Ovislink OV504WN
User Manual

Ver 1.0

Contents

1 Safety Precautions

Read the following information carefully before operating the device. Please follow the following precaution items to protect the device from risks and damage caused by fire and electric power:

- Use volume labels to mark the type of power.
- Use the power adapter that is packed within the device package.
- Pay attention to the power load of the outlet or prolonged lines. An overburden power outlet or damaged lines and plugs may cause electric shock or fire accident. Check the power cords regularly. If you find any damage, replace it at once.
- Proper space left for heat dissipation is necessary to avoid any damage caused by overheating to the device. The 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 a place where a heat source exits or high temperature occurs. Avoid the device from direct sunshine.
- Do not put this device close to a place where is over damp or watery. Do not spill any fluid on this device.
- Do not connect this device to any PC or electronic product, unless our customer engineer or your broadband provider instructs you to do this, because any wrong connection may cause any power or fire risk.
- Do not place this device on an unstable surface or support.

2 Overview

The DSL Router is a highly ADSL2+ Integrated Access Device and can support ADSL link with downstream up to 24 Mbps and upstream up to 1 Mbps. It is designed to provide a simple and cost-effective ADSL Internet connection for a private Ethernet or 802.11g/802.11b/802.11n wireless network. The Router combines high-speed ADSL Internet connection, IP routing for the LAN and wireless connectivity in one package. It is usually preferred to provide high access performance applications for the individual users, the SOHOs, and the small enterprises.

The Router is easy to install and use. The Modem connects to an Ethernet LAN or computers via standard Ethernet ports. The ADSL connection is made using ordinary telephone line with standard connectors. Multiple workstations can be networked and connected to the Internet by a single Wide Area Network (WAN) interface and single global IP address. The advanced security enhancements, packet filtering and port redirection, can help protect your network from potentially devastating intrusions by malicious agents from outside your network.

Network and Router management is done through the web-based management interface that can be accessed through the local Ethernet using any web browser. You may also enable remote management to enable configuration of the Router via the WAN interface.

2.1 Application

- Home gateway
- SOHOs
- Small enterprises
- Higher data rate broadband sharing
- PC file and application sharing
- Network and online gaming

2.2 Features

- User-friendly GUI for web configuration

- Several pre-configured popular games. Just enable the game and the port settings are automatically configured.
- Compatible with all standard Internet applications
- Industry standard and interoperable DSL interface
- Simple web-based status page displays a snapshot of system configuration, and links to the configuration pages
- Downloadable flash software updates
- Support for up to 16 permanent virtual circuits (PVC)
- Support for up to 8 PPPOE sessions
- Support NAT
- WLAN with high-speed data transfer rates of up to 130 Mbps, compatible with IEEE 802.11b/g/n, 2.4GHz/5G compliant equipment
- Optimized Linux 2.6 Operating System
- IP routing and bridging
- Asynchronous transfer mode (ATM) and digital subscriber line (DSL) support
- Point-to-point protocol (PPP)
- Network/port address translation (NAT/PAT)
- Quality of service (QoS)
- Wireless LAN security: WPA, 802.1x, RADIUS client
- Virtual private network (VPN): IPSec
- Universal plug-and-play
- Management and control
  - Web-based management (WBM)
  - Command line interface (CLI)
  - TR-069 WAN management protocol
- Remote update
- System statistics and monitoring
- DSL router is targeted at the following platforms: DSL modems, wireless access points and bridge.

2.3 Standards Compatibility and Compliance

- Support application level gateway (ALG)
- ITU G.992.1 (G.dmt)
- ITU G.992.2 (G.lite)

- ITU G.994.1 (G.hs)
- ITU G.992.3 (ADSL2)
- ITU G.992.5 (ADSL2+)
- ANSI T1.413 Issue 2
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n

