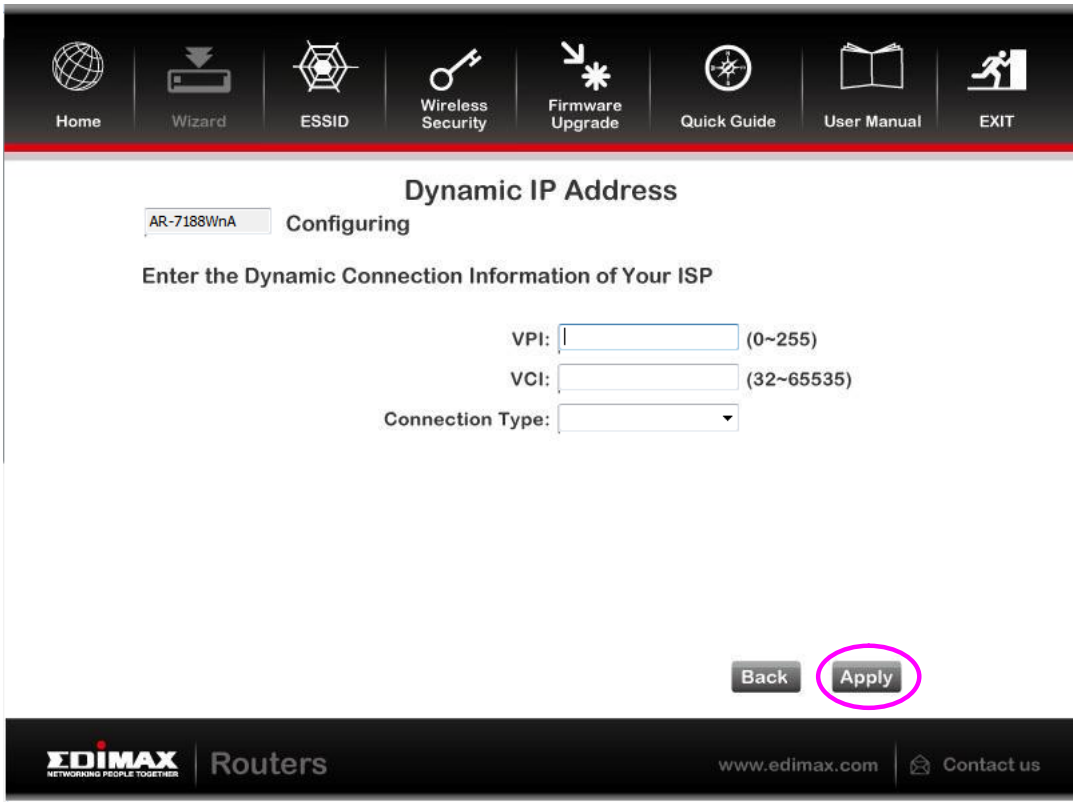
Parameter	Description
User Name	Enter the username exactly as your ISP assigned.
Password	Enter the password that your ISP has assigned to you.
VPI	Virtual path identifier (VPI) is the virtual path between two points in an ATM network. Its valid value is in the range of 0 to 255. Enter the correct VPI provided by your ISP. By default, VPI is set to 8.
VCI	Virtual channel identifier (VCI) is the virtual channel between two points in an ATM network. Its valid value is in the range of 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the correct VCI provided by your ISP. By default, VCI is set to 35.
Connection type	Please check with your ISP the method of multiplexing. In PPPoE/PPPoA mode, please select “PPPoE LLC”, “PPPoE VCMUX”, “PPPoA LLC” or “PPPoA VCMUX”.

4.2.2. Bridge Mode



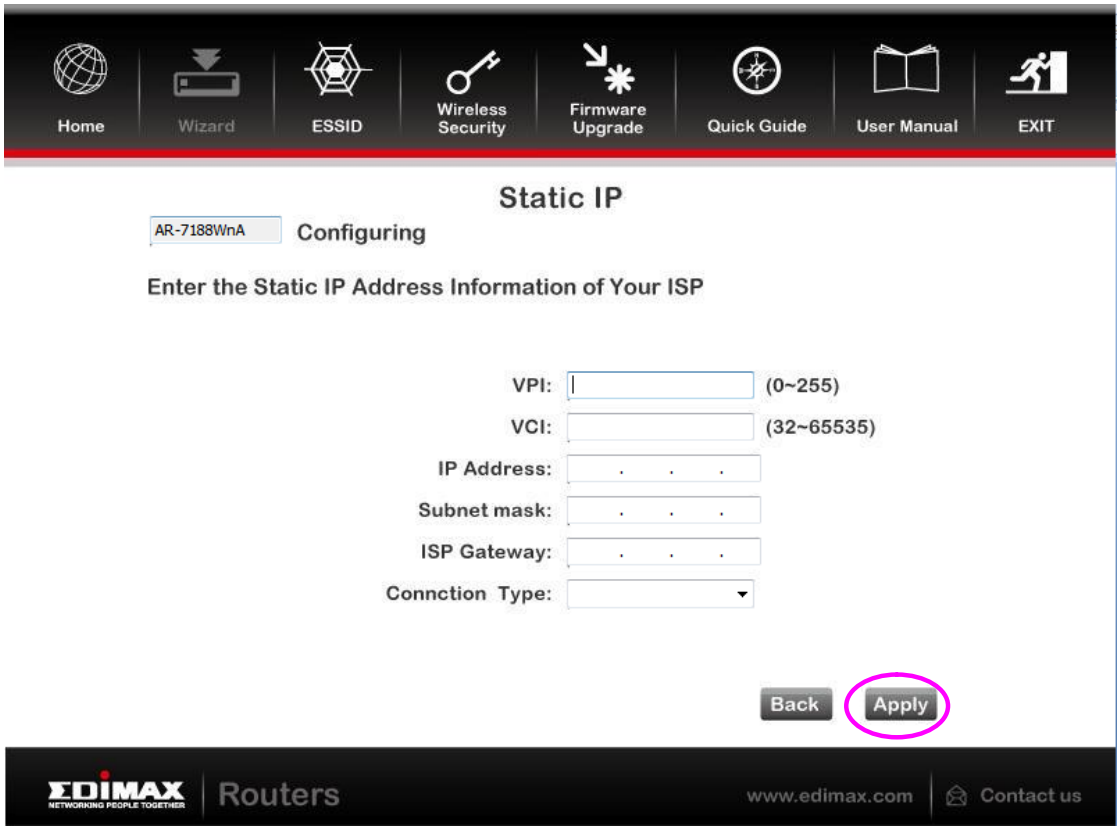
Parameter	Description
VPI	Virtual path identifier (VPI) is the virtual path between two points in an ATM network. Its valid value is in the range of 0 to 255. Enter the correct VPI provided by your ISP. By default, VPI is set to 8.
VCI	Virtual channel identifier (VCI) is the virtual channel between two points in an ATM network. Its valid value is in the range of 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the correct VCI provided by your ISP. By default, VCI is set to 35.
Connection Type	Please check with your ISP the method of multiplexing. In Bridge Mode, please select “ADSLTYPE_ROUTER_LLC” or “ADSLTYPE_ROUTER_VCMUX”.

4.2.3. Dynamic IP Address



Parameter	Description
VPI	Virtual path identifier (VPI) is the virtual path between two points in an ATM network. Its valid value is in the range of 0 to 255. Enter the correct VPI provided by your ISP. By default, VPI is set to 8.
VCI	Virtual channel identifier (VCI) is the virtual channel between two points in an ATM network. Its valid value is in the range of 32 to 65535. (0 to 31 is reserved for local management of ATM traffic) Enter the correct VCI provided by your ISP. By default, VCI is set to 35.
Connection Type	Please check with your ISP the method of multiplexing. In Bridge Mode, please select “ADSLTYPE_ROUTER_LLC” or “ADSLTYPE_ROUTER_VCMUX”.

4.2.4. Static IP

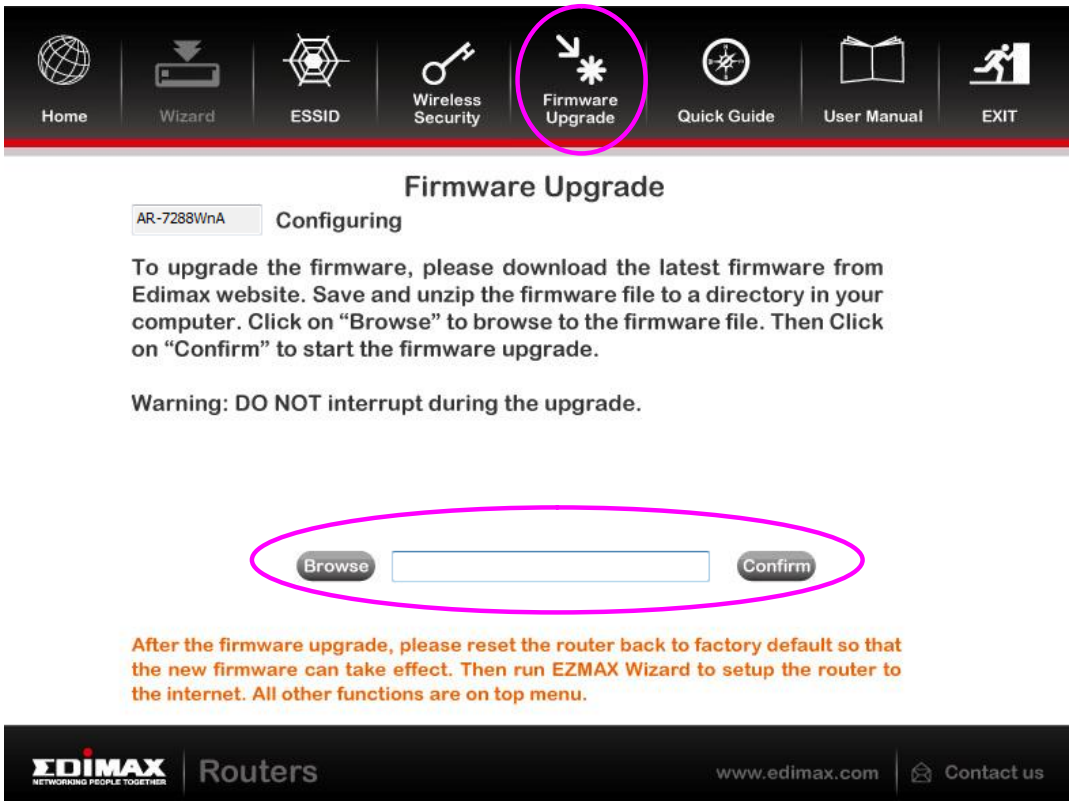


Parameter	Description
VPI	Virtual path identifier (VPI) is the virtual path between two points in an ATM network. Its valid value is in the range of 0 to 255. Enter the correct VPI provided by your ISP. By default, VPI is set to 8.
VCI	Virtual channel identifier (VCI) is the virtual channel between two points in an ATM network. Its valid value is in the range of 32 to 65535. (0 to 31 is reserved for local management of ATM traffic) Enter the correct VCI provided by your ISP. By default, VCI is set to 35.
Static IP Address	Enter the IP Address assigned by your ISP.
IP Subnet Mask	Enter the Subnet Mask assigned by your ISP.
Gateway	Enter the Gateway assigned by your ISP.

Connection Type	Please check with your ISP the method of multiplexing. In Bridge Mode, please select “ADSLTYPE_ROUTER_LLC” or “ADSLTYPE_ROUTER_VCMUX”.

4.3. Firmware Upgrade

The wizard includes a tool to upgrade the router’s firmware. Firmware can be downloaded from the Edimax website; if you wish to upload new firmware, select “Firmware Upgrade” from the menu across the top of the screen.



5. Web-Based Management

The router can also be configured using the web-based configuration interface. Follow the instructions below.

5.1. Accessing the Router

To access the web-based configuration interface:

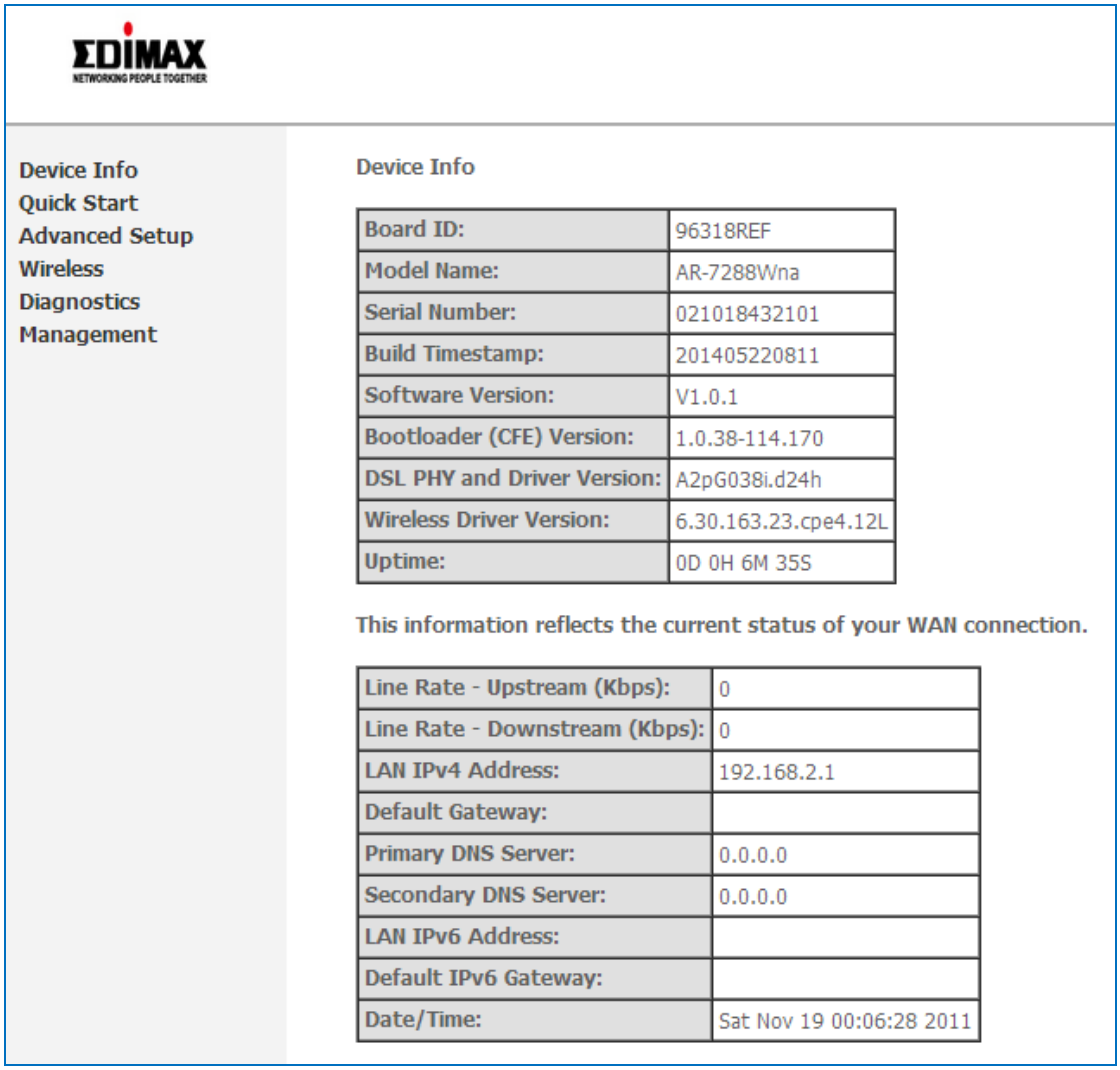
1. Open the Internet Explorer (IE) browser and enter **http://192.168.2.1**.

2. In the **Login** page that is displayed, enter the username and password.

- The username and password of the super user are **admin** and **1234**.

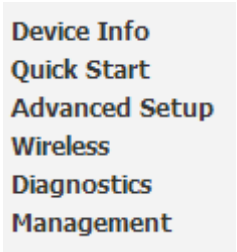
Note:
In the Web configuration page, the settings can be saved permanently.

After logging in to the DSL router as a super user, the page shown as the following figure appears. You can query, configure, and modify all the settings, and diagnose the system.



5.2. Device Info

Choose **Device Info**, and the submenus of **Device Info** are shown as below: You can view the basic information of the router and running status of all interfaces.



5.3. Advanced Setup

Click **Advanced Setup** and the submenus of **Advanced Setup** appears. In this section, you can set the parameters of the router to connect to the internet

5.3.1. Layer2 Interface

- **ATM Interface**

For the first time to configure your router, you need to add at least an ATM Interface.

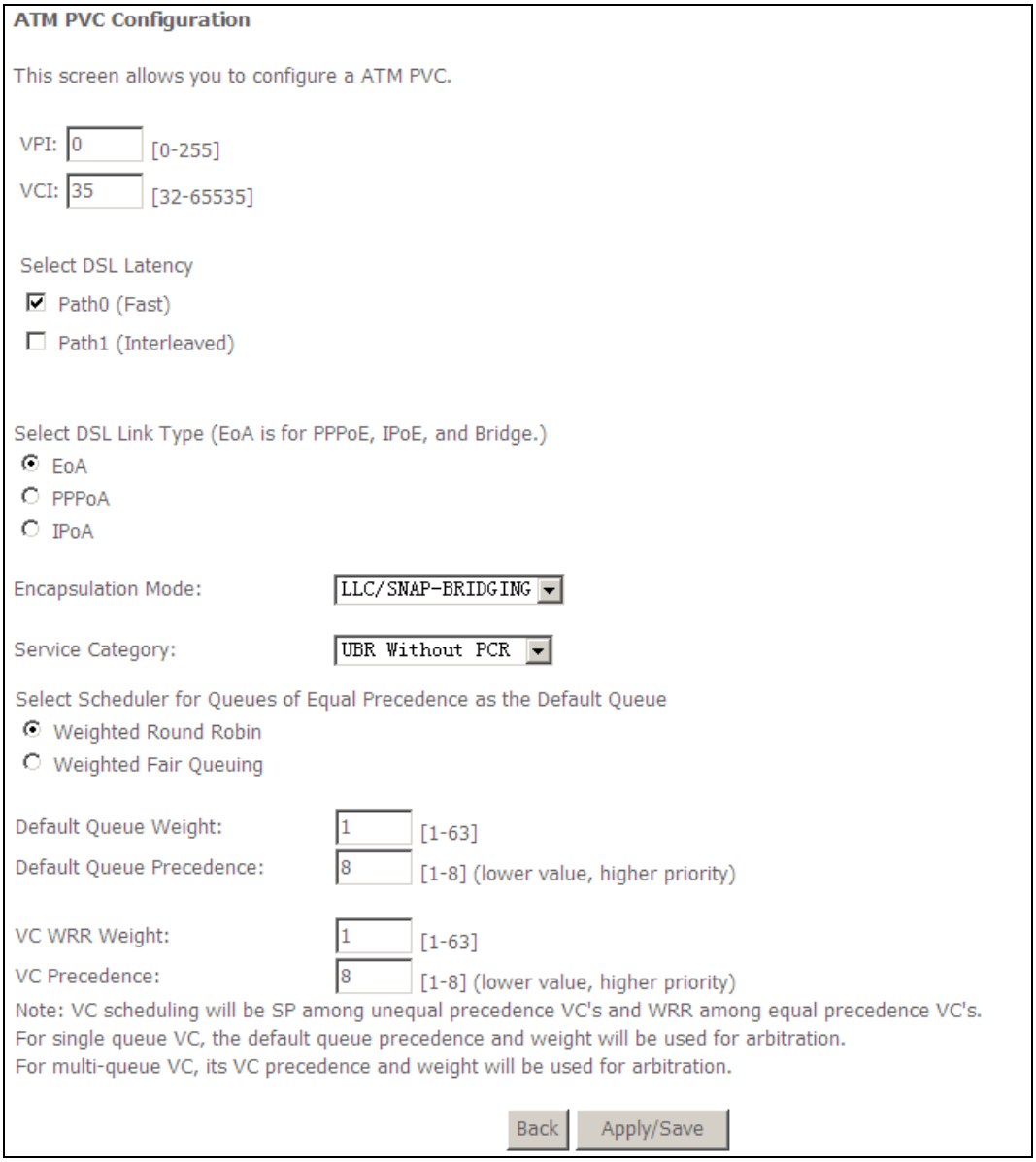
Step 1 Choose **Advance Setup** > **Layer2 Interface** > **ATM Interface**, and the following page appears. In this page, you can add or remove the DSL ATM Interfaces.

DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Peak Cell Rate(cells/s)	Sustainable Cell Rate(cells/s)	Max Burst Size(bytes)	Min Cell Rate(cells/s)	Link Type	Connection Mode	IP QoS	MPAAL Prec/Alg/Wght	Remove

Step 2 In this page, click **Add** to add an ATM interface, and the following page appears.



Step 3 In this page, you can set the parameters of an ATM interface. Select **DSL Link Type** to be **EoA** if you want to add a PPPoE WAN Service. Keep other parameters as default. Then click **Apply/Save**. An ATM Interface is added as the coming page displays.

DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Peak Cell Rate(cells/s)	Sustainable Cell Rate(cells/s)	Max Burst Size(bytes)	Min Cell Rate(cells/s)	Link Type	Connection Mode	IP QoS	MPAAL Prec/Alg/Wght	Remove
atm0	0	35	Path0	UBR					EoA	VlanMuxMode	Support	8/WRR/1	☐

Add Remove

Note:

QoS cannot be set for CBR and Realtime VBR.

- **ETH Interface**

Choose **Advanced Setup > Layer2 Interface > ETH Interface**, and the following page appears.

ETH WAN Interface Configuration

Choose Add, or Remove to configure ETH WAN interfaces.
Allow one ETH as layer 2 wan interface.

Name	Connection Mode	Remove

Add Remove

In this page, you can add or remove the DSL ETH Interfaces.

Click the **Add** button to display the following page. In this page, select a Ethernet port to configure. After setting, click the **Apply/Save** button to enable the settings.

ETH WAN Configuration

This screen allows you to configure an ETH port .

Select an ETH port:

eth0/eth0

Back Apply/Save

5.3.2. WAN Service

Choose **Advance Setup** > **WAN Service** and the following page appears. In this page, you may add, remove or edit a WAN service.