3 Hardware Description and Hardware Installation

3.1 Hardware Description

3.1.1 Front Panel

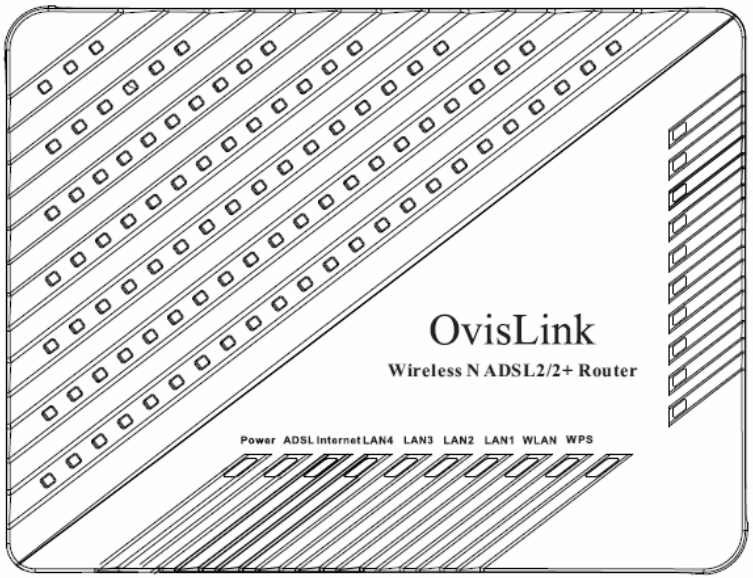


Figure 1 Front panel

The following table describes the indicators on the front panel.

Indicator	Color	Status	Description
Power	Green	On	Power is on.
	Red	On	Power is on and the device is initiating.
	Red	Blink	The firmware is upgrading.
		Off	Power is off or the device is down.

Indicator	Color	Status	Description
ADSL	Green	On	DSL link has established.
	Green	Blink twice at every second	No DSL link is detected.
	Green	Blink four times at every second	DSL link is detected.
	-	Off	Device is powered off.
Internet	Green	On	PPP/DHCP takes effect.
	Green	Blink	PPP/DHCP is negotiating.
	Green	Blink quickly	Data is being transmitted.
	Red	On	Authentication fails.
LAN 4/3/2/1	Green	On	The Ethernet interface is connected.
	Green	Blink	Data is being transmitted through the Ethernet interface.
	-	Off	The Ethernet interface is disconnected.
WLAN	Green	On	WLAN is enabled.
	Green	Blink	Data is being transmitted through the wireless interface.
	-	Off	WLAN is disabled.
WPS	Green	On	Connection succeeds under Wi-Fi Protected Setup.
	Green	Blink	Negotiation is in progress under Wi-Fi Protected Setup.
	-	Off	Wi-Fi Protected Setup is disabled.

3.1.2 Rear Panel

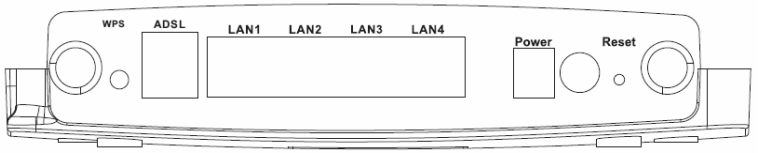


Figure 2 Rear panel

The following table describes the interfaces or the buttons on the rear panel.

Interface	Description
WPS	This button is used for enabling WPS PBC mode. If WPS is enabled, press this button, and then the wireless router starts to accept the negotiation of PBC mode.
ADSL	RJ-11 port, for connecting the ADSL cable.
LAN 1~4	RJ-45 port, for connecting the router to a PC or another network device.
Power	Power interface, for connecting the power adapter.
◯	Power switch.
Reset	Press the button for at least 1 second and then release it. System restores the factory default settings.

⚠ **Warning:**

*Do not press the **Reset** button unless you want to clear the current settings. The **Reset** button is in a small circular hole on the rear panel. If you want to restore the default settings, please press the **Reset** button gently for 1 second with a fine needle inserted into the hole and then release the button. The system reboots and returns to the factory defaults.*

The power specification is 12V, 1A. If the power adapter does not match the specification, it may damage the device.