Wide Area Network (WAN) Service Setup

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

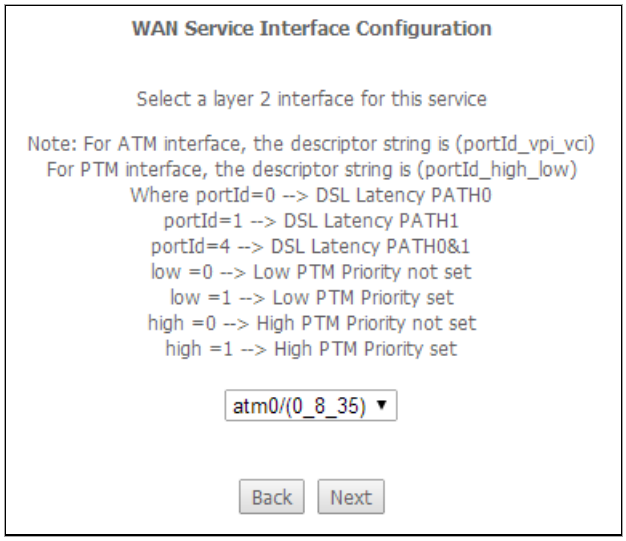
Interface	Description	Type	Vlan802.1p	VlanMuxId	Igmp	NAT	Firewall	IPv4	IPv6	Mld	Remove	Edit	Action

Add Remove

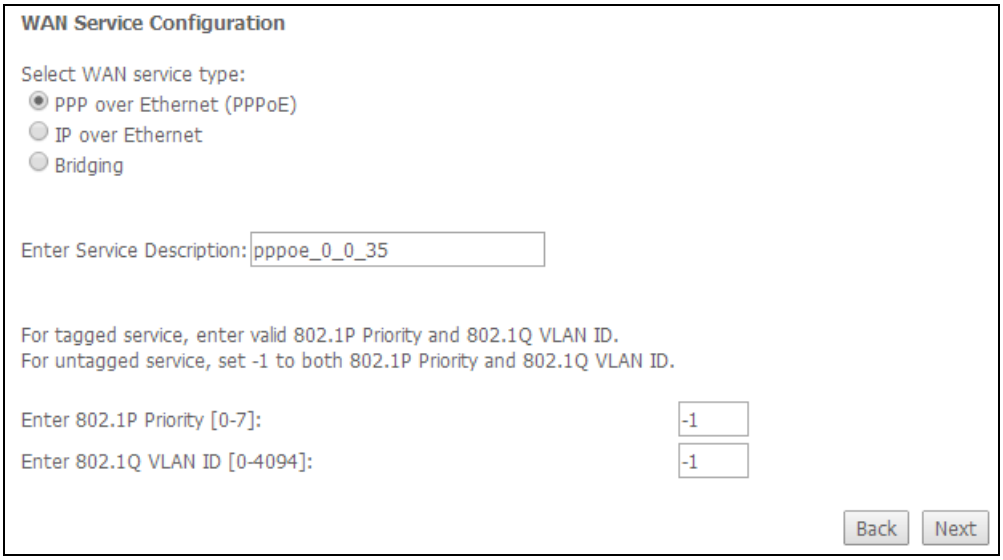
- **Adding a PPPoE WAN Service**

This section describes the steps for adding the PPPoE WAN service.

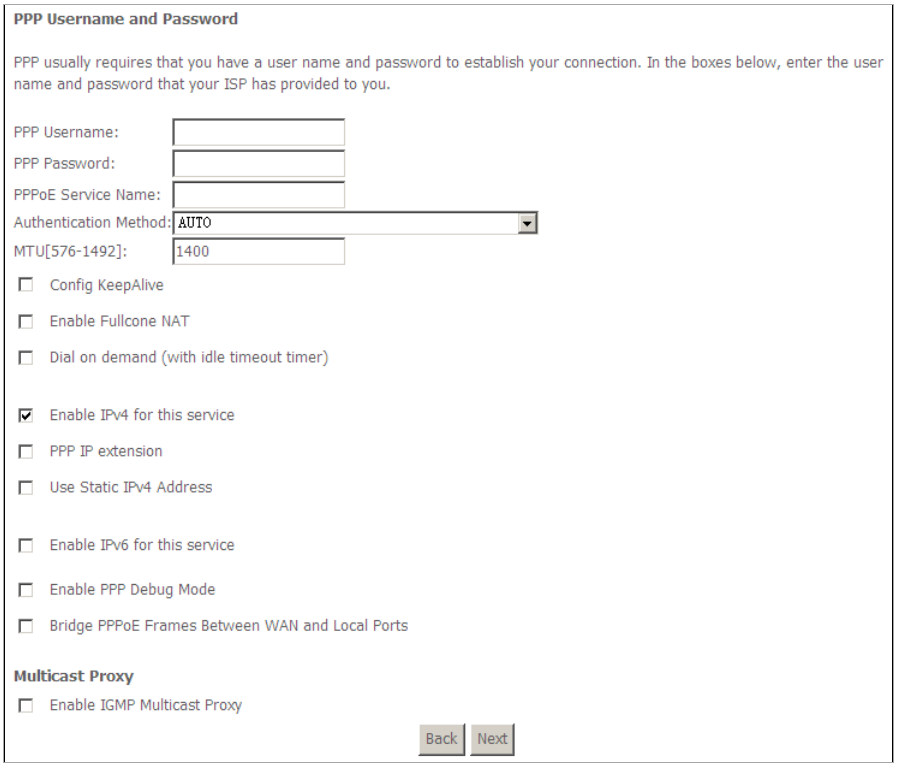
Step 1 In the **Wide Area Network (WAN) Service Setup** page, click the **Add** button to display the following page. (First a proper ATM configuration should be added for this WAN service.)



Step 2 In this page, you can select an ATM Interface for the WAN service. After selecting the ATM interface, click **Next** to display the following page.



Step 3 In this page, select the WAN service type to be **PPP over Ethernet (PPPoE)**. Click **Next** to display the following page.

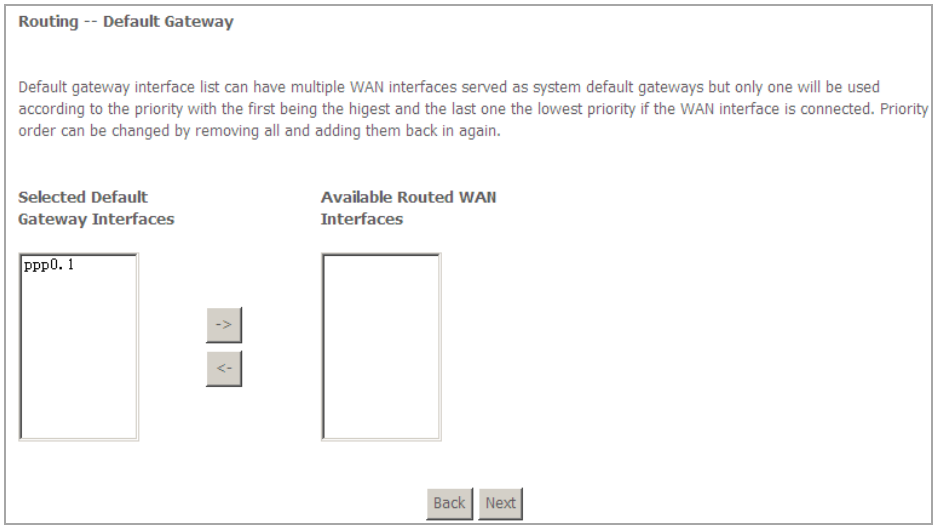


Step 4 In this page, you can modify the PPP username, PPP password, PPPoE service name and authentication method.

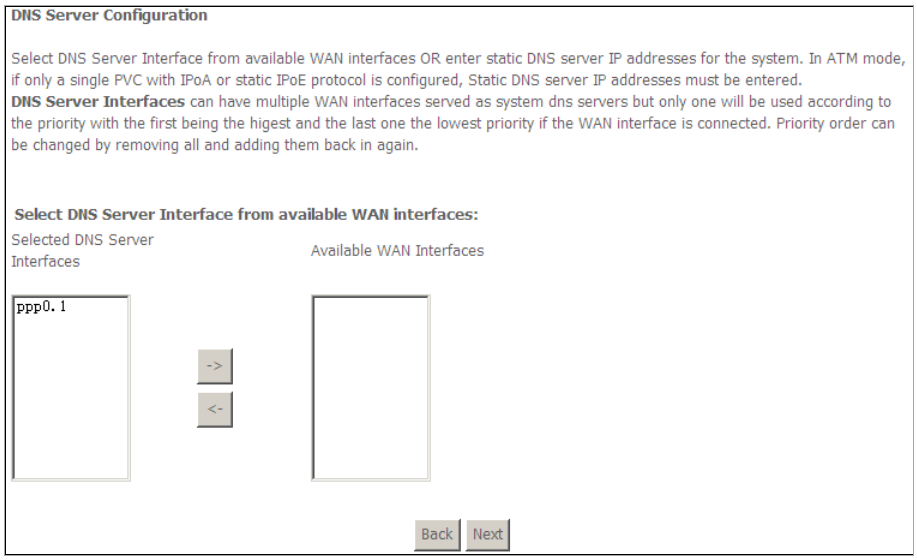
- **PPP Username**: The correct user name provided by your ISP.
- **PPP Password**: The correct password provided by your ISP.
- **PPPoE Service Name**: If your ISP provides it to you, please enter it. If not, do not enter any information.
- **Authentication Method**: The method to testify the entered PPP username and password. Usually, you can select AUTO.
- **Enable Fullcone NAT**: NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.
- **Dial on demand (with idle timeout timer)**: If this function is enabled, you need to enter the idle timeout time. Within the preset minutes, if the router does not detect the flow of the user continuously, the router automatically stops the PPPoE connection. Once it detects the flow (like access to a webpage), the router restarts the PPPoE dialup. If this function is disabled, the router performs PPPoE dial-up all the time.
- **PPP IP extension**: If you want to configure DMZ Host, you should enable it first.
- **Use Static IPv4 Address**: If this function is disabled, the router obtains an IP address assigned by uplink equipment such as BAS, through PPPoE dial-up. If this function is enabled, the router uses this IP address as the WAN IP address.

- **Enable PPP Debug Mode**: Enable or disable this function.
- **Bridge PPPoE Frames Between WAN and Local Ports**: Enable or disable this function.
- **Enable IGMP Multicast Proxy**: If you want PPPoE mode to support IPTV, enable it.

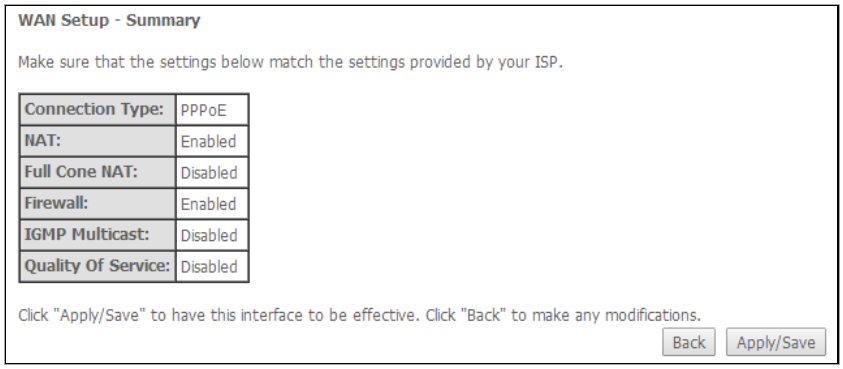
Step 5 After setting the parameters, click **Next** to display the following page.



Step 6 In this page, select a **preferred WAN interface** as the system default gateway interface and then click **Next** to display the following page.



Step 7 In this page, you may select a **DNS server interface** from the available WAN interfaces. Click **Next**, and the following page appears.

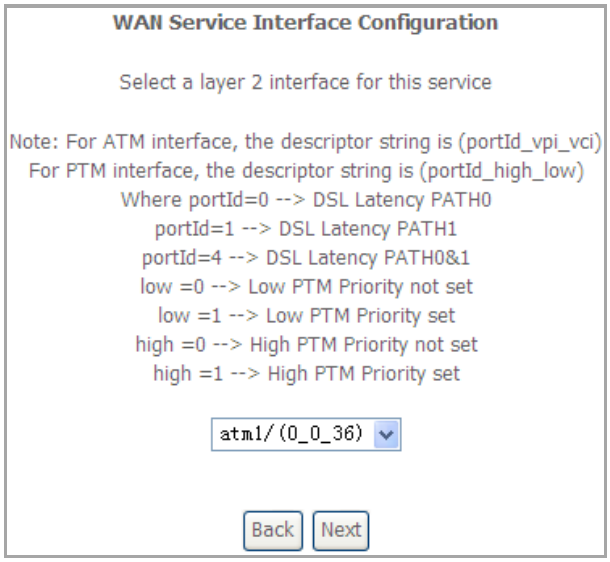


Step 8 In this page, it displays the information about the PPPoE settings. Click **Apply/Save** to save and apply the settings.

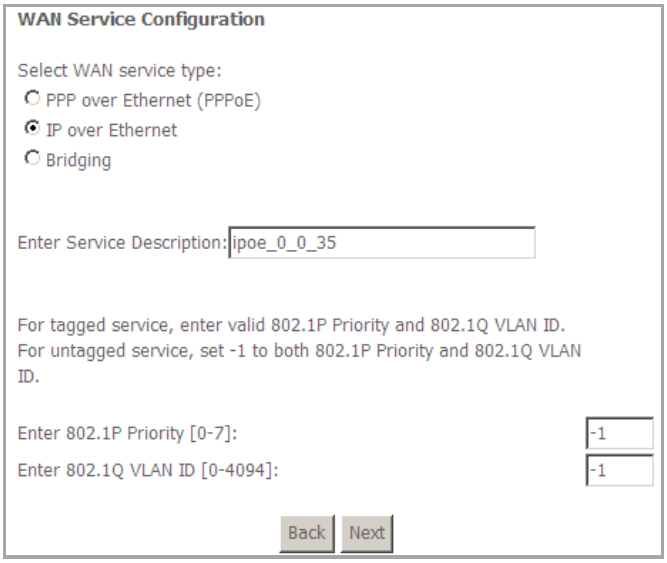
Adding a MER (IPoE) WAN service

This section describes the steps for adding the MER WAN service.

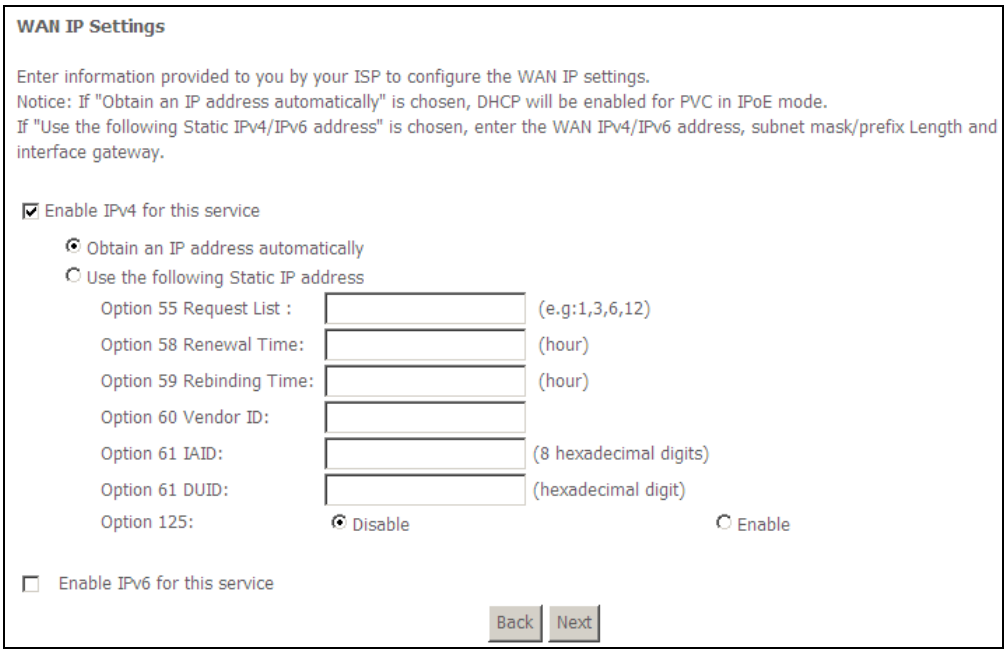
Step 1 Back to the **Wide Area Network (WAN) Service Setup** page, and click the **Add** button to display the following page. (At first, you must add an ATM interface for this WAN service.)



Step 2 Select an ATM Interface, and then click **Next** to display the following page.



Step 3 In this page, select the WAN service type to be **IP over Ethernet**, enter the service description for this service. After setting, click **Next** to display the following page.

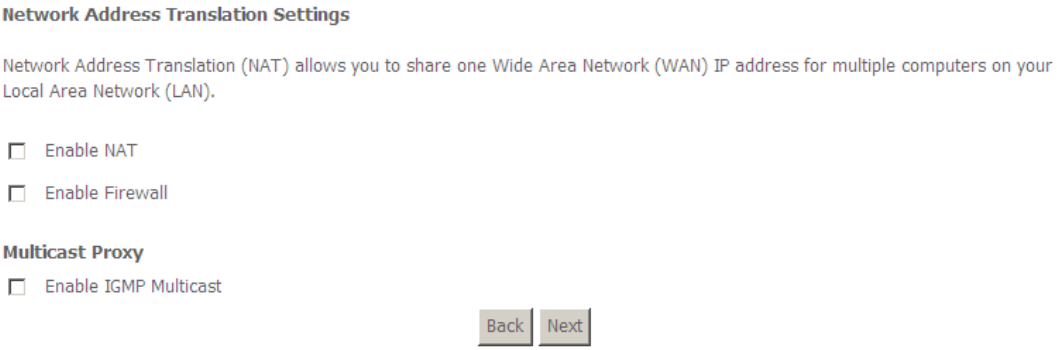


Step 4 In this page, you may modify the WAN IP settings. You may select obtain an IP address automatically or manually enter the IP address provided by your ISP. Click **Next** and the following page appears.

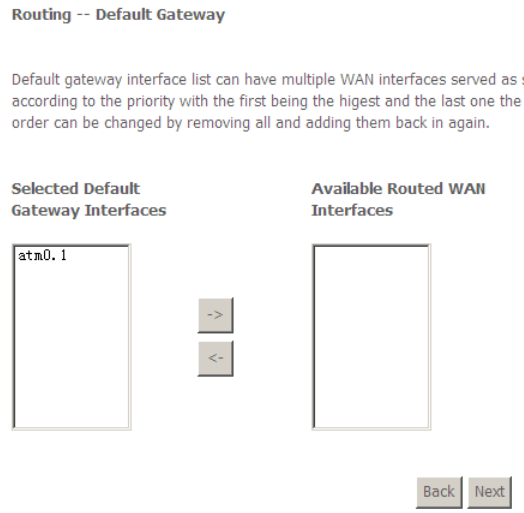
Note:

*If selecting **Obtain an IP address automatically**, DHCP will be enabled for PVC in MER mode.*

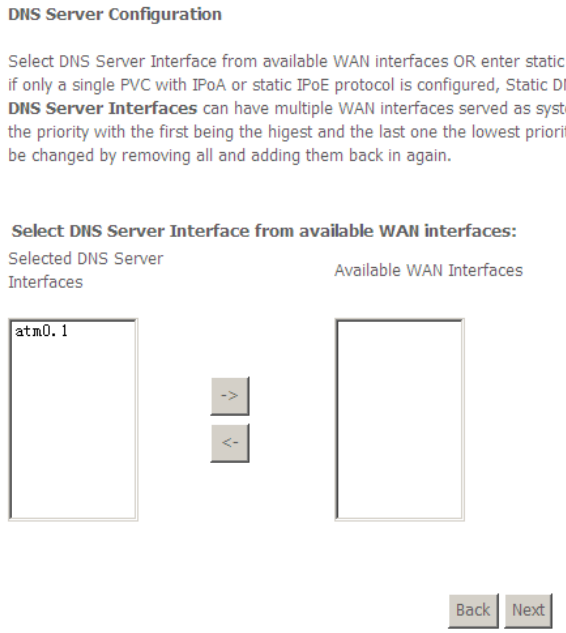
*If selecting **Use the following Static IP address**, please enter the WAN IP address, subnet mask and gateway IP address.*



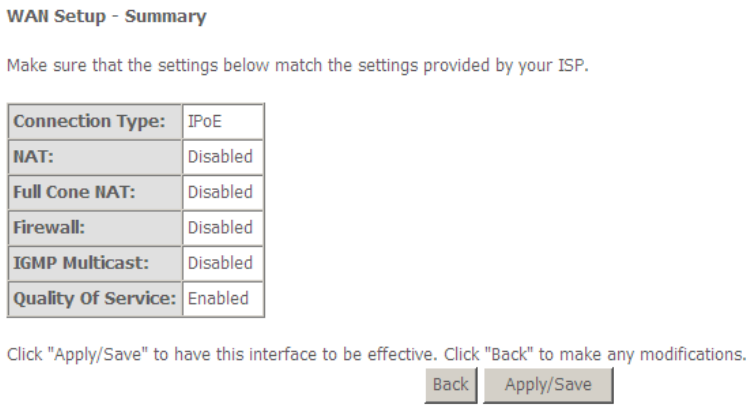
Step 5 In this page, you can set the network address translation settings,for example, enabling NAT, enabling firewall, and enabling IGMP multicast. After setting, click **Next** and the following page appears.



Step 6 In this page, select a preferred WAN interface as the system default gateway interface and then click **Next** to display the following page.



Step 7 In this page, you may select a DNS server interface from the available WAN interfaces. After setting, click **Next** to display the following page.

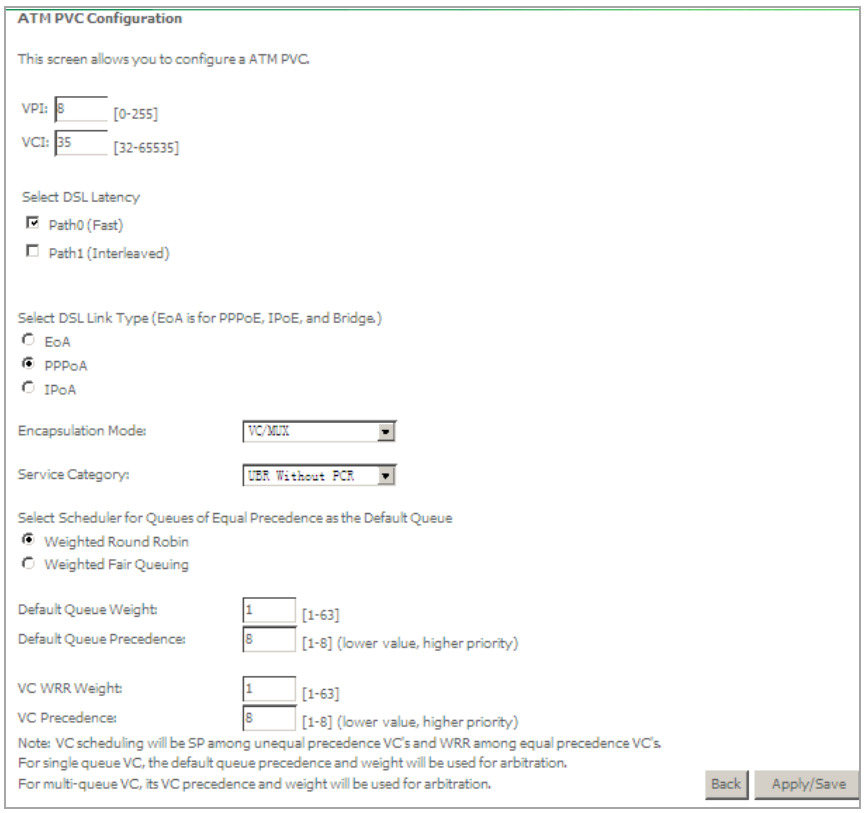


Step 8 In this page, it displays the information about the IPoE settings. Click **Apply/Save** to save and apply the settings.

Adding a PPPoA WAN service

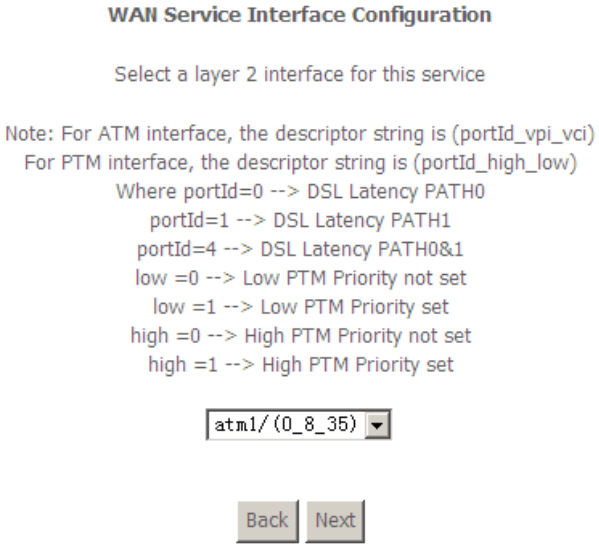
This section describes the steps for adding the PPPoA WAN service.

Step 1 Choose **Advanced Setup** > **Layer2 Interface** > **ATM Interface** to dsipaly the **DSL ATM Interface Configuration** page. In this page, you need to add a PVC for PPPoA mode. Click the **Add** button in the **DSL ATM Interface Configuration** page to display the following page.



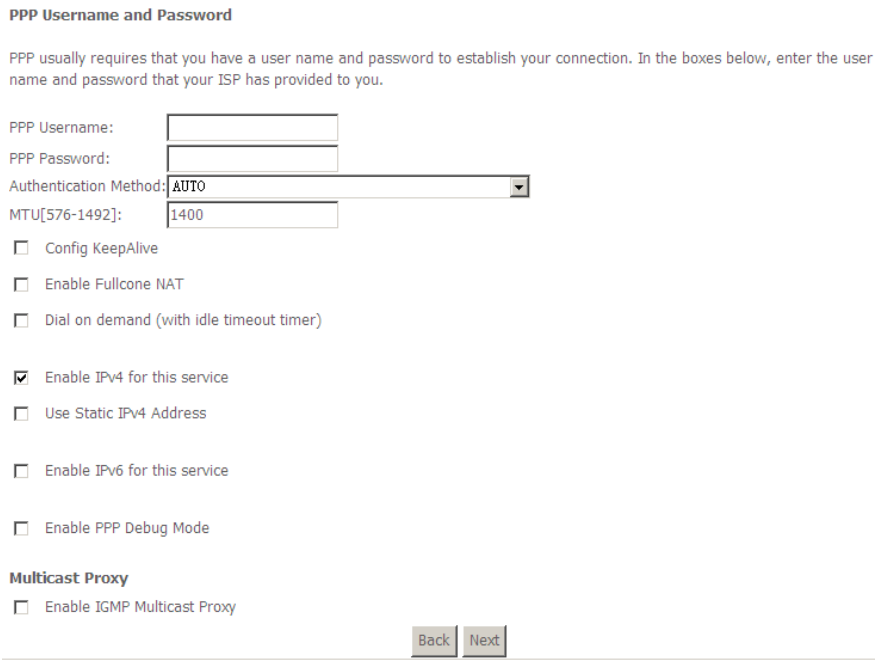
Step 2 Select the DSL link type to be **PPPoA**, and select the encapsulation mode to be **VC/MUX** (according to the uplink equipment). After setting, click the **Apply/Save** button to apply the settings.

Step 3 Choose **WAN Service** and click **Add** to display the following page.



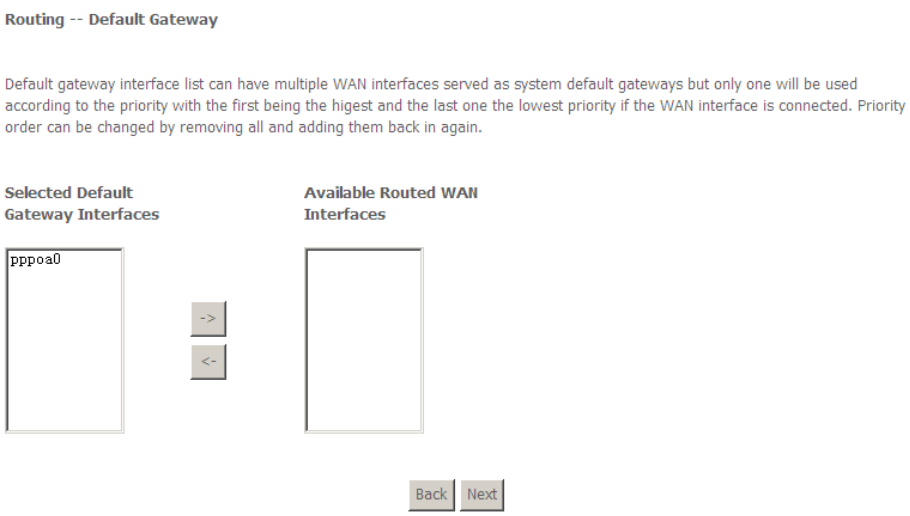
Step 4 Select the proper interface for the WAN service, and then click **Next** to display the following page.

Step 5 In this page, you may modify the service description. Click **Next** to display the following page.

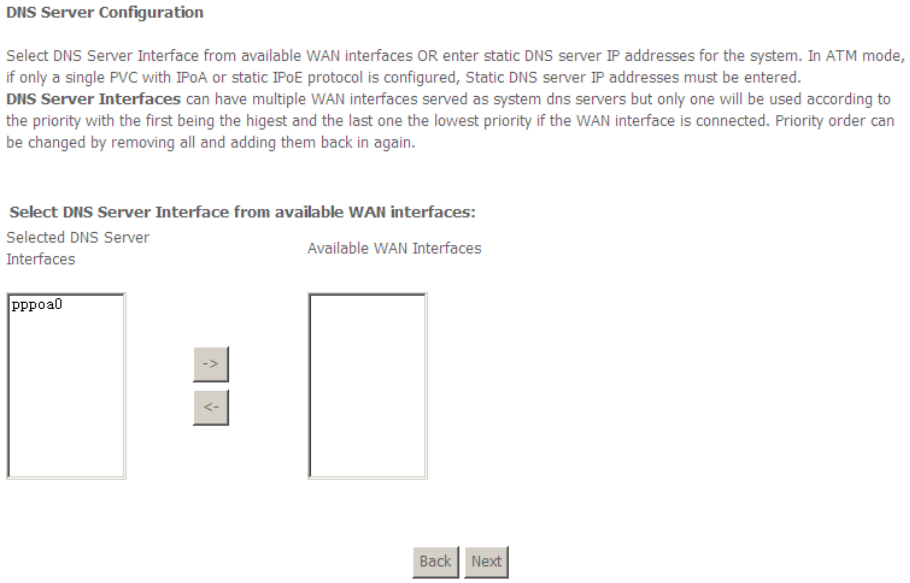


Step 6 In this page, you can enter the PPP username and PPP password provided by your ISP. Select the authentication method according to your requirement. After setting, click **Next** to display the following page.

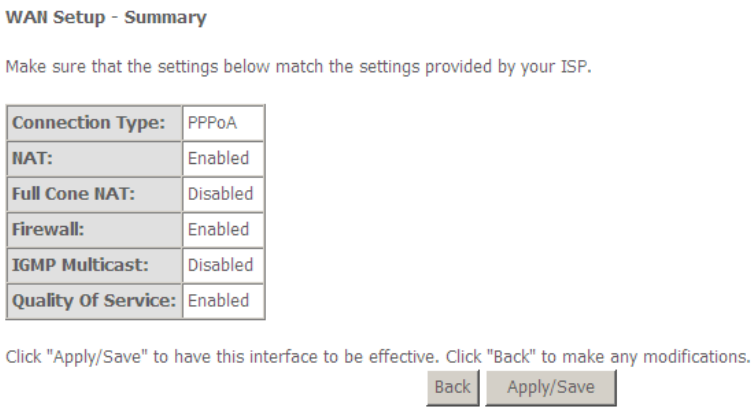
- **PPP Username/PPP Password:** The correct user name provided by your ISP.
- **Authentication Method:** The value can be **AUTO**, **PAP**, **CHAP**, or **MSCHAP**. Usually, you can select **AUTO**.
- **Enable Fullcone NAT:**. NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.
- **Dial on demand (with idle timeout timer):** If this function is enabled, you need to enter the idle timeout time. Within the preset minutes, if the modem does not detect the flow of the user continuously, the modem automatically stops the PPPoA connection. Once it detects the flow (like access to a webpage), the modem restarts the PPPoA dialup. If this function is disabled, the modem performs PPPoA dial-up all the time. The PPPoA connnection does not stop, unless the modem is powered off and DSLAM or uplink equipment is abnormal.
- **Enable IPv4 for this service**: Check this checkbox, this interface will support IPv4.
- **Use Static IPv4 Address:** If this function is disabled, the modem obtains an IP address assigned by an uplink equipment such as BAS, through PPPoA dial-up. If this function is enabled, the modem uses this IP address as the WAN IP address.
- **Enable IPv6 for this service:** Check this checkbox, this interface will support IPv4.
- **Enable PPP Debug Mode:**Enable or disable this function.
- **Enable IGMP Multicast Proxy:** If you want PPPoE mode to support IPTV, enable it.



Step 7 In this page, select a preferred WAN interface as the system default gateway interface and then click **Next** to display the following page.



Step 8 In this page, you may select a DNS server interface from the available WAN interfaces. After setting, click **Next** to display the following page.

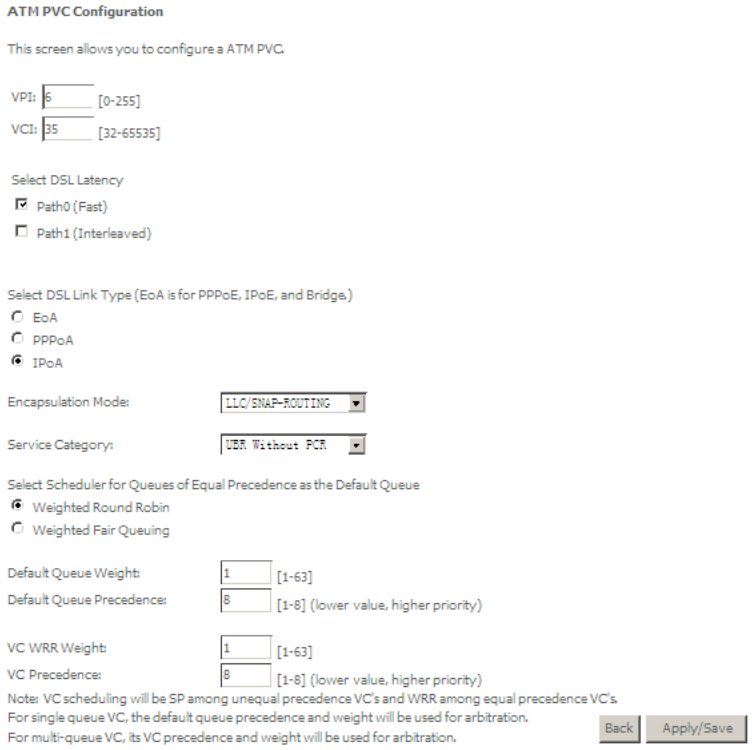


Step 9 In this page, it displays the information about the PPPoA settngs.Click **Apply/Save** to apply the settings. You can modify the settings by clicking the **Back** button if necessary.

Adding an IPoA WAN service

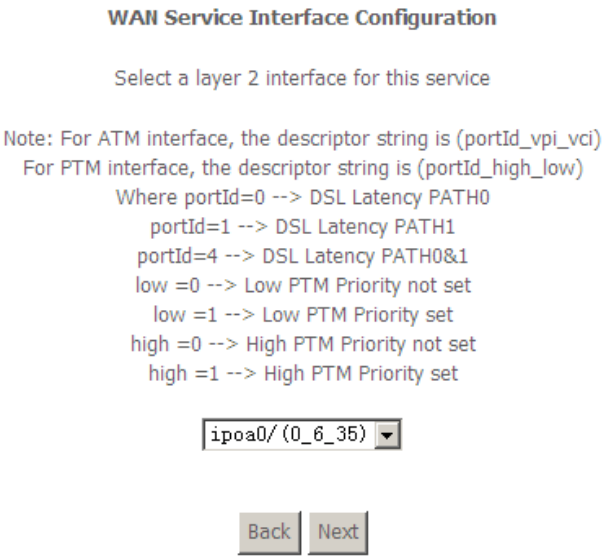
This section describes the steps for adding the IPoA WAN service.

Step 1 Choose **Advanced Setup > Layer2 Interface > ATM Interface** to dsipaly the **DSL ATM Interface Configuration** page. In this page, you need to add a PVC for IPoA mode. Click the **Add** button in the **DSL ATM Interface Configuration** page to display the following page.

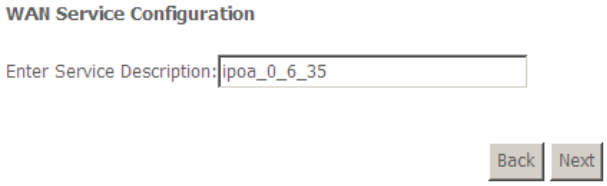


Step 2 Select the DSL link type to be **IPoA**, and select the encapsulation mode to be **LLC/SNAP-ROUTING** (according to the uplink equipment). After setting, click the **Apply/Save** button to save the settings.

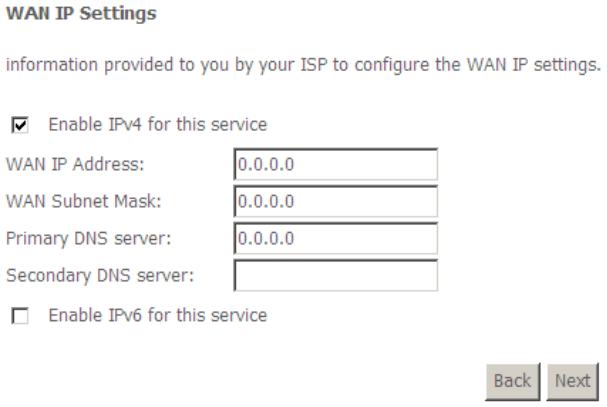
Step 3 Choose **WAN Service** and click **Add** to display the following page.



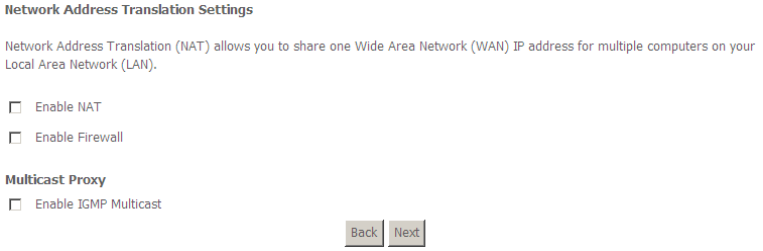
Step 4 Select the proper interface for the WAN service ,and then click **Next** to display the following page.



Step 5 In this page, you may modify the service description. Click **Next** to display the following page.



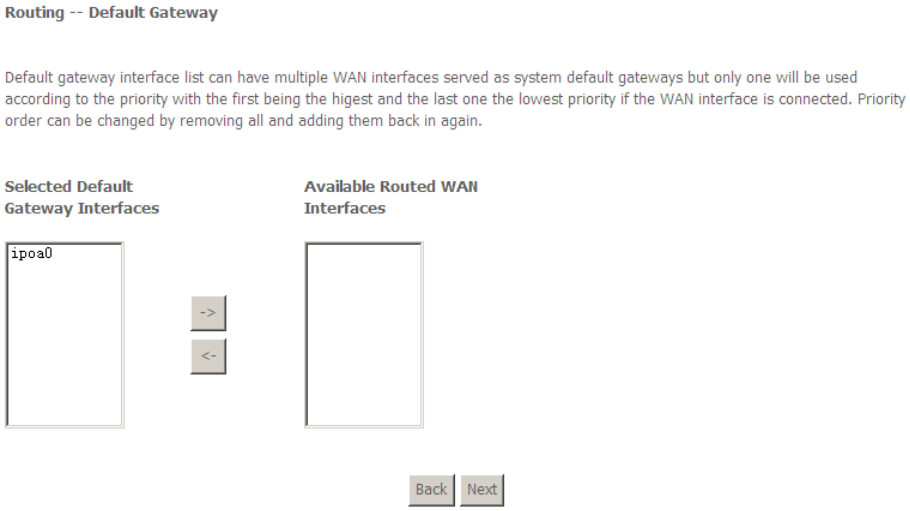
Step 6 In this page, enter the WAN IP address and the WAN subnet mask provided by your ISP and then click **Next** to display the following page.



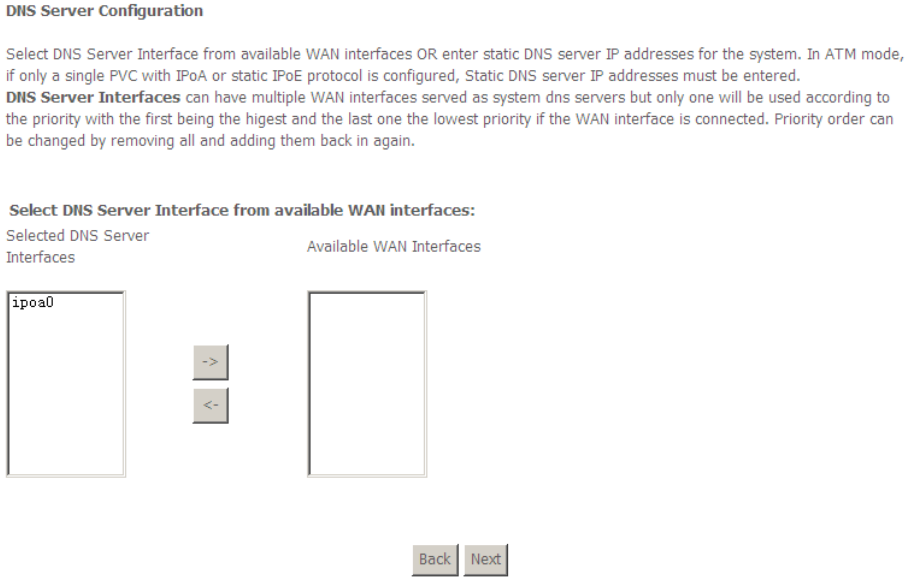
In this page, Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

If you do not want to enable NAT, and wish the user of modem to access the Internet normally, you need to add a route on the uplink equipment. Otherwise, the access to the Internet fails. Normally, please enable the NAT function.

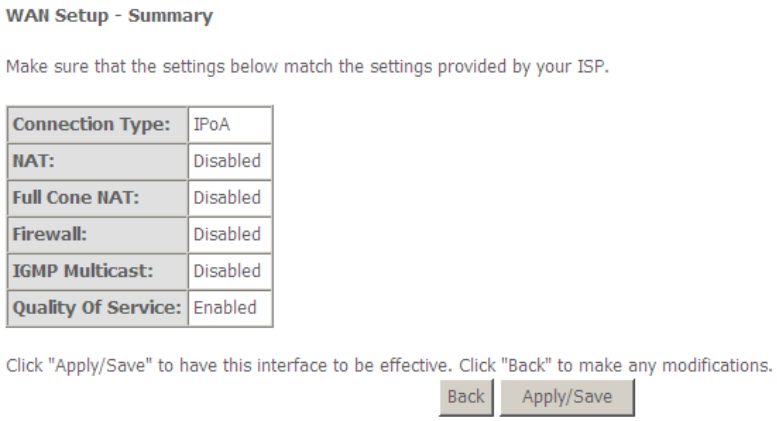
Step 7 After setting, click **Next** to display the following page.



Step 8 In this page, select a preferred WAN interface as the system default gateway interface and then click **Next** to display the following page.



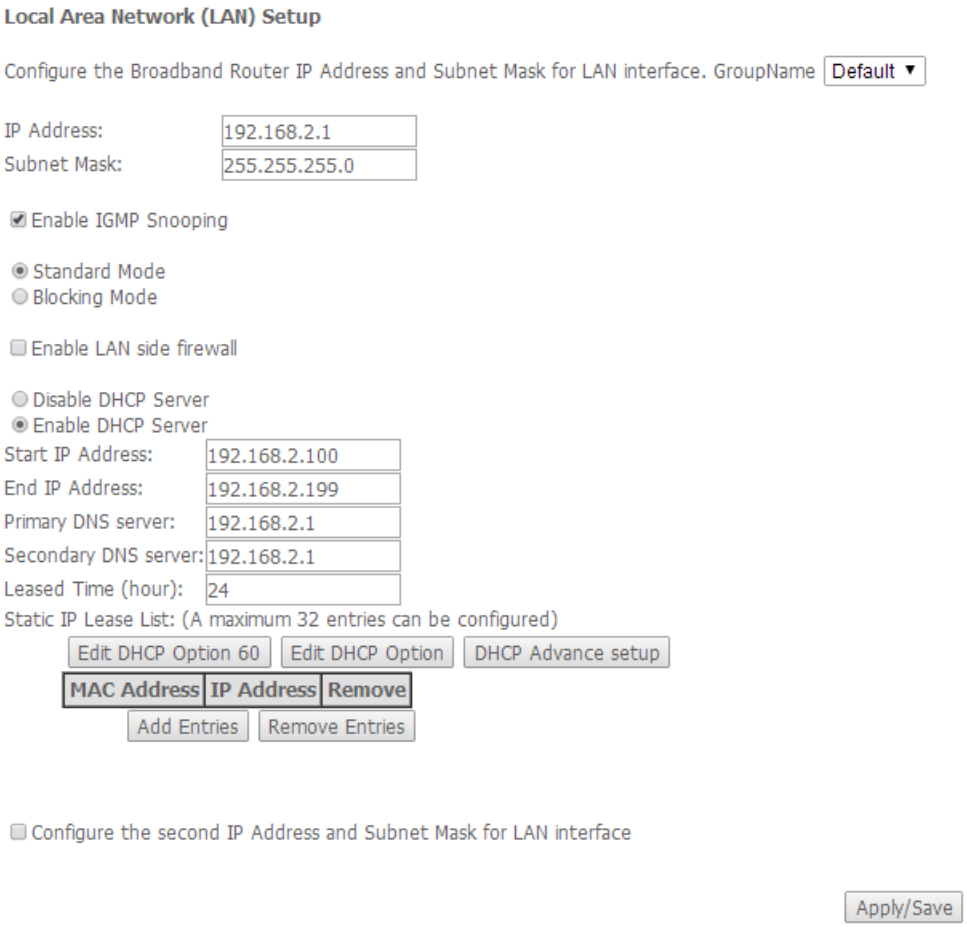
Step 9 In this page, you may select a DNS server interface from the available WAN interfaces. Click **Next** to display the following page.