3.2 Hardware Installation

3.2.1 Choosing the Best Location for Wireless Operation

Many environmental factors may affect the effective wireless function of the DSL Router. If this is the first time that you set up a wireless network device, read the following information:

The access point can be placed on a shelf or desktop, ideally you should be able to see the LED indicators in the front, as you may need to view them for troubleshooting. Designed to go up to 100 meters indoors and up to 300 meters outdoors, wireless LAN lets you access your network from anywhere you want. However, the numbers of walls, ceilings, or other objects that the wireless signals must pass through limit signal

range. Typical ranges vary depending on types of materials and background RF noise in your home or business.

3.2.2 Connecting the Device

Please follow the steps below to connect the device.

Step1 Connect the **ADSL** port of the DSL router with a telephone cable.

Step2 Connect the LAN port of the DSL router to the network card of the PC via an Ethernet cable.

Step3 Plug one end of the power adapter to the wall outlet and connect the other end to the Power port of the DSL Router.

The followig figure displays the connection of the DSL router, PC, and telephones.

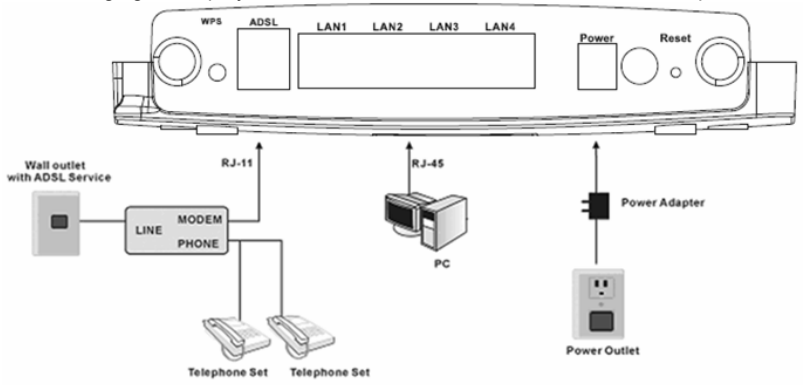


Figure 3 Connecting the DSL router

4 PC Network Configuration and Login

4.1 PC Network Configuration

Each network interface on the PC should either be configured with a statically defined IP address and DNS address, or be instructed to automatically obtain an IP address using the network DHCP server. DSL router provides a DHCP server on its LAN and it is recommended to configure your LAN to automatically obtain its IP address and DNS server IP address.

The configuration principle is identical but should be carried out differently on each operating system.

The following displays the **TCP/IP Properties** dialog box on Windows XP.