Step 10 In this page, it displays the information about the IPoA settngs. Click **Apply/Save** to save and apply the settings. You can modify the settings by clicking the **Back** button if necessary.

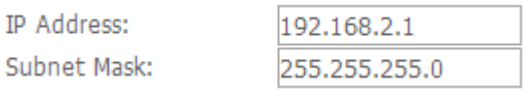
5.3.3. LAN Configuration

Choose **Advanced Setup > LAN**, and the following page appears.



In this page, you can configure an IP address for the DSL router, enable IGMP snooping, enable or disable the DHCP server, edit the DHCP option, configure the DHCP advanced setup and set the binding between a MAC address and an IP address.

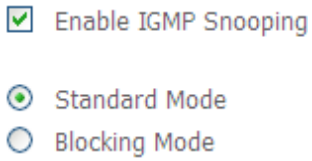
Configuring the Private IP Address for the DSL Router



In this page, you can modify the IP address of the device. The preset IP address is 192.168.1.1.

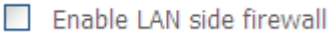
Enable IGMP Snooping

IGMP snooping enables the router to forward multicast traffic intelligently, instead of flooding all ports in the VLAN. With IGMP snooping, the router listens to IGMP membership reports, queries and leave messages to identify the switch ports that are members of multicast groups. Multicast traffic will only be forwarded to ports identified as members of the specific multicast group or groups.



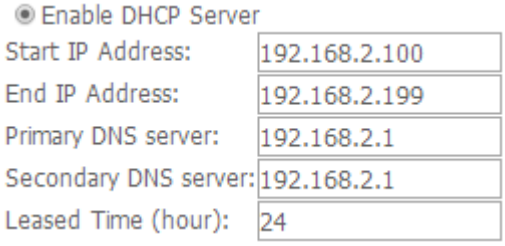
Enabling the LAN Side Firewall

Firewall can prevent unexpected traffic on the Internet from your host in the LAN.



In this page, you can enable or disable the LAN side firewall.

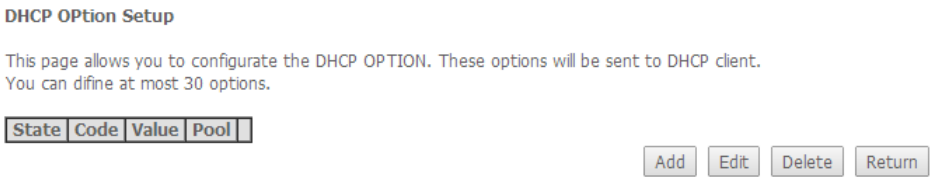
Configuring the DHCP Server



If you enable the DHCP sever, the clients will automatically acquire the IP address from the DHCP server. If the DHCP server is disabled, you need to manually set the start IP address, end IP address and the lease time for the clients in the LAN.

Editing the DHCP Option

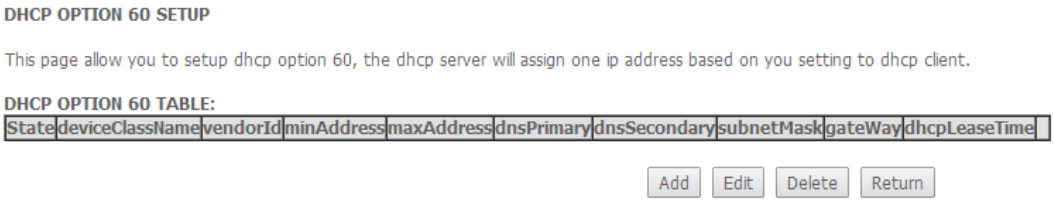
Click the **Edit DHCP Option** button in the **Local Area Network (LAN) Setup** page to display the **DHCP Option Setup** page.



In this page, you can add, edit or delete the DHCP options, and these options will be sent to the DHCP client.

Editing the DHCP Option60

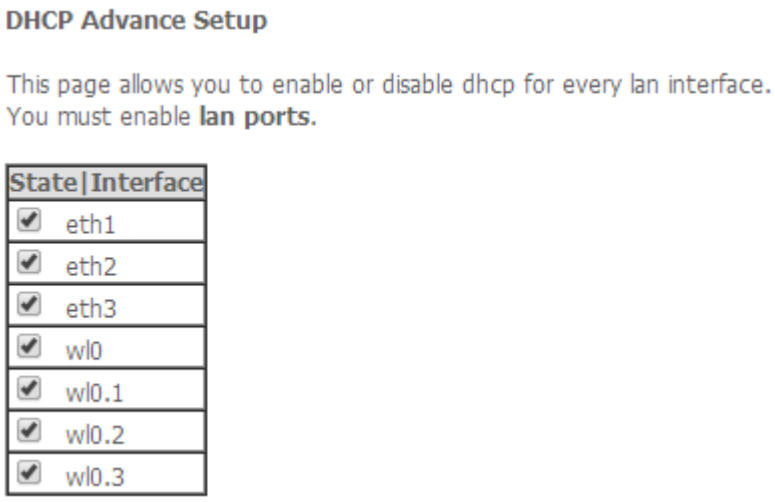
Click the **Edit DHCP Option60** button in the **Local Area Network (LAN) Setup** page to display the **DHCP Option60 Setup** page.



In this page, you can add, edit or delete the DHCP60 options.

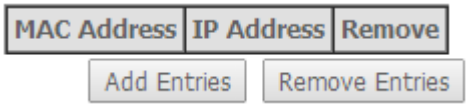
DHCP Advanced Setup

Click the **DHCP Advance Setup** button in the **Local Area Network (LAN) Setup** page to display the following page. In this page, you can enable or disable DHCP for every LAN interface.



Configuring the DHCP Static IP Lease List

The lease list of static IP address can reserve the static IP addresses for the hosts with the specific MAC addresses. When a host whose MAC address is in the lease list of static IP address requests the DHCP server for an IP address, the DHCP server assigns the reserved IP address to the host.

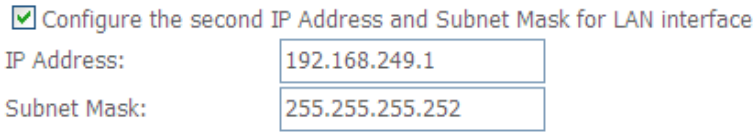


Click the **Add Entries** button in the **Local Area Network (LAN) Setup** page to display the **DHCP Static IP Lease** page.

In this page, enter the MAC address of the LAN host and the static IP address that is reserved for the host, and then click the **Apply/Save** button to apply the settings.

Configuring the Second IP Address and Subnet Mask for a LAN Interface

In the **Local Area Network (LAN) Setup** page, you may set the second IP address and the subnet mask for a LAN interface.



After enabling **Configure the second IP Address and Subnet Mask for LAN interface**, enter an IP address and a subnet mask for the LAN interface.

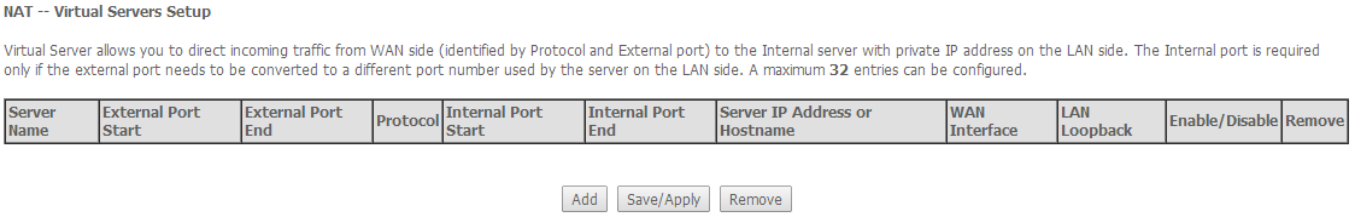
After setting, click the **Apply/Save** button to apply the settings.

5.3.4. NAT

5.3.4.1. Virtual Servers

Firewall can prevent unexpected traffic on the Internet from your host on the LAN. The virtual server can create a channel that can pass through the firewall. In that case, the host on the Internet can communicate with a host on your LAN within certain port range.

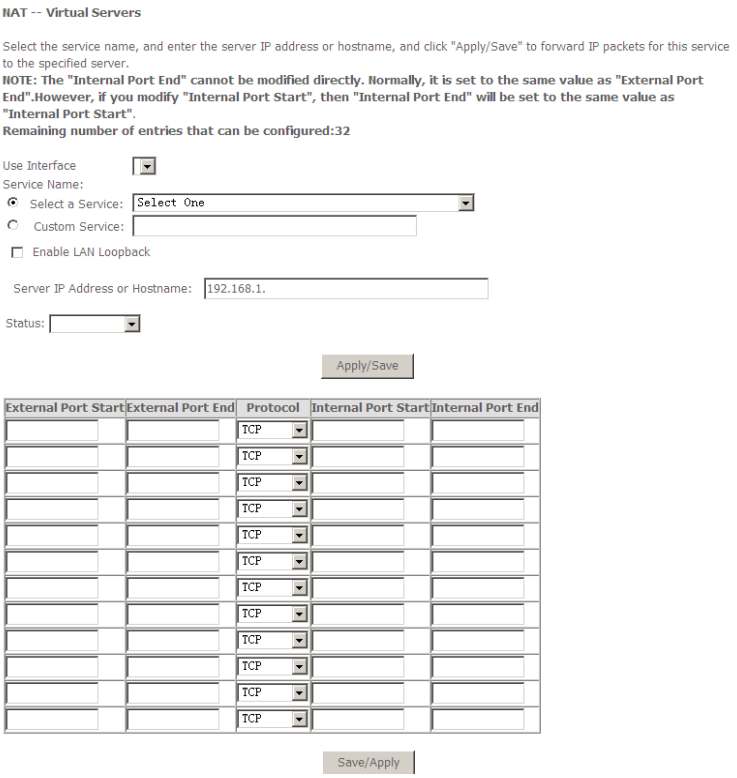
Choose **Advanced Setup > NAT > Virtual Servers**, and the following page appears.



In this page, you are allowed to add or remove a virtual server entry.

To add a virtual server, do as follows:

Step 1 Click the **Add** button to display the following page.



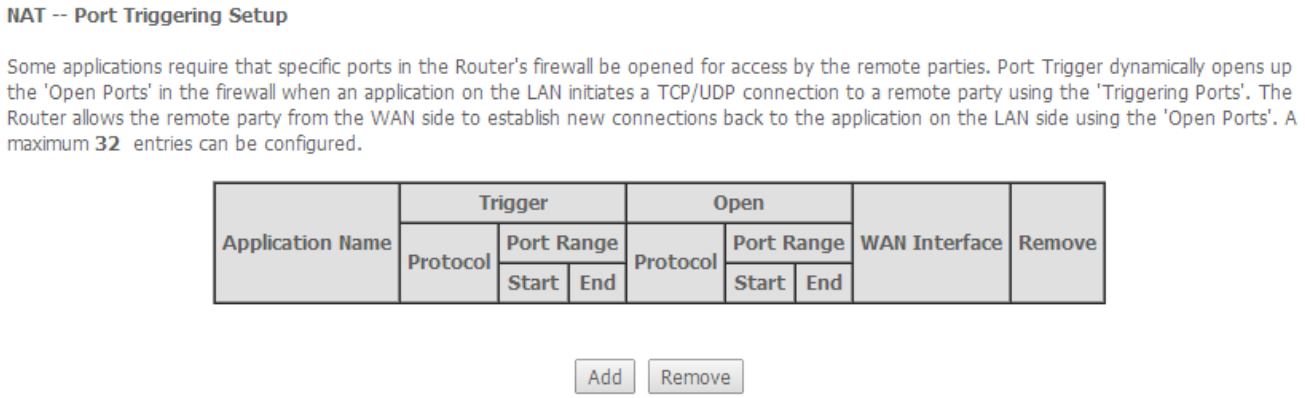
- **Use interface**: Select an interface that you want to configure.
- **Select a Service**: Select a proper service in the drop-down list.
- **Custom Server**: Enter a new service name to establish a user service type.
- **Server IP Address or Hostname**: Assign an IP address to virtual server.
- **External Port Start**: When selecting a service, the port number will automatically be displayed. You can modify it if necessary.
- **External Port End**: When selecting a service, the port number will automatically be displayed. You can modify it if necessary.
- **Protocol**: You may select TCP/UDP, TCP, or UDP in the drop-down list.
- **Internal Port Start**: When selecting a service, the port number will automatically be displayed. You can modify it if necessary.
- **Internal Port End**: When selecting a service, the port number will automatically be displayed. You can modify it if necessary.

Step 2 After setting, click **Save/Apply** to save and apply the settings.

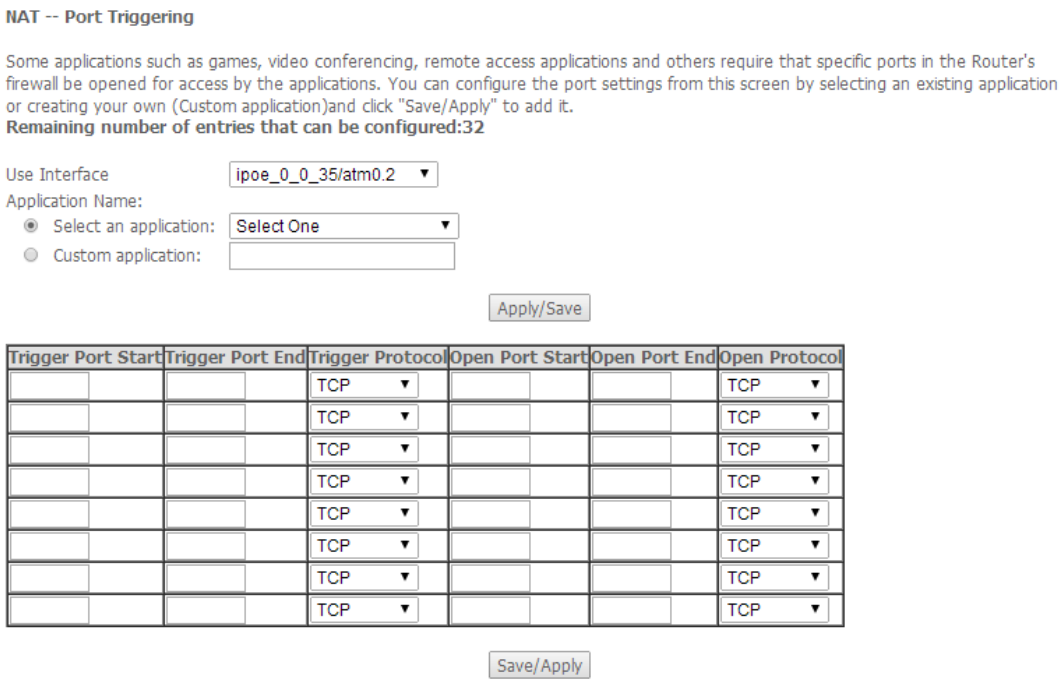
5.3.4.2. Port Triggering

Some applications need some ports to be opened in the firewall for the remote access. When an application initializes a TCP/UDP to connect to a remote user, port triggering dynamically opens the open ports of the firewall.

Choose **Advanced Settings > NAT > Port Triggering**, and the following page appears.



In this page, you may add or remove an entry of port triggering.
Click the **Add** button to display the following page.



- **Use interface**: Select an interface that you want to configure.
- **Select an application:** Select a proper application in the drop-down list.
- **Custom application:** Manually define an application.
- **Trigger port Start:** The start port number that LAN uses to trigger the open port.
- **Trigger port End:** The end port number that LAN uses to trigger the open port.
- **Trigger Protocol:** Select the application protocol. You may select TCP/UDP, TCP, or UDP.
- **Open Port Start:** The start port number that is opened to WAN.
- **Open Port End:** The end port number that is opened to WAN.
- **Open Protocol:** Select the proper protocol that is opened to WAN. You may select TCP/UDP, TCP, or UDP.

After setting, click **Save/Apply** to apply the settings.

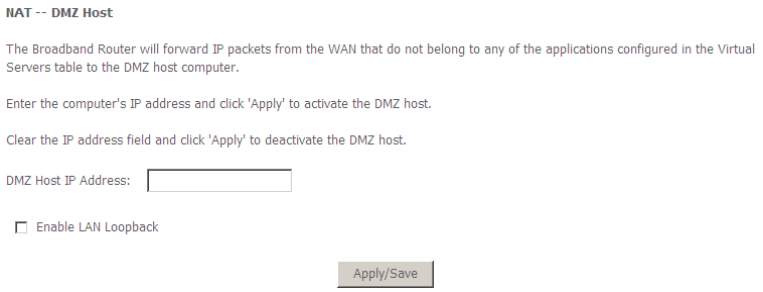
Note:

You can use a single port number, several port numbers separated by commas, port blocks consisting of two port numbers separated by a dash, or any combination of these, for example 80, 90-140, 180.

5.3.4.3. DMZ Host

DMZ allows all the ports of a PC on your LAN to be exposed to the Internet. Set the IP address of the PC to be DMZ host, so that the DMZ host will not be blocked by firewall.

Choose **Advanced Setup > NAT > DMZ host** to display the following page.



In this page, enter the IP address of the DMZ host.

After setting, click the **Apply/Save** button to apply the settings.

To clear the DMZ function of the host, delete the IP address of the host in the field of **DMZ Host IP Address**, and then click the **Apply/Save** button.

5.3.5. Security

By default, the firewall is enabled. The firewall is used to block the file transmission between the Internet and your PC. It serves as a safety guard and permits only the authorized files to be sent to the LAN.

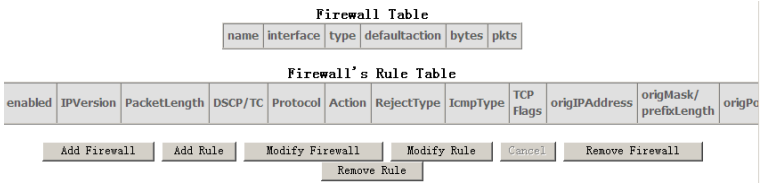
Note:

If the DSL router is configured as bridge mode, **Firewall** is disabled.

Firewall

When the Firewall is enabled on the DSL router, the security functions for the local network and the internet are enabled at the same time.

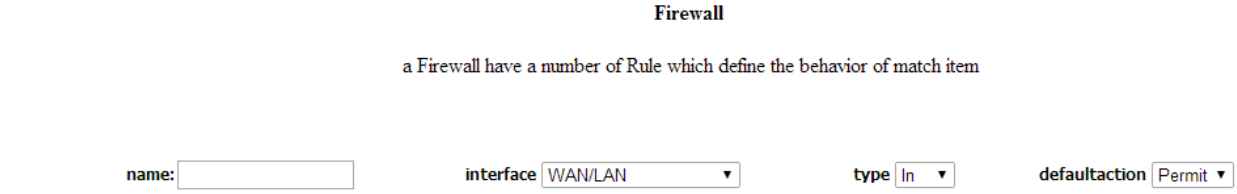
Choose **Security > Firewall** and the following page appears.



Click **Modify Firewall** or **Remove Firewall** to modify or remove the firewall.

Click **Modify Rule** or **Remove Rule** to modify or remove the rule.

Click **Add Firewall**, and the following page appears.



- **Name**: The name of the firewall.
- **Interface**: You can select **a proper interface** from the drop-down list.
- **Type**: select **In**, the firewall blocks or permits the IP packet transmisstion from the internet. Select **Out**, the firewall blocks or permits the IP packet transmission from LAN.
- **Defaultaction**: Select **Permit** to allow IP packet transmission at the direction specified in **type**. Select **Drop** to block the IP packet transmission at the direction specified in **type**.

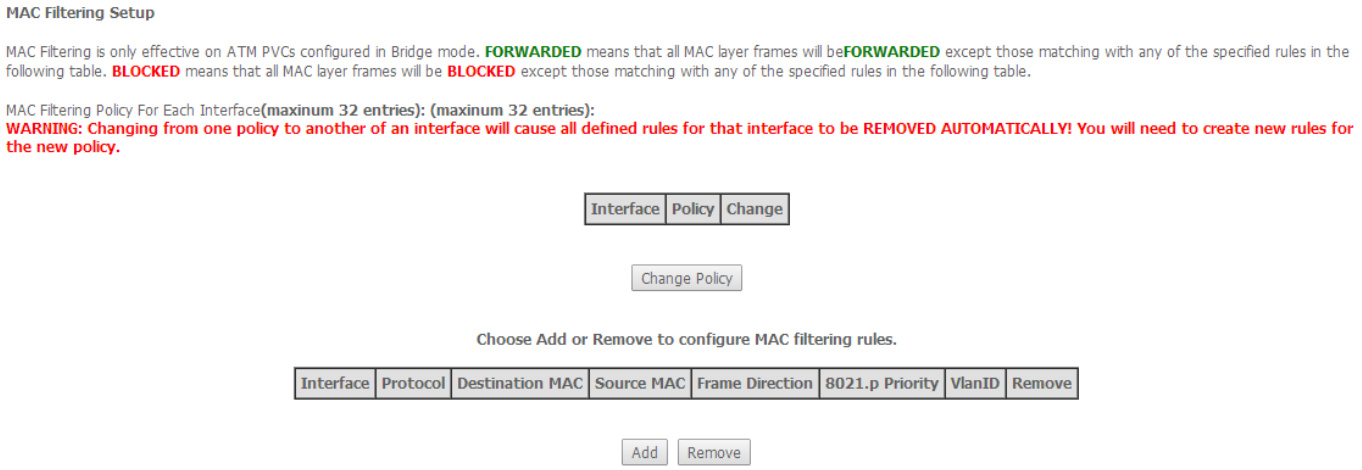
MAC Filtering

In some cases, you may want to manage Layer2 MAC address to block or permit a computer within the home network. When you enable MAC filter rules, the DSL router serves as a firewall that works at layer 2.

Note:

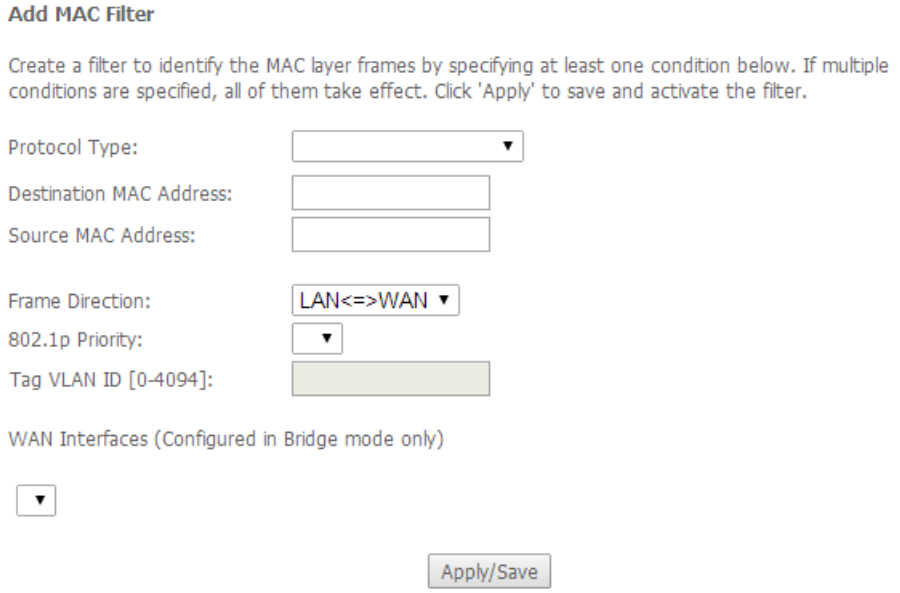
MAC filtering is only effective on ATM PVCs configured in **bridge mode**.

If the connection type is set to be **bridge** mode, Choose **Security** > **MAC Filtering** and the following page appears.



In this page, you can add or remove the MAC filtering rule. You may change the MAC filtering policy from **FORWARDED** to **BLOCKED** by clicking the **Change Policy** button.

Click the **Add** button to display the following page.



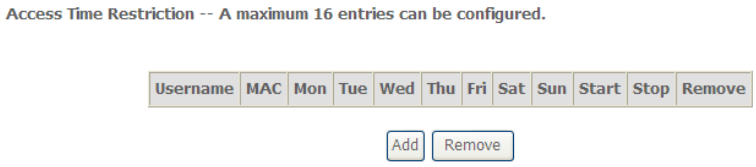
- **Protocol Type**: Select the proper protocol type.
- **Destination MAC Address**: Enter the destination MAC address.
- **Source MAC Address**: Enter the source MAC address.
- **Frame Direction**: The direction of transmission frame.
- **WAN Interface (Configured in bridge mode only)**: Select the proper WAN interface in the drop-down list.

After setting, click **Apply/Save** to save and apply the filtering rule.

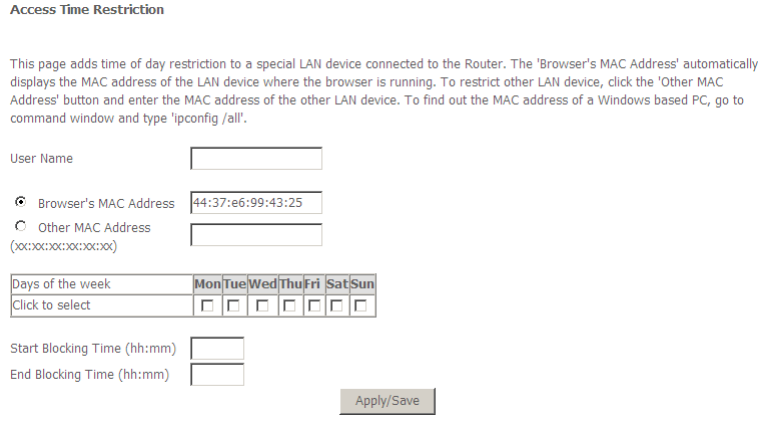
5.3.6. Parental Control

Time Restriction

Choose **Advanced Setup** > **Parental Control** > **Time Restriction**, and the following page appears.



Click the **Add** button to display the following page.

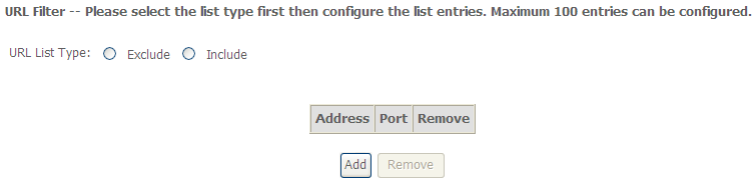


This page is used to control the time restriction to a special LAN device that connects to the DSL router. In this page, enter the user name and configure the time settings.

After setting, click the **Apply/Save** button to save and apply the settings.

Url Filter

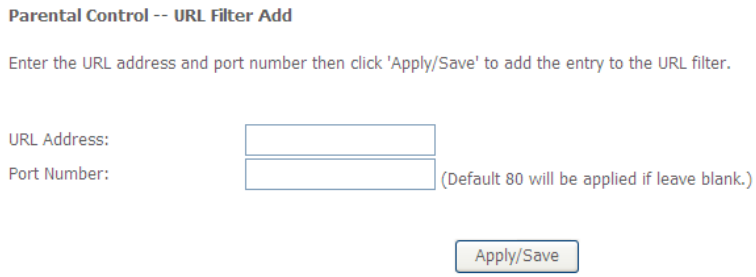
Click **Advanced Setup** > **Parental Contr**ol > **Url Filter**, and the following page appears.



Thisp age is used to prevent the LAN users from accessing some Websites in the WAN.

In this page, you may select the **Exclude** URL list type or the **Include** URL list type. If you select the **Exclude** URL list type, it means that the URLs in the list are not accessible. If you select the select the **Include** URL list type, you are allowed to access the URLs in the list.

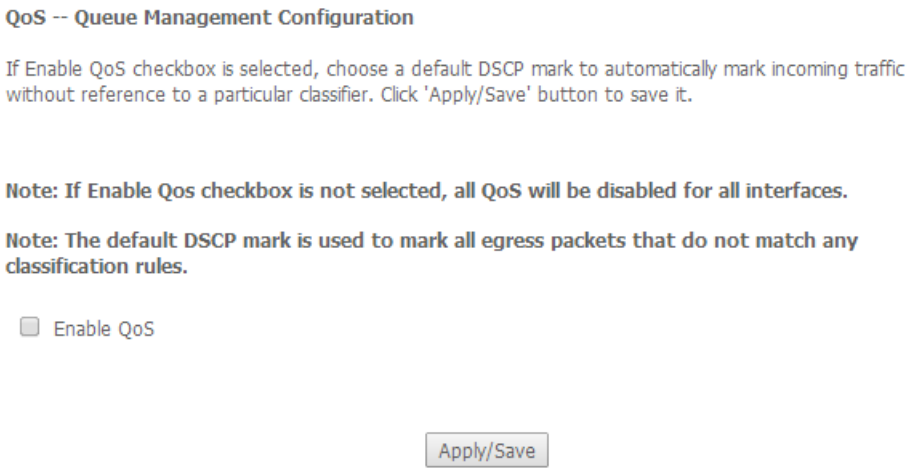
Click the **Add** button to display the following page.



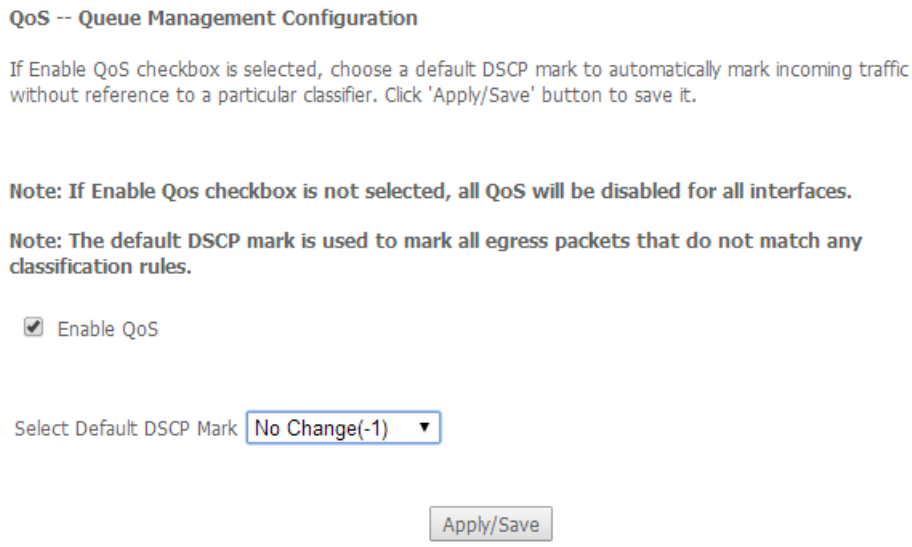
In this page, enter the URL address and its corresponding port number. For example, enter the URL address ***http://www.google.com*** and the port number **80**, and then click the **Apply/Save** button. See the following figure:

5.3.7. Quality of Service

Choose **Advance Setup > Quality of Service** and the following page appears.



Select **Enable QoS** to enable QoS and configure the default DSCP mark.



In this page, enable the QoS function and select the default DSCP mark.

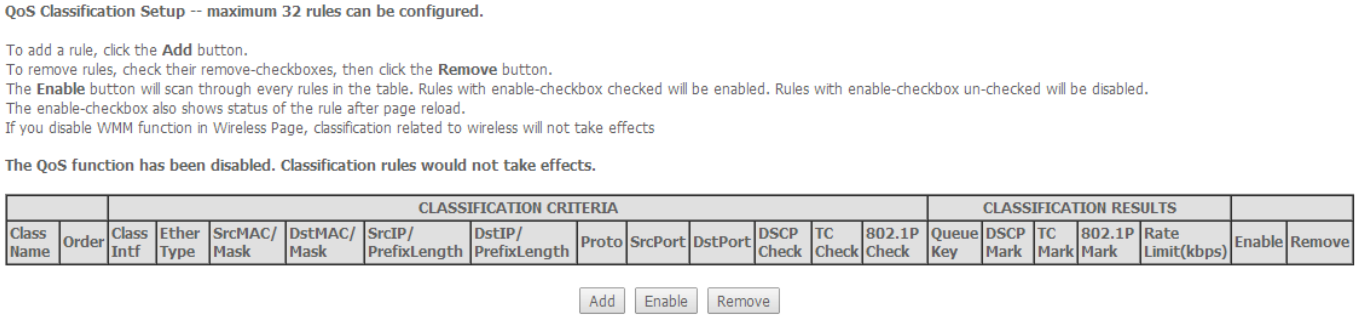
After setting, click **Apply/Save** to save and apply the settings.

Note:

If the **Enable QoS** checkbox is not selected, all QoS will be disabled for all interfaces. The default DSCP mark is used to mark all egress packets that do not match any classification rules.

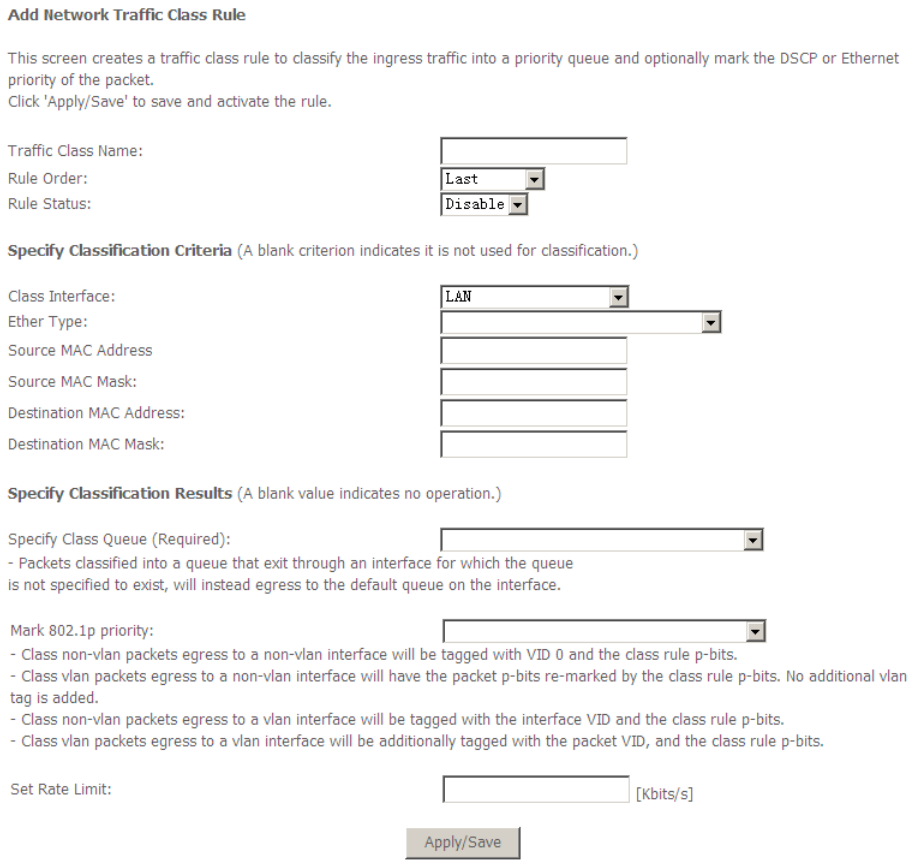
Queue Classification

Choose **Advanced Setup** > **Quality of Service** > **QoS Classification** and the following page appears.



In this page, you can enable, add or remove a QoS classification rule.

Click the **Add** button to display the following page.



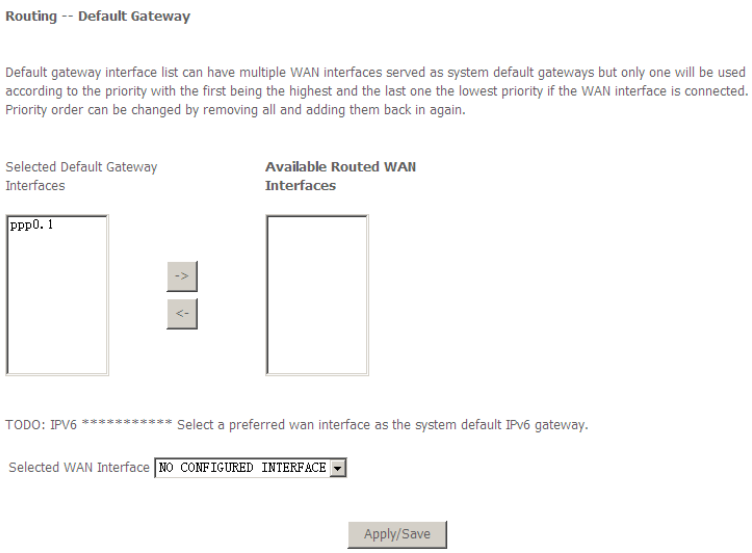
In this page, enter the traffic name, select the rule order and the rule status, and specify the classification criteria and the classification results.

After setting, click **Apply/Save** to save and apply the settings.

5.3.8. Routing

Default Gateway

Choose **Advanced Setup** > **Routing** > **Default Gateway**, and the following page appears.



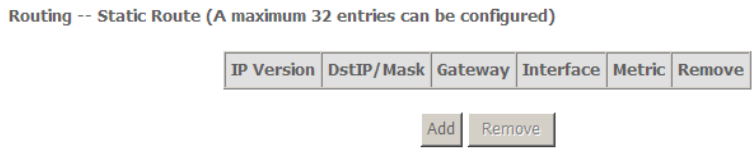
In this page, you can modify the default gateway settings.

Select a proper WAN interface and add it to the column of **Selected Default Gateway Interface** as the system default gateway.

After setting, click **Apply/Save** to save and apply the settings.

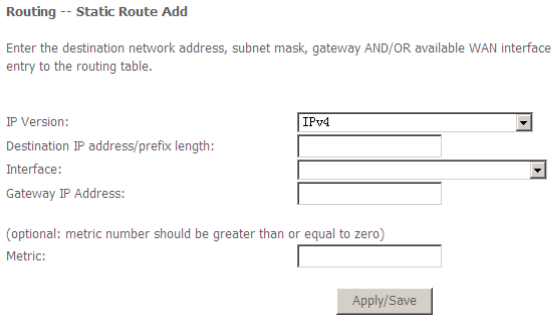
Static Route

Choose **Advanced Setup** > **Routing** > **Static Route** and the following page appears.



In this page, you can add or remove a static routing rule.

Click the **Add** button to display the following page.

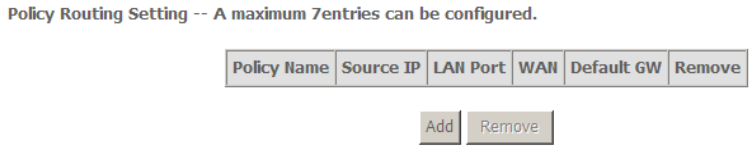


- **IP Version:** Select the IP version to be IPv4.
- **Destination IP address/prefix length:** Enter the destination IP address.
- **Interface:** Select the proper interface for the rule.
- **Gateway IP Address:** The next-hop IP address.
- **Metric:** The metric value of routing.

After setting, click **Apply/Save** to save and apply the settings.

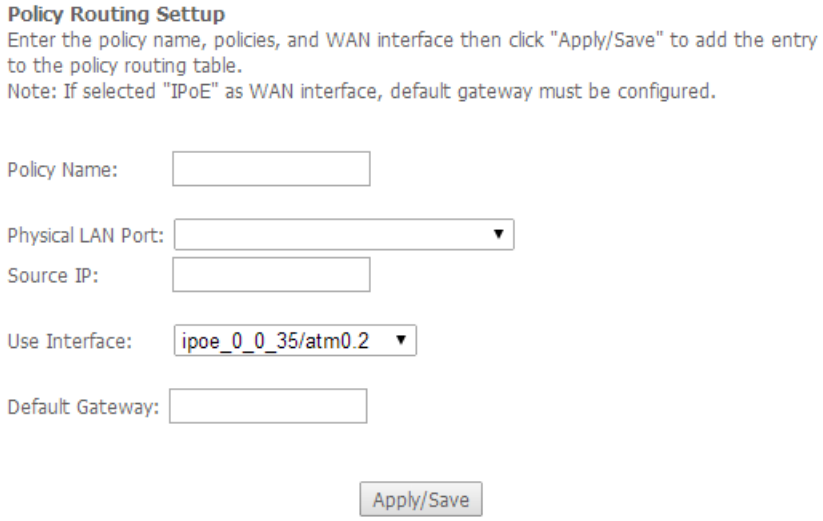
Policy Routing

Choose **Advanced Setup** > **Routing** > **Policy Routing** and the following page appears.



In this page, you can add or remove a static policy rule.

Click the **Add** button to display the following page.

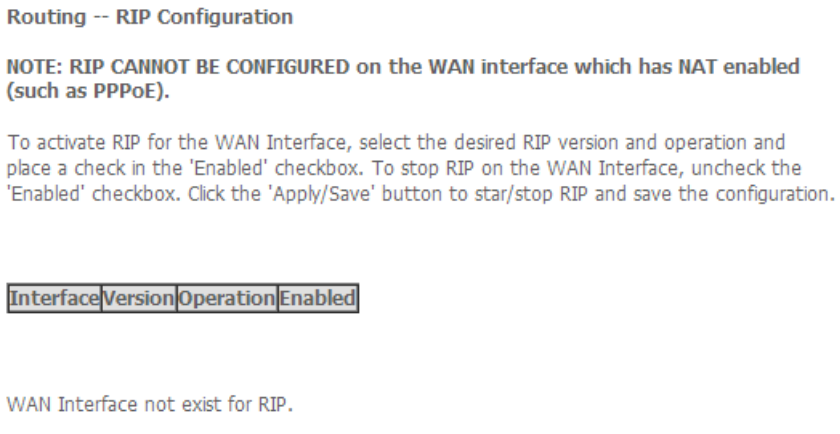


In this page, enter the policy name, source IP and default gateway, and select the physical LAN port and interface.

After setting, click **Apply/Save** to save and apply the settings.

RIP

Choose **Advanced Setup > Routing > RIP** and the following page appears.



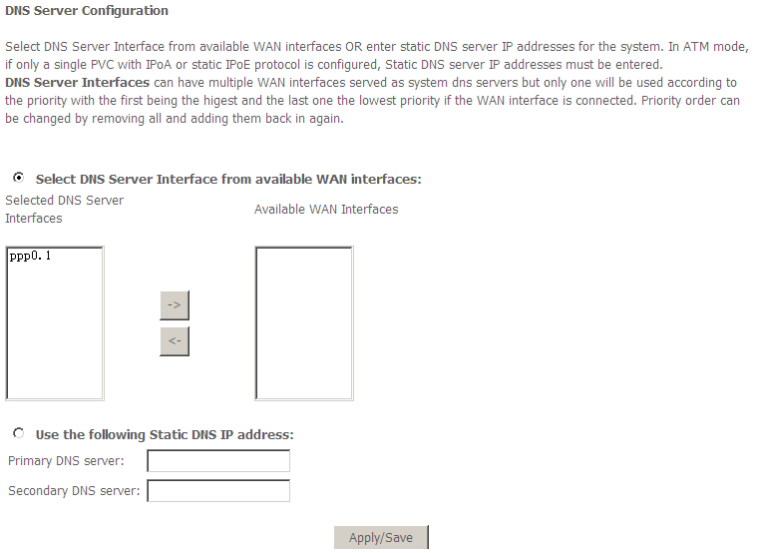
In this page, to configure an individual interface, select the desired RIP version and operation, and then select the **Enabled** checkbox for the interface.

After setting, click **Apply/Save** to save and apply the settings.

5.3.9. DNS

DNS Server

Choose **Advanced Setup > DNS > DNS Server** and the following page appears.

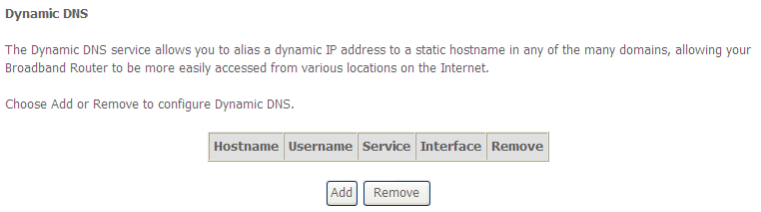


In this page, you can select a DNS server interface from the available interfaces, manually enter the DNS server addresses, or obtain the DNS address from a WAN interface.

After setting, click **Apply/Save** to save and apply the settings.

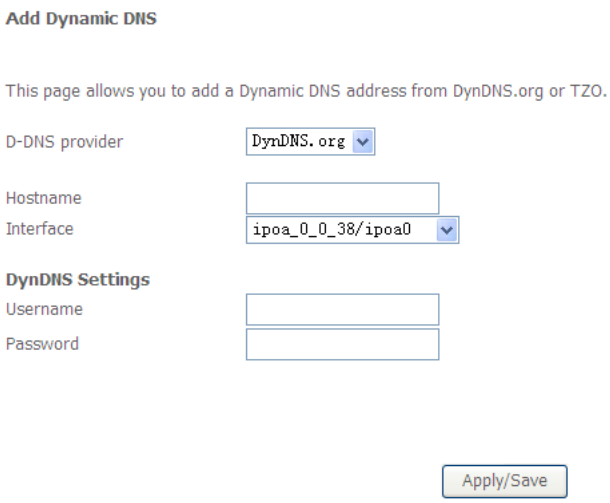
Dynamic DNS

Choose **Advanced Setup > DNS > Dynamic DNS** and the following page appears.



In this page, you are allowed to modify the DDNS settings.

Click the **Add** button to display the following page.

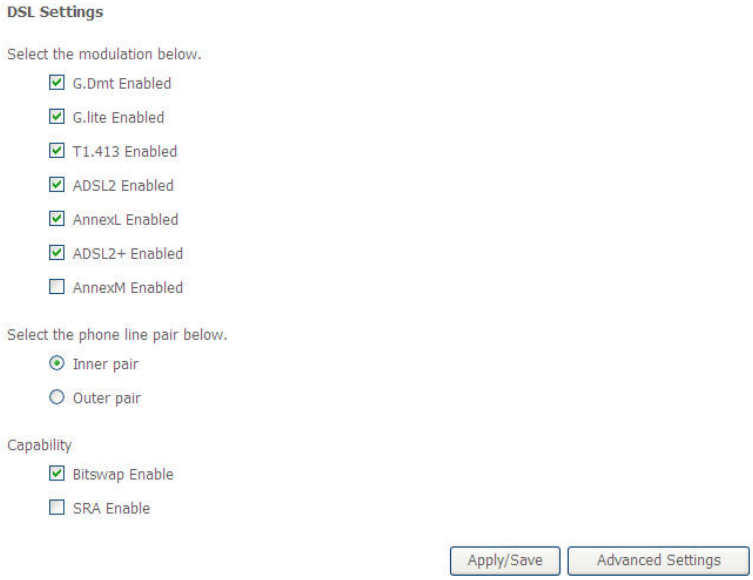


- **D-DNS provider:** Select a proper DDNS server in the drop-down list.
- **Hostname:** It is the domain name and it can be modified.
- **Interface:** The interface that the packets pass through on the DSL router.
- **Username:** Enter the username for accessing the DDNS management interface.
- **Password:** Enter the password for accessing the DDNS management interface.

After setting, click **Apply/Save** to save and apply the settings.

5.3.10. DSL

Choose **Advanced Setup** > **DSL** and the following page appears. In this page, you can view the DSL settings. Usually, you can keep this factory default setting. The modem negotiates the modulation mode with the DSLAM.

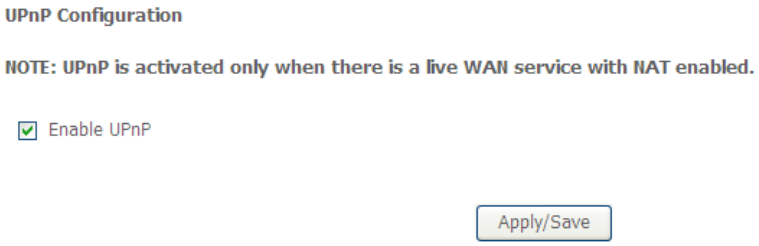


In this page, you can set the DSL settings. Usually, you do not need to modify the factory default settings.

After setting, click **Apply/Save** to save and apply the settings.

5.3.11. UPnP

Choose **Advanced Setup > UPnP** and the following page appears.

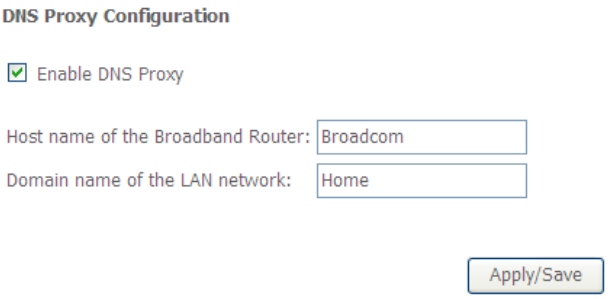


In this page, you can enable or disable the UPnP function.

After setting, click **Apply/Save** to save and apply the settings.

5.3.12. DNS Proxy

Choose **Advanced Setup > DNS Proxy** and the following page appears.

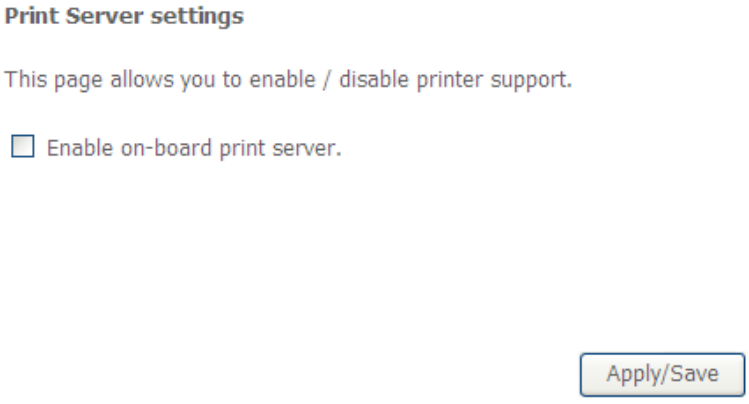


In this page, you can enable or disable the DNS proxy function.

After enabling the DNS proxy function, enter the host name of the broadband router and the domain name of the LAN network, and then click **Apply/Save** to save and apply the settings.

5.3.13. Print Server

Choose **Advanced Setup > Printer Server** and the following page appears.

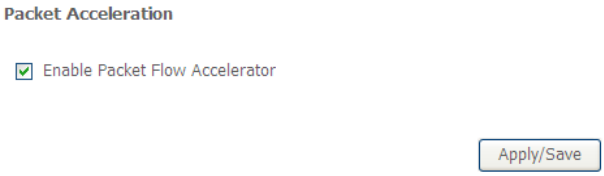


In this page, you can enable or disable the printer server.

After setting, click **Apply/Save** to save and apply the settings.

5.3.14. Packet Acceleration

Choose **Advanced Setup > Packet Acceleration** and the following page appears. In this page, you can enable packet flow accelerator.



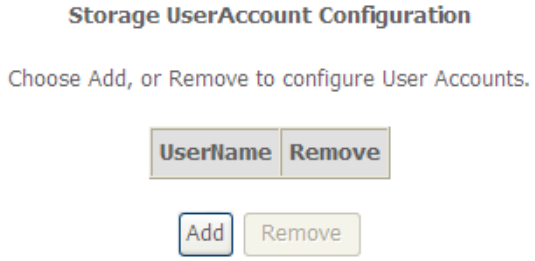
5.3.15. Storage Service

Storage Device Info

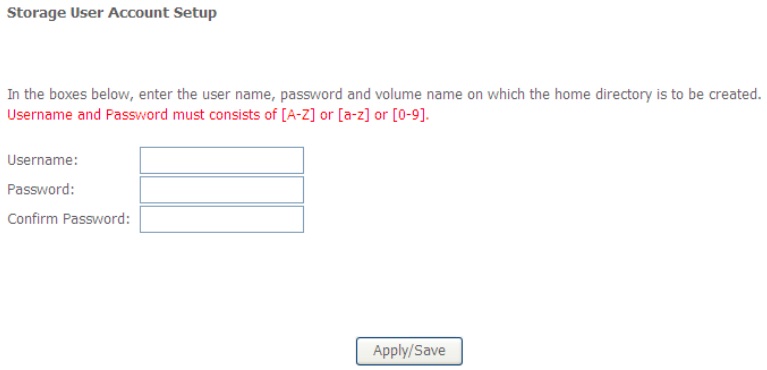
Choose **Advanced Setup > Storage Service > Storage Device Info**, and the following page appears. In this page, you can view the USB device info.

User Accounts

Choose **Advanced Setup > Storage Service > User Accounts**, and the following page appears. In this page, you may add or remove storage user accounts.



Click the **Add** button to display the following page.

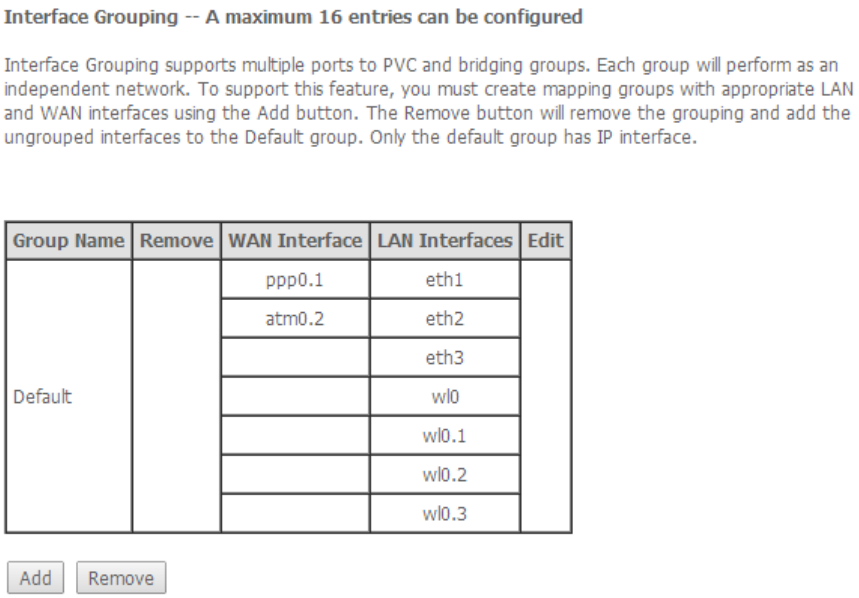


Enter the user name, password and volume name, and then click **Apply/Save** to finish setting up an account.

To delete an account, select it in the **Storage UserAccount Configuration** page, and then click **Remove**.

5.3.16. Interface Grouping

Choose **Advanced Setup > Interface Grouping** and the following page appears.



Interface Grouping -- A maximum 16 entries can be configured

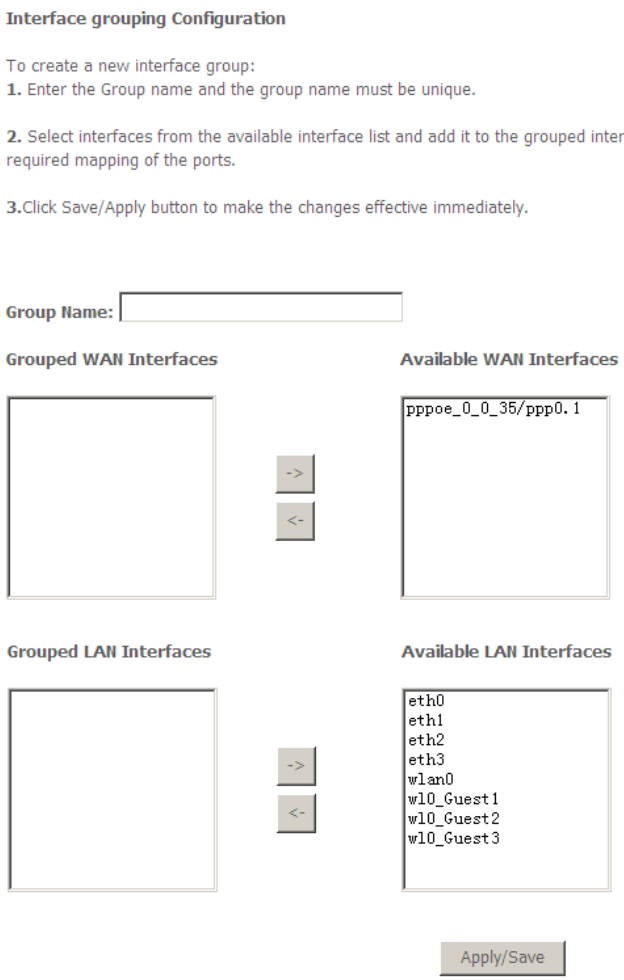
Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Group Name	Remove	WAN Interface	LAN Interfaces	Edit
Default		ppp0.1	eth1	
		atm0.2	eth2	
			eth3	
			wl0	
			wl0.1	
			wl0.2	
			wl0.3	

Add Remove

Interface grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with the appropriate LAN and WAN interfaces using the **Add** button. The **Remove** button will remove the grouping and add the ungrouped interfaces to the default group. Only the default group has IP interface.

Click the **Add** button to display the following page.



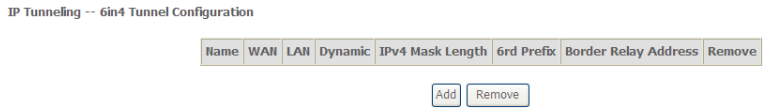
In this page, please follow the on-screen configuration steps to configure the parameters of the interface grouping.

After setting, click **Apply/Save** to save and apply the settings.

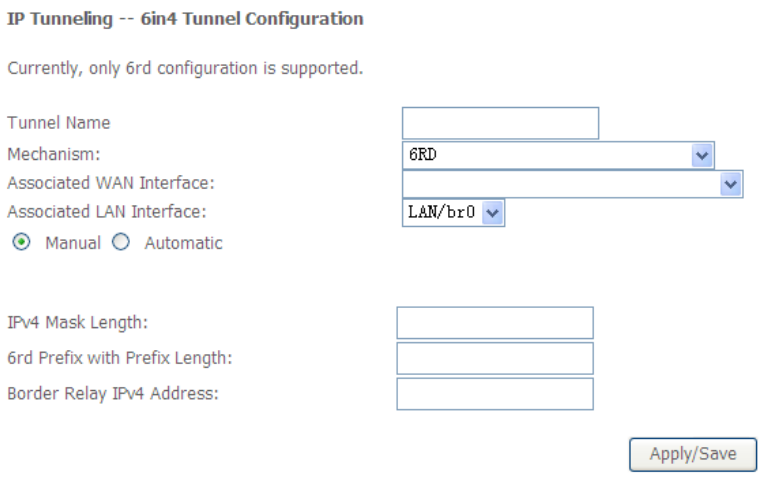
5.3.17. IP Tunnel

IPv6inIPv4

Choose **Advanced Setup > IP Tunnel > IPv6inIPv4**, and the following page appears.



Click the **Add** button, and the following page appears.

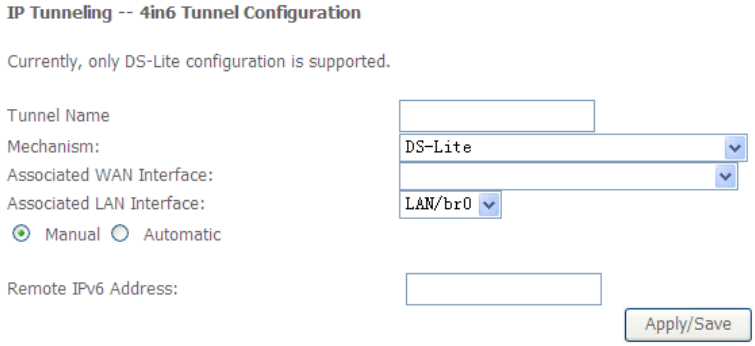


Click **Apply/Save** to save and enable the settings.

IPv4inIPv6

Choose **Advanced Setup > IP Tunnel > IPv4inIPv6**, and the following page appears.

Click the **Add** button, and the following page appears.

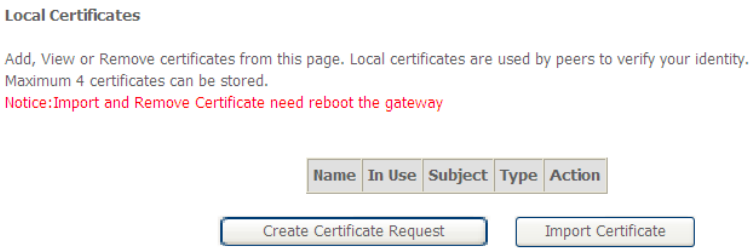


Click **Apply/Save** to save and enable the settings.

5.3.18. Certificate

Local

Choose **Advanced Setup > Certificate > local** and the following page appears.



In this page, you can acquire the local certificate by creating a certificate request or importing a certificate. You may also create or remove a certificate.

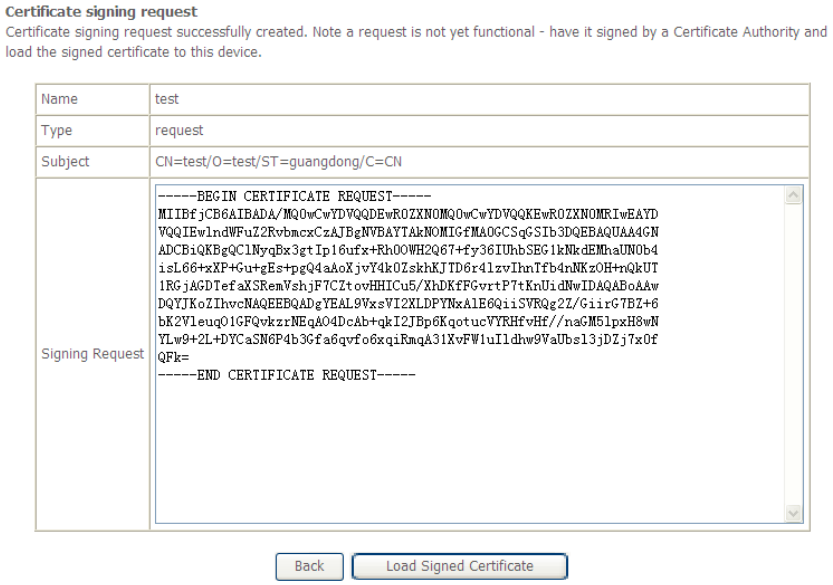
- **Creating a New Certificate Request**

Click the **Create Certificate Request** button to display the following page.

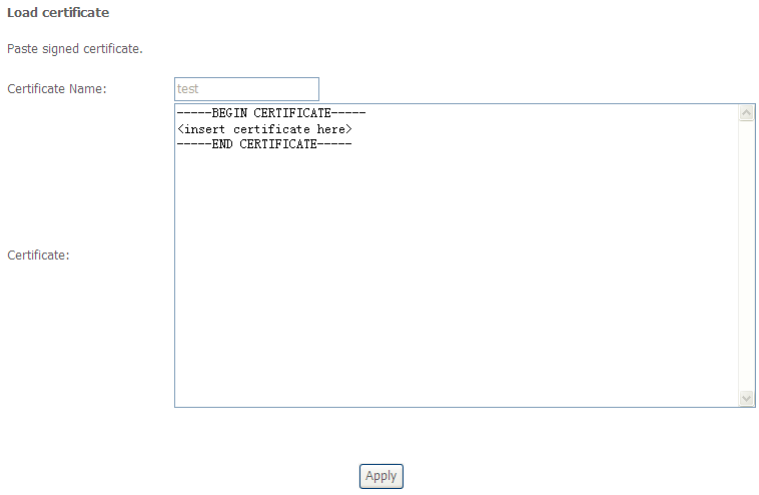
In this page, please set the following parameters.

- **Certificate name:** Set the certificate name.
- **Common Name:** The common name is the "fully qualified domain name," (or FQDN) used for DNS lookups of your server (for example, www.mydomain.com). Browsers use this information to identify your Web site. Some browsers will refuse to establish a secure connection with your site if the server name does not match the common name in the certificate. Please do not include the protocol symbol "http://" or any port numbers or pathnames in the common name. Do not use wildcard characters such as * or ?, and do not use an IP address.
- **Organization Name:** The name of the organization to which the entity belongs (such as the name of a company).
- **State/Province Name:** This is the name of the state or province where your organization's head office is located. Please enter the full name of the state or province.
- **Country/Region Name:** This is the two-letter ISO abbreviation for your country (for example, GB for the United Kingdom).

After setting, click the **Apply** button to apply the settings.



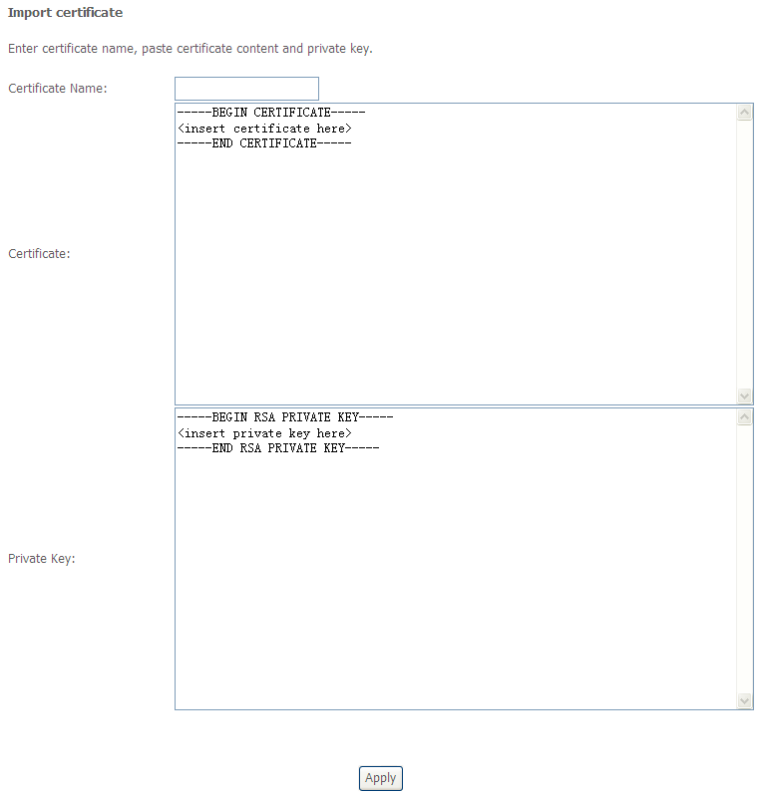
The certificate request needs to be submitted to a certificate authority, which will sign the request. Then the signed certificate needs to be loaded to the DSL router. Click **Load Signed Certificate** in this page, and the following page appears.



In this page, paste the signed certificate, and then click the **Apply** button. A new certificate is created.

- **Importing an Existing Local Certificate**

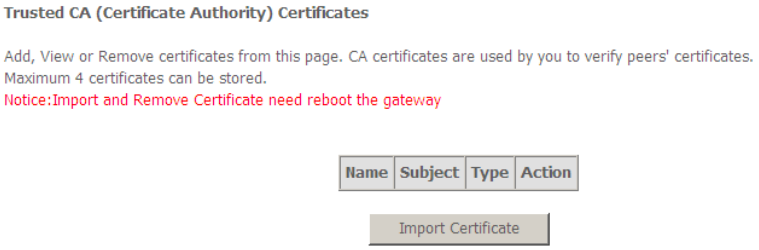
To import an existing certificate, click the **Import Certificate** button to display the following page.



In this page, paste the certificate and the private key. Finally, click the **Apply** button to import the certificate.

Trusted CA

Choose **Advanced Setup > Certificate > Trusted CA** and the following page appears.



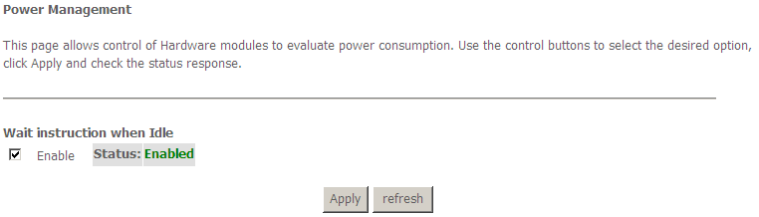
In this page, you may import or remove a CA certificate.

Click the **Import Certificate** button to display the following page.

In this page, enter the certificate name and paste the certificate content. Finally, click the **Apply** button to import the certificate.

5.3.19. Power Management

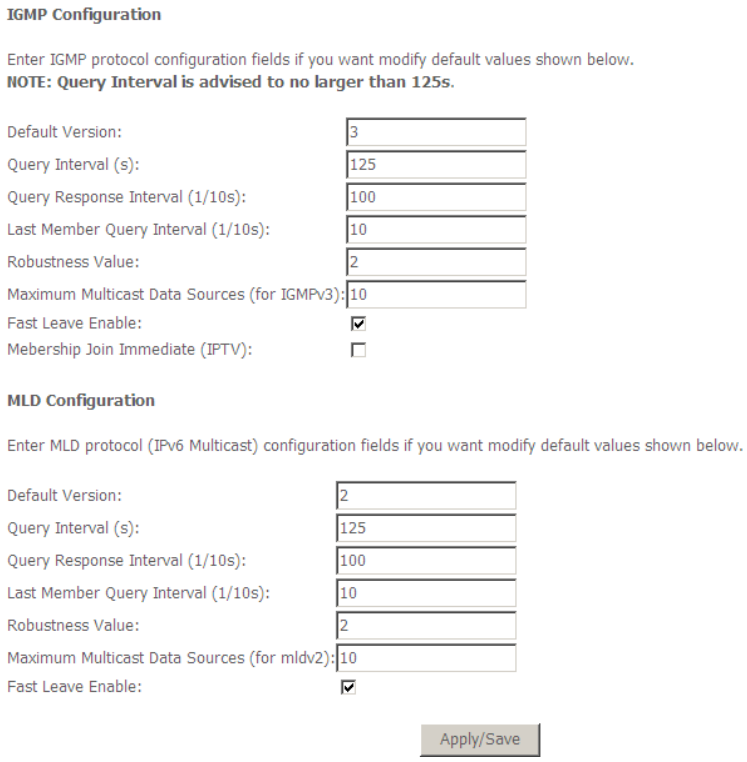
Choose **Advanced Setup** > **Power Management** and the following page appears. This page allows control of Hardware modules to evaluate power consumption. Use the control buttons to select the desired option.



After proper configurations, click **Apply** to take the configurations effect.

5.3.20. Multicast

Choose **Advanced Setup > Multicast** and the following page appears.

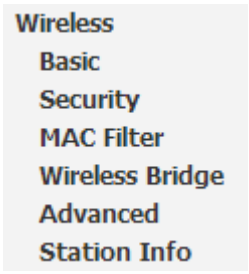


In this page, you can configure the multicast parameters.

After setting, click **Apply/Save** to save and apply the settings.

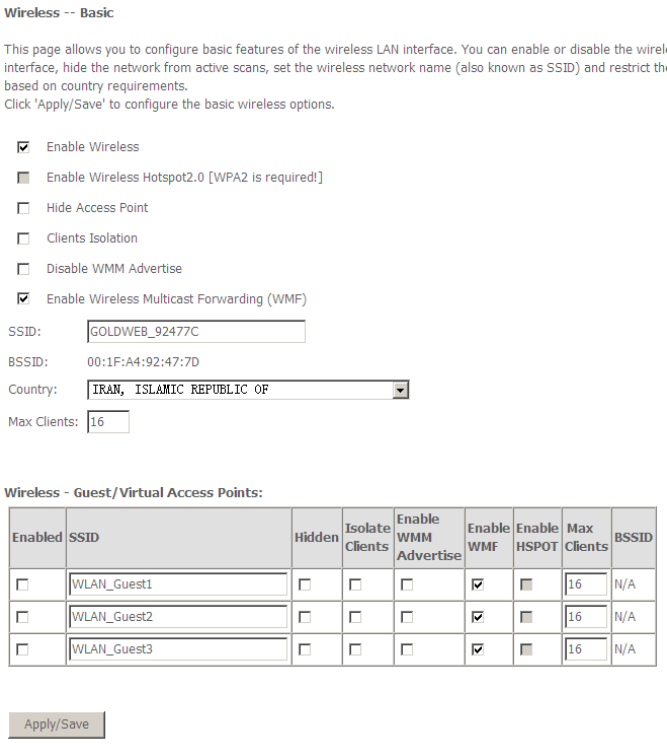
5.4. Wireless

Choose **Wireless** and the submenus of **Wireless** are shown as below:



5.4.1. Basic

Choose **Wireless** > **Basic** to display the following page.



This page allows you to configure the basic features of the wireless LAN interface.

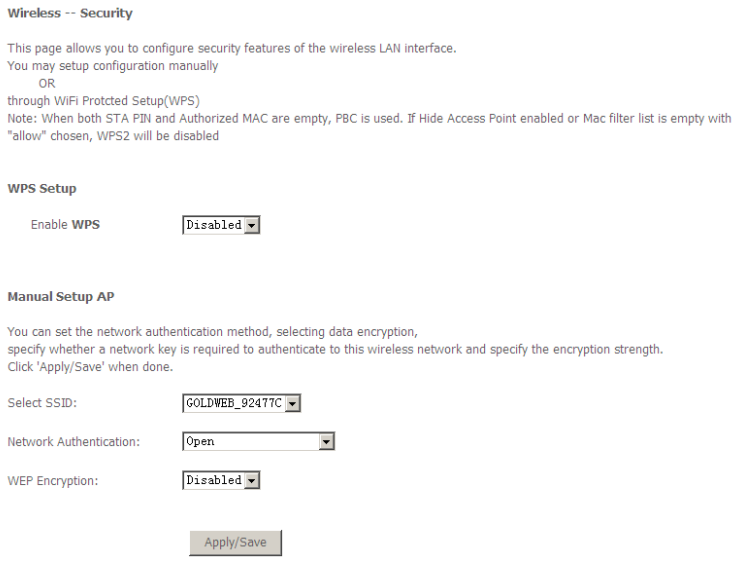
- **Enable Wireless:** Enable or disable the wireless function.
- **Hide Access Point:** if you want to hide any access point for your router, select this option, and then a station cannot obtain the SSID through the passive scanning.
- **Clients Isolation:** When many clients connect to the same access point, they can access each other. If you want to disable the access between the clients that connect to the same access point, you can select this option.
- **Disable WMM Advertise:** After enabling this option, the transmission performance multimedia of the voice and video data can be improved.
- **Enable Wireless Multicast Forwarding (WMF):** After enabling this option, the transmission quality of video service such as IPTV can be improved.
- **SSID**: For the security reason, you should change the default SSID to a unique name.
- **BSSID:** Display the MAC address of the wireless interface.
- **Country**: The name of the country with which your gateway is configured. This parameter further specifies your wireless connection. For example, the channel will adjust according to nations to adapt to each nation's frequency provision.

- **Max Clients:** Specify the maximum wireless client stations to be enabled to link with AP. Once the clients exceed the max vlaue, all other clients are refused. The value of maximum clients is 16.
- **Wireless - Guest/Virtual Access Points:** If you want to make Guest/Virtual network function be available, you have to check those boxes in the table below. In the current software version, three virtual access points can be configured.

After setting, click **Apply/Save** to save the basic wireless settings and make the settings take effect.

5.4.2. Security

Choose **Wireless > Security** to display the following page.



This page allows you to configure the security features of the wireless LAN interface. In this page, you can configure the network security settings by the Wi-Fi Protected Setup (WPS) method or setting the network authentication mode.

- **WPS Setup**

There are 2 primary methods used in the Wi-Fi Protected Setup:

PIN entry, a mandatory method of setup for all WPS certified devices.

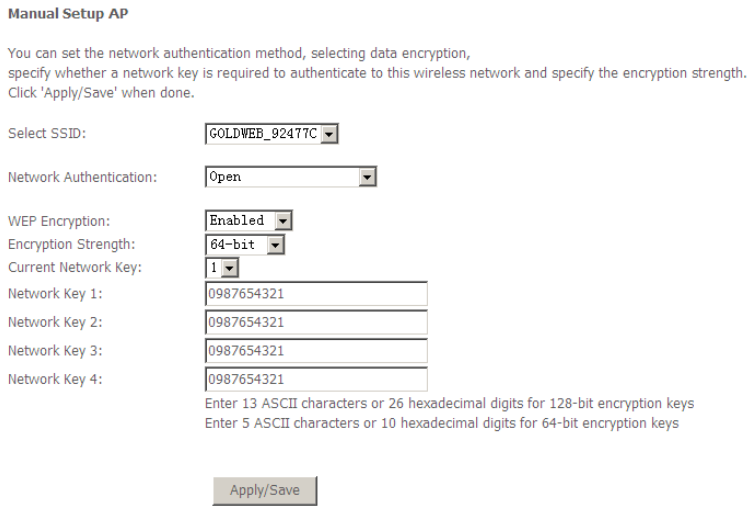
Push button configuration (PBC), an actual push button on the hardware or through a simulated push button in the software. (This is an optional method on wireless client).

If you are using the PIN method, you will need a Registrar (access point/wireless router) to initiate the registration between a new device and an active access point/wireless router. (**Note:** *The PBC method may also need a Registrar when used in a special case where the PIN is all zeros*)

In order to use the push-button for WPS authentication, you must ensure that the network card support the function. if it supports, you need not to do any configuration. You can press the WPS button directly to enable the WPS function.

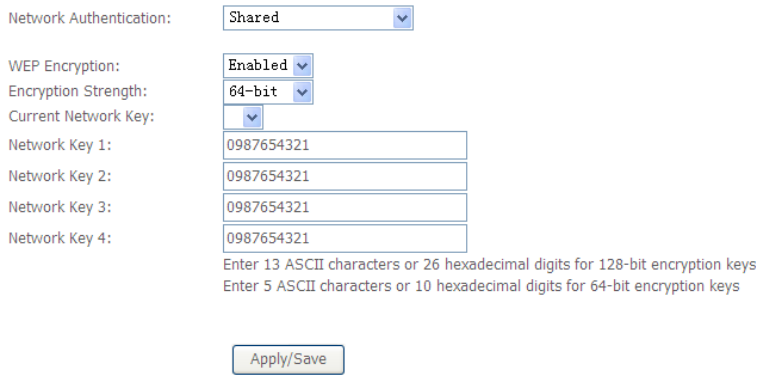
- **Manual Setup AP**

- Open Mode



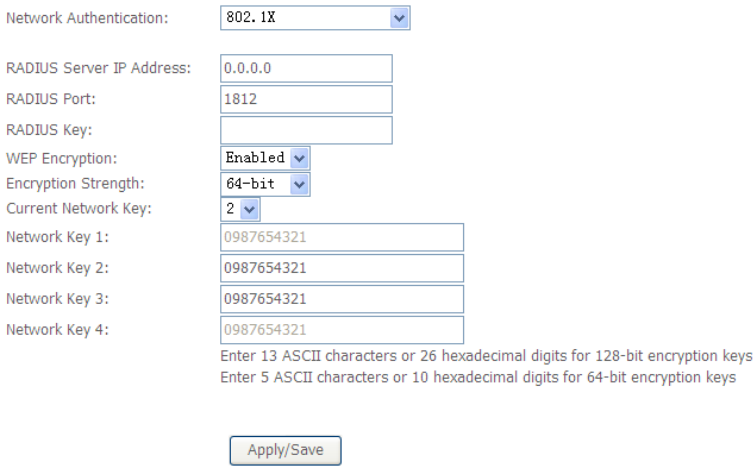
- **Select SSID:** Select a SSID for configuring the security settings.
- **Network Authentication:** Select the Open mode.
- **WEP Encryption:** Enable or disable WEP encryption. After enabling this function, you can set the encryption strength, current network key, and network keys.
- **Encryption Strength:** You can set 64-bit or 128-bit key.
- **Current Network Key:** The current key that you use.
- **Network Key1/2/3/4:** Set the network key. If it is 128-bit key, you need to enter 13 ASCII characters or 26 hexadecimal digits. For the 64-bit key, you need to enter 5 ASCII characters or 10 hexadecimal digits.

- Shared Mode



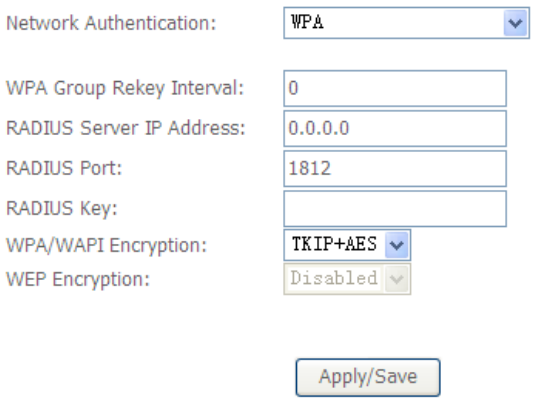
For the parameter description of shared mode, refer to the **Open Mode**.

- 802.1x



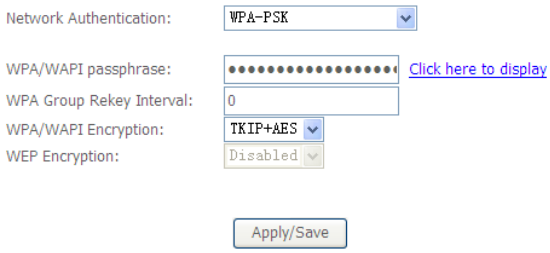
- **Select SSID:** Select a SSID for configuring the security settings.
- **Network Authentication:** Select the 802.1X in the drop-down list.
- **RADIUS Server IP Address:** Enter the IP address of the RADIUS server. RADIUS server is used to authenticate the hosts on the wireless network.
- **RADIUS Port:** The port number that the RADIUS server uses. The default port number is 1812. You may change it according to the server setting.
- **RADIUS Key:** Set the RADIUS key for accessing the RADIUS server.
- **WEP Encryption:** You can only select **Enabled**.
- **Encryption Strength:** You can set 64-bit or 128-bit key.
- **Current Network Key:** The current key that you use.
- **Network Key1/2/3/4:** Set the network key. If it is 128-bit key, you need to enter 13 ASCII characters or 26 hexadecimal digits. For the 64-bit key, you need to enter 5 ASCII characters or 10 hexadecimal digits.

- WPA Mode



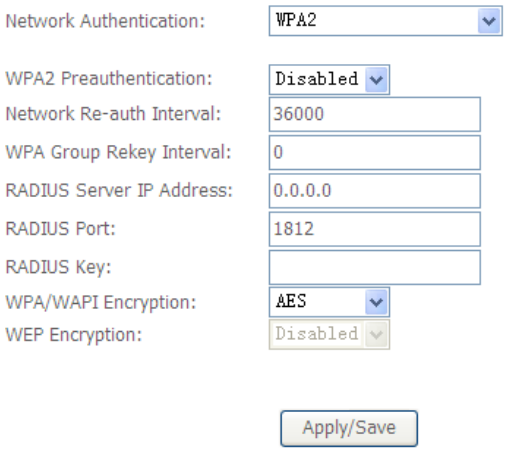
- **Select SSID:** Select a SSID for configuring the security settings.
- **Network Authentication:** Select the WPA-PSK mode.
- **WPA Group Rekey Interval:** Setting the interval for renewing key.
- **RADIUS Server IP Address:** Enter the IP address of the RADIUS server. RADIUS server is used to authenticate the hosts on the wireless network.
- **RADIUS Port:** The port number that the RADIUS server uses. The default port number is 1812. You may change it according to the server setting.
- **RADIUS Key:** Set the RADIUS key for accessing the RADIUS server.
- **WPA/WAPI Encryption:** You may select AES, or TKIP+AES.

- WPA-PSK Mode



- **Select SSID:** Select a SSID for configuring the security settings.
- **Network Authentication:** Select the WPA-PSK mode.
- **WPA/WAPI passphrase:** The key for WPA encryption. Click the **Click here to display** button to display the current key. The default key is 87654321.
- **WPA Group Rekey Interval:** Setting the interval for renewing key.
- **WPA/WAPI Encryption:** You may select AES, or TKIP+AES.

- WPA2 Mode

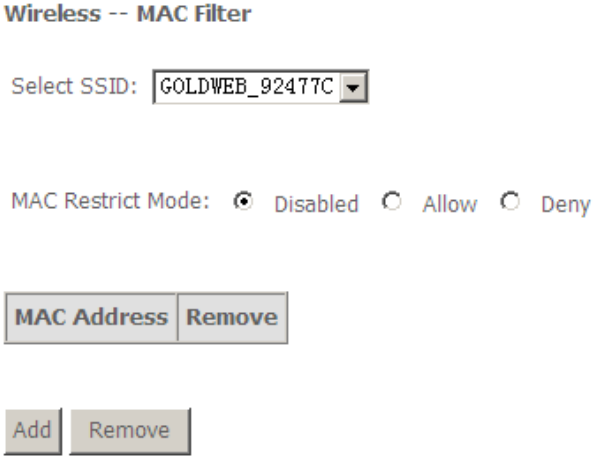


- **Select SSID:** Select a SSID for configuring the security settings.
- **Network Authentication:** Select the WPA2 mode.
- **WPA2 Preauthentication:** Enable or disable pre-authentication.
- **Network Re-auth Interval:** Set the network re-auth interval.
- **WPA Group Rekey Interval:** Setting the interval for renewing key.
- **RADIUS Server IP Address:** Enter the IP address of the RADIUS server. RADIUS server is used to authenticate the hosts on the wireless network.
- **RADIUS Port:** The port number that the RADIUS server uses. The default port number is 1812. You may change it according to the server setting.
- **RADIUS Key:** Set the RADIUS key for accessing the RADIUS server.
- **WPA/WAPI Encryption:** You may select AES, or TKIP+AES.

For the parameters' description of **WPA2-PSK**, **Mixed WPA2/WPA**, **Mixed WPA2/WPA-PSK** mode, please refer to the **WPA-PSK mode**.

5.4.3. MAC Filter

Choose **Wireless > MAC Filter** to display the following page.



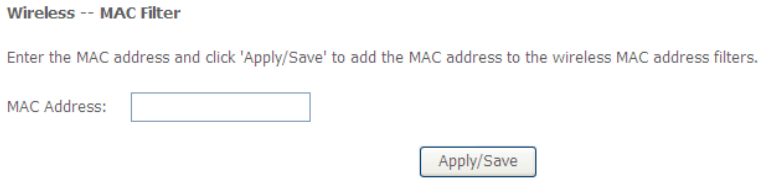
This page is used to allow or reject the wireless clients to access the wireless network of the wireless router.

In this page, you can add or remove the MAC filters.

The MAC restrict modes include **Disabled**, **Allow**, and **Deny**.

- **Disabled**: Disable the wireless MAC address filtering function.
- **Allow**: Allow the wireless clients with the MAC addresses in the **MAC Address** list to access the wireless network of the wireless router.
- **Deny**: Reject the wireless clients with the MAC addresses in the **MAC Address** list to access the wireless network of the wireless router.

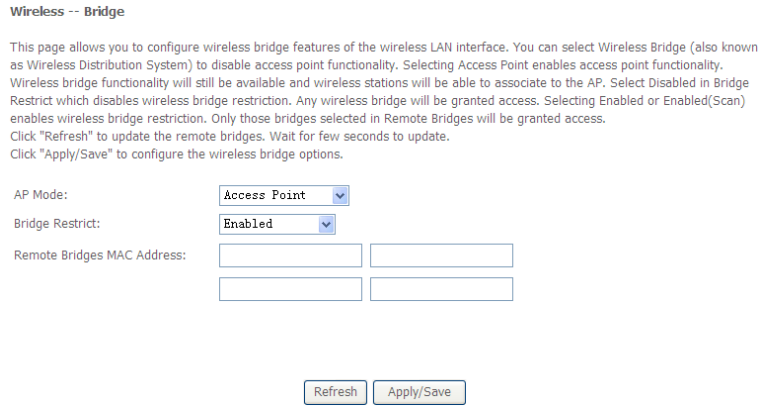
Click the **Add** button to display the following page.



In this page, enter the MAC address of the wireless client, and then click the **Apply/Save** button to add the MAC address to the MAC address list.

5.4.4. Wireless Bridge

Choose **Wireless > Wireless Bridge** to display the following page.



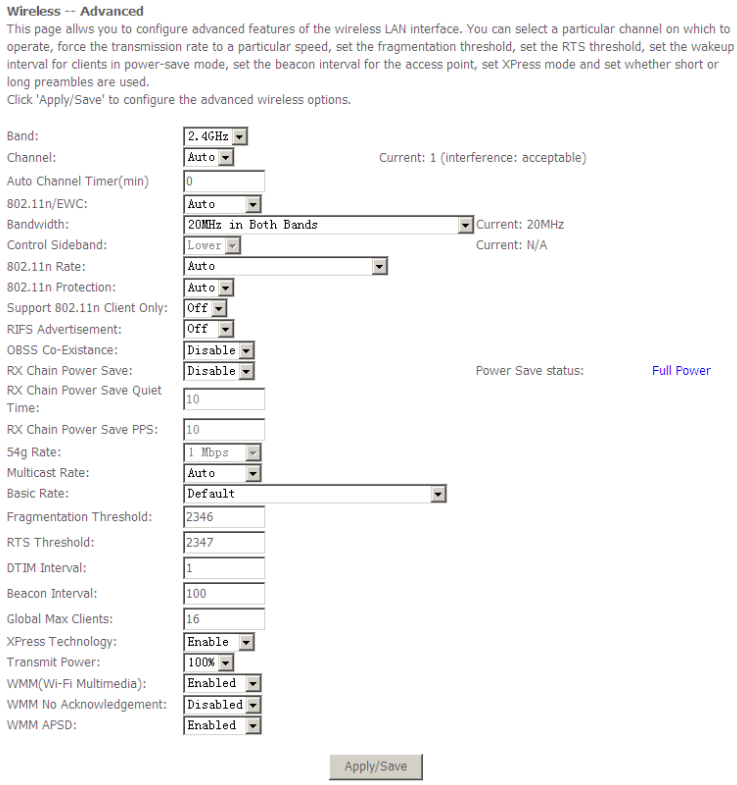
This page allows you to configure the wireless bridge features of the wireless LAN interface.

- **AP mode**: you may select **Access Point** or **Wireless Bridge**.
- **Bridge Restrict**: Enable or disable the bridge restrict function.
- **Remote Bridges MAC Address**: Enter the remote bridge MAC address.

After setting, click the **Apply/Save** button to save and apply the settings.

5.4.5. Advanced

Choose **Wireless** > **Advanced** to display the following page. This page allows you to configure the advanced features of the wireless LAN interface. Usually, you do not need to change the settings in this page.



- **Band:** The radio frequency remains at 2.4GHz.
- **Channel:** Fill in the appropriate channel to correspond with your network settings. All devices in your wireless network must use the same channel in order to work correctly. This router supports auto channeling functionality.
- **Auto Channel Timer (min):** Specifies the timer of auto channelling.
- **802.11n/EWC:** Select **disable** 802.11n or **Auto**.
- **Bandwidth:** Select the bandwidth for the network.
- **802.11n Rate:** Select the transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is **Auto**.

- **802.11n Protection:** The 802.11n standards provide a protection method so 802.11b/g and 802.11n devices can co-exist in the same network without “speaking” at the same time.
- **Support 802.11n Client Only:** Only stations that are configured in 802.11n mode can associate.
- **Multicast Rate:** Select the multicast transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is **Auto**.
- **Basic Rate:** Select the basic transmission rate ability for the AP.
- **Fragmentation Threshold:** Packets that are larger than this threshold are fragmented into multiple packets. Try to increase the fragmentation threshold if you encounter high packet error rates. Do not set the threshold too low, since this can result in reduced networking performance.
- **RTS Threshold:** This value should remain at its default setting of 2347.Should you encounter inconsistent data flow, only minor reductions are recommended. Should you encounter inconsistent data flow, only minor reduction of the default value, 2347, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of 2347.
- **DTIM Interval:** (Delivery Traffic Indication Message) Enter a value between 1 and 255 for the Delivery Traffic Indication Message (DTIM.) A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.
- **Beacon Interval:** A beacon is a packet of information that is sent from a connected device to all other devices where it announces its availability and readiness. A beacon interval is a period of time (sent with the beacon) before sending the beacon again. The beacon interval may be adjusted in milliseconds (ms). Default (100) is recommended.

- **XPress Technology:** Select Enable or Disable. This is a special accelerating technology for IEEE802.11g. The defaule is Disabled.
- **Transmit Power:** Adjust the transmission range here. This tool can be helpful for security purposes if you wish to limit the transmission range.

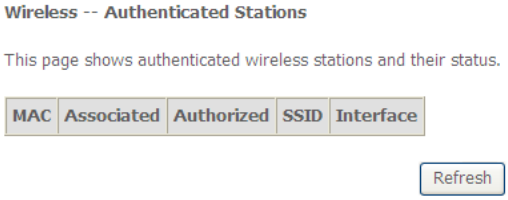
Click **Apply/Save** to configure the advanced wireless options and make the changes take effect.

Note:

The advanced wireless setting is only for the advanced user. For the common user, do not change any settings in this page.

5.4.6. Station Info

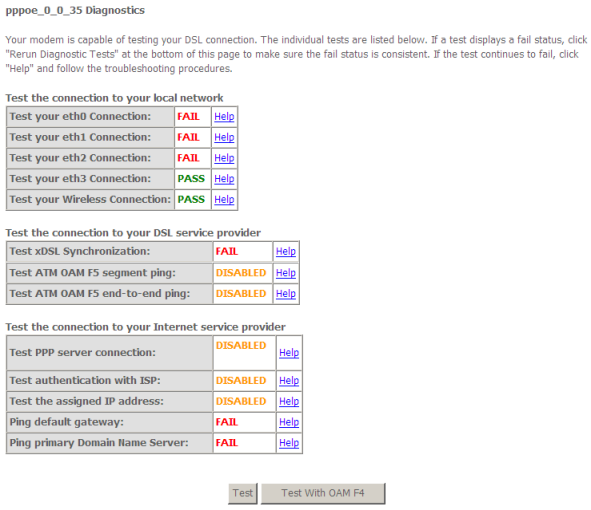
Choose **Wireless** > **Station Info** to display the following page.



This page shows the authenticated wireless stations and their status.

5.5. Diagnostics

Click **Diagnostics** > **Diagnostics**, and the following page appears.



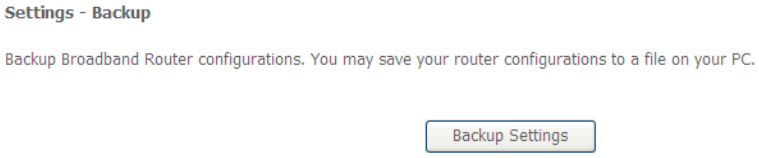
Your modem is capable of testing your DSL connection. The individual tests are listed below. If the test continues to fail, click **Help** and follow the troubleshooting procedures.

5.6. Management

5.6.1. Settings

Backup

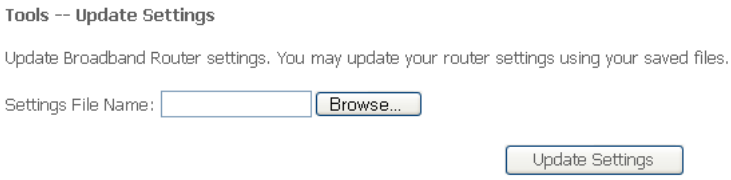
Choose **Management > Settings > Backup** to display the following page.



In this page, click the **Backup Settings** button to save your router's settings to your local PC.

Update

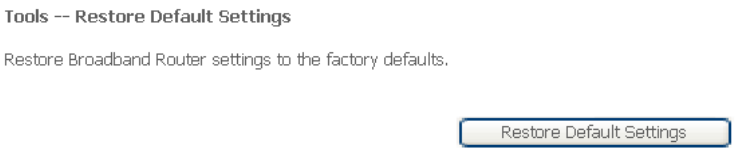
Choose **Management > Settings > Update**, and the following page appears.



In this page, click the **Browse…** button to select the correct new settings file, and then click the **Update Settings** button to update the router's settings.

Restore Default

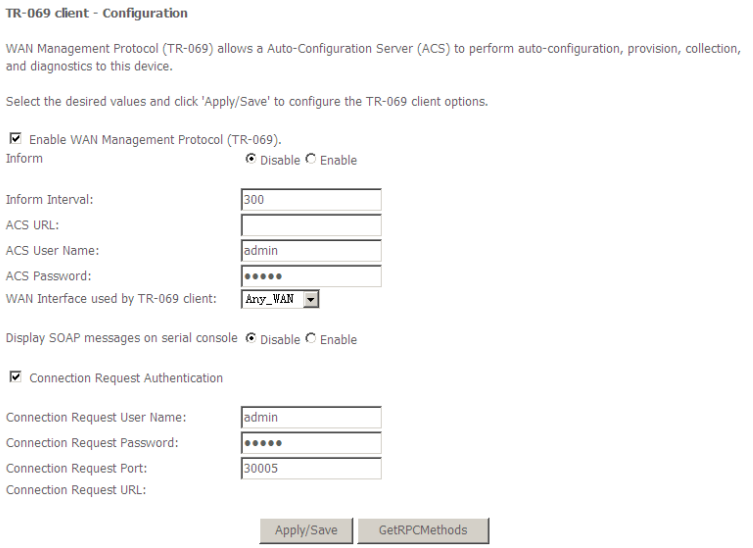
Choose **Management > Settings > Restore Default** to display the following page.



In this page, click the **Restore Default Settings** button, and then the system returns to the default settings.

5.6.2. TR-069 Client

Choose **Management > TR-069Client** to display the following page.



WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

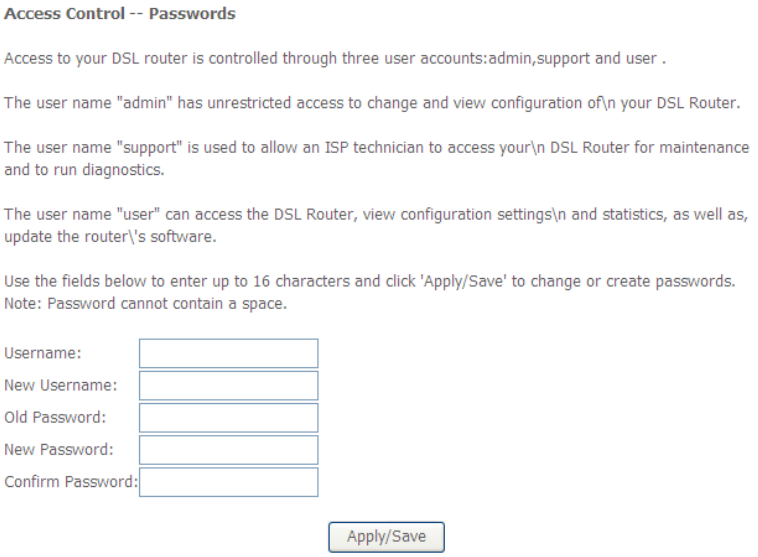
In this page, you may configure the parameters such as the ACS URL, ACS password, and connection request user name.

After setting, click the **Apply/Save** button to save and apply the settings.

5.6.3. Access Control

Passwords

Choose **Management > Access Control > Passwords**, and the following page appears.

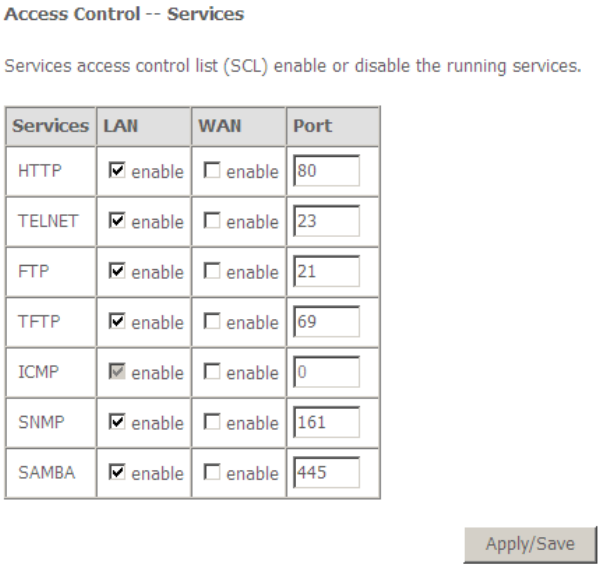


In the page, you can modify the username and password of different users.

After setting, click the **Apply/Save** button to save and apply the settings.

Services Control

Choose **Management > Access Control > Services Control** and the following page appears.

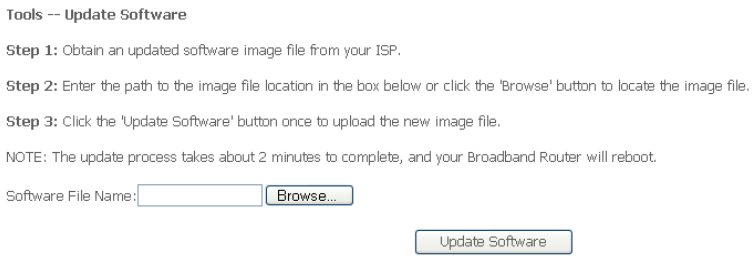


In this page, you can enable or disable the different types of services. It is recommended to keep it as default.

After setting, click the **Apply/Save** button to save and apply the settings.

5.6.4. Update Software

Choose **Management > Update Software**, and the following page appears.



If you want to upload the software, click the **Browse…** button to choose the new software, and then click the **Update Software** button.

Note:

When software update is in progress, do not shut down the router. After software update completes, the router automatically reboots.

Please make sure that the new software for updating is correct, and do not use other software to update the router.

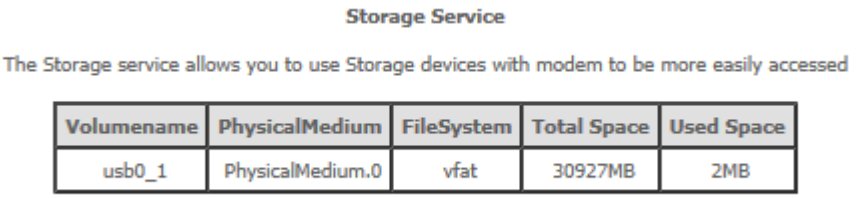
5.6.5. Reboot

Choose **Management > Reboot** and the following page appears.

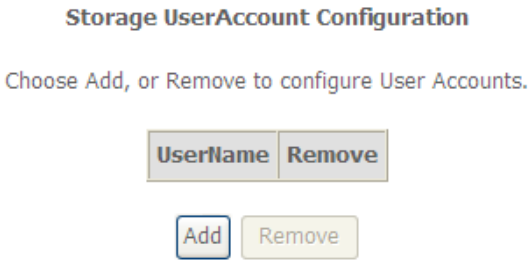
In this page, click the **Reboot** button, and then the router reboots.

Appendix I: How to Install and Access the USB Storage

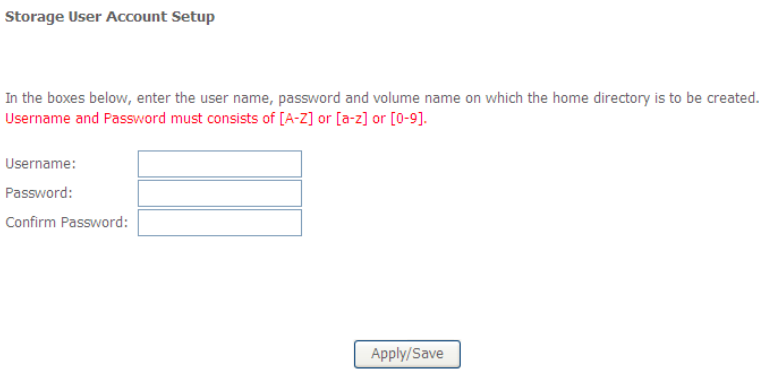
1. Plug USB storage into USB on AR-7288WnA.
2. Log in web management. (Example: HTTP://192.168.2.1)
3. Choose **Advanced Setup > Storage Service Storage Device Info**, and the following page appears. In this page, you can view the USB device info.



4. Choose **Advanced Setup > Storage Service > User Accounts**, and the following page appears. In this page, you may add or remove storage user accounts.

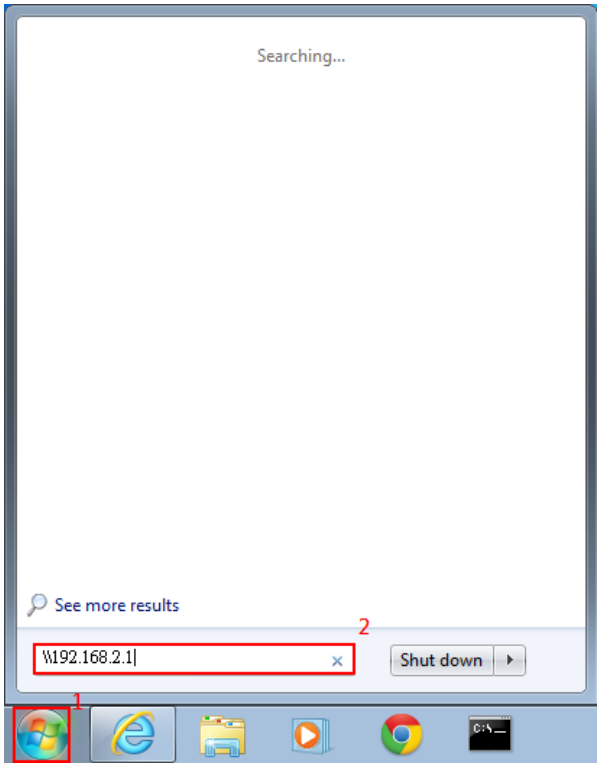


Click the **Add** button to display the following page.

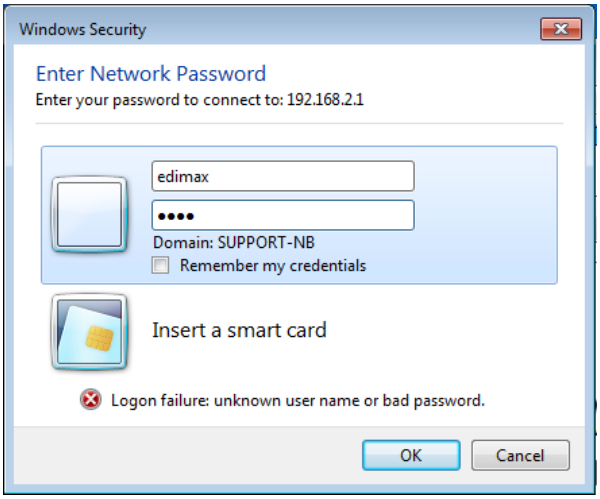


Enter the user name, password and volume name, and then click **Apply/Save** to finish setting up an account.
To delete an account, select it in the **Storage UserAccount Configuration** page, and then click **Remove**.

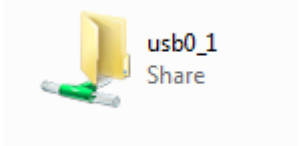
5. Click **Start**, input **\\192.168.2.1** (192.168.2.1 is IP address of AR-7288WnA), and then press **Enter.**



6. Enter username and password which you have added at step 4, and then click **OK**.



7. It will display the USB device. Double click left mouse on the fold, and then you are able to access the data in the USB storage.



Appendix II

The following are the general settings usually provided by the Internet Service Providers (ISP).
Upon running the "setup wizard" on CD-ROM (See *Quick Installation Guide page 8)* OR "Quick Start" (See *Quick Installation Guide page 10)*, all the below Settings (Pointers No. 1 & No. 2) are Pre-Set in AR-7288WnA; except Pointer No. 3, Username and Password (As provided by your ISP). Need to be Input by User accordingly.

General Setting For Australia
1) VPI/VCI set to 8/35
2) Protocol set to PPP over Ethernet (PPPoE) (RFC 2516) with LLC encapsulation
3) Username and password set according to the user ID that the customer has on the service they are
trying to connect to (either ISP or corporate). The user name must be set to the user ID followed by an @ symbol followed by the domain name e.g. example1@isp1.com.au or example2@isp2.net.au

General Setting For New Zealand
1) VPI/VCI set to 0/100
2) Protocol set to PPP over ATM (PPPoA) (RFC 2364) with VC-multiplexed encapsulation
3) Username and password set according to the user ID that the customer has on the service they are
trying to connect to (either ISP or corporate). The user name must be set to the user ID followed by an @ symbol followed by the domain name e.g. example@isp.co.nz
4) Operating Mode set to G.992.1, G.DMT or ANSI T1.413 iss 2 but not G.Lite or G.992.2

Note that:
1. *Reset the device to factory defaults (see Quick Installation Guide page 4.) if you have difficulty to setup your User Name and Password or if you would like to setup new user name or password.*
2. *Please contact your ISP (Internet Service Provider) if you are not sure about your ADSL 2/2+ modem setup information.*

PTC General Warning

The grant of a Telepermit for any item of terminal equipment indicates only that Telecom has accepted that the item complies with minimum conditions for connection to its network. It indicates no endorsement of the product by Telecom, nor does it provide any sort of warranty. Above all, it provides no assurance that any item will work correctly in all respects with another item of Telepermitted equipment of a different make or model, nor does it imply that any product is compatible with all of Telecom's network services.

Distributed by:
TechBrands by Electus Distribution Pty Ltd.
320 Victoria Road
Rydalmere, NSW 2116 Australia
www.techbrands.com
Tel: 1300 738 555
Int'l: +61 2 8832 3200
Fax: 1300 738 500

Manufactured by:
Edimax Technology Australia Pty Ltd
Level 1, 203 Blackburn Road, Mt Waverley, VIC3152, Australia
+61-8-61022811 (AUS) +64-9-8870589(NZ)
support@edimax-au.com / www.edimax.com

Australia Support Toll Free Number #1300 540 833
New Zealand Support Toll Free Number #0800 452 922

Trouble Shooting

Question	Answer
Why are all the indicators off?	• Check the connection between the power adapter and the power socket. • Check whether the power switch is turned on.
Why is the **LAN** indicator off?	• Check the connection between the device and your PC, hub or switch. • Check the running status of the computer, hub, or switch.
Why is the **ADSL** indicator off?	Check the connection between the **Line** port of the device and the wall jack.
Why does Internet access fail while the ADSL indicator is on?	Check whether the VPI, VCI, user name and password are correctly entered.
Why can I not access the web configuration page of the DSL router?	Choose **Start** > **Run** from the desktop, and ping ***192.168.2.1*** (IP address of the DSL router). If the DSL router is not reachable, check the type of network cable, the connection between the DSL router and the PC, and the TCP/IP configuration of the PC.
How to load the default settings after incorrect configuration?	To restore the factory default settings, turn on the device, and press the reset button for about 3 seconds, and then release it. The default IP address and the subnet mask of the DSL router are **192.168.2.1** and **255.255.255.0**, respectively. • User/password of super user: **admin/1234**

EU Declaration of Conformity

English: This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC, 2009/125/EC.

Français: Cet équipement est conforme aux exigences essentielles et autres dispositions de la directive 1999/5/CE, 2009/125/CE

Čeština: Toto zařízení je v souladu se základními požadavky a ostatními příslušnými ustanoveními směrnic 1999/5/ES, 2009/125/ES.

Polski: Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE 1999/5/EC, 2009/125/EC

Română: Acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 1999/5/CE, 2009/125/CE.

Русский: Это оборудование соответствует основным требованиям и положениям Директивы 1999/5/EC, 2009/125/EC.

Magyar: Ez a berendezés megfelel az alapvető követelményeknek és más vonatkozó irányelveknek (1999/5/EK, 2009/125/EC)

Türkçe: Bu cihaz 1999/5/EC, 2009/125/EC direktifleri zorunlu istekler ve diğer hükümlerle ile uyumludur.

Українська: Обладнання відповідає вимогам і умовам директиви 1999/5/EC, 2009/125/EC.

Slovenčina: Toto zariadenie spĺňa základné požiadavky a ďalšie príslušné ustanovenia smerníc 1999/5/ES, 2009/125/ES.

Deutsch: Dieses Gerät erfüllt die Voraussetzungen gemäß den Richtlinien 1999/5/EC, 2009/125/EC.

Español: El presente equipo cumple los requisitos esenciales de la Directiva 1999/5/EC, 2009/125/EC.

Italiano: Questo apparecchio è conforme ai requisiti essenziali e alle altre disposizioni applicabili della Direttiva 1999/5/CE, 2009/125/CE.

Nederlands: Dit apparaat voldoet aan de essentiële eisen en andere van toepassing zijnde bepalingen van richtlijn 1999/5/EC, 2009/125/EC.

Português: Este equipamento cumpre os requesitos essênciais da Directiva 1999/5/EC, 2009/125/EC

Norsk: Dette utstyret er i samsvar med de viktigste kravene og andre relevante regler i Direktiv 1999/5/EC, 2009/125/EC.

Svenska: Denna utrustning är i överensstämmelse med de väsentliga kraven och övriga relevanta bestämmelser i direktiv 1999/5/EG, 2009/125/EG.

Dansk: Dette udstyr er i overensstemmelse med de væsentligste krav og andre relevante forordninger i direktiv 1999/5/EC, 2009/125/EC.

Suomi: Tämä laite täyttää direktiivien 1999/5/EY, 2009/125/EY oleelliset vaatimukset ja muut asiaankuuluvat määräykset.

FOR USE IN AT BE CY CZ DK EE FI FR RU DE GR HU IE IT LV LT LU MT NL PL PT UA SK SI ES SE GB IS LI NO CH BG RO TR

N20379

WEEE Directive & Product Disposal

At the end of its serviceable life, this product should not be treated as household or general waste. It should be handed over to the applicable collection point for the recycling of electrical and electronic equipment, or returned to the supplier for disposal.

Declaration of Conformity

We, Edimax Technology Co., LTD., declare under our sole responsibility, that the equipment described below complies with the requirements of the European Council directive (1995/5/EC, 2006/95/EC).

Equipment : **N300 Wireless ADSL Modem Router**
Model No. : **AR-7288WnA**

The following European standards for essential requirements have been followed:

Spectrum : **ETSI EN 300 328 : V1.8.1(2012-06)**
EMC : **EN 301 489-1 V1.9.2(2011-09)**
EN 301 489-17 V2.2.1(2012-09)
EMF : **EN 50385:2002**
Safety (LVD) : **IEC 60950-1:2005(2nd)+A1:2009**
EN 60950-1 : 2006+A11:2009+A1:2010+A12:2011

Edimax Technology Co., Ltd.
No. 3, Wu Chuan 3rd Road,
Wu-Ku Industrial Park.
New Taipei City, Taiwan

Date of Signature: March, 2014
Signature:

Printed Name: Albert Chang
Title: Director
Edimax Technology Co., Ltd.