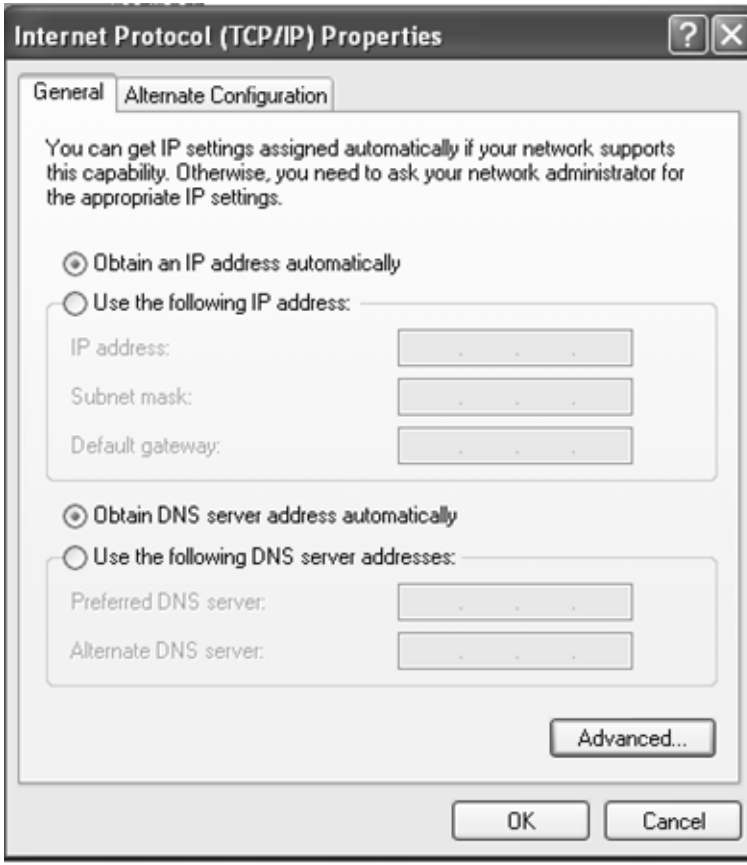


Figure 4 IP and DNS configuration

TCP/IP configuration steps for Windows XP are as follows:

Step1 Choose **Start** > **Control Panel** > **Network Connections**.

Step2 Right-click the Ethernet connection icon and choose **Properties**.

Step3 On the **General** tab, select the **Internet Protocol (TCP/IP)** component and click **Properties**.

Step4 The **Internet Protocol (TCP/IP) Properties** window appears.

Step5 Select the **Obtain an IP address automatically** radio button.

Step6 Select the **Obtain DNS server address automatically** radio button.

Step7 Click **OK** to save the settings.

4.2 Logging In to the DSL Router

To log in to the DSL router, do as follows:

Step1 Open a Web browser on your computer.

Step2 Enter ***http://192.168.1.1*** (the default IP address of the DSL router) in the address bar. The login page appears.

Step3 Enter the user name and the password. The default username and password of the super user are **admin** and **admin**. The username and password of the common user are **user** and **user**. You need not enter the username and the password again if you select the option **Remember my password**. It is recommended to change these default values after logging in to the DSL router for the first time.

Step4 Click **OK** to log in to the Web page. Otherwise, please click **Cancel** to exit the login page.

Figure 5 Login page

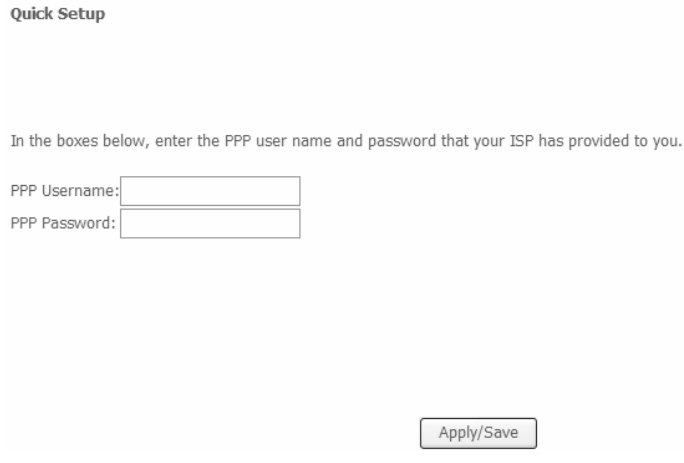
After logging in to the DSL router as a super user, you can query, configure, and modify all the settings, and diagnose the system.

5 Web-Based Management

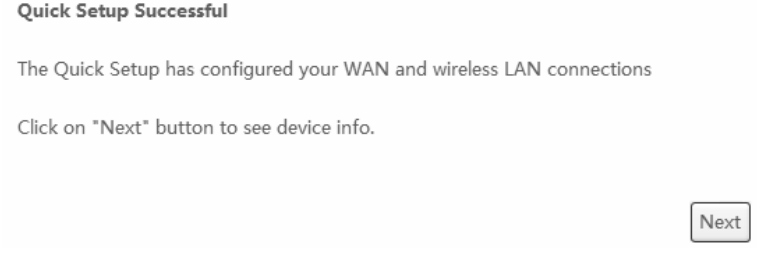
This chapter describes how to use Web-based management of the DSL router, which allows you to configure and control all of DSL router features and system parameters in a user-friendly GUI.

5.1 Quick Setup

Choose **Quick Setup** and the following page is displayed.



Enter the username and password your ISP has provided to you. The following page is displayed if quick setup is successful. Click **Next** to see the device information.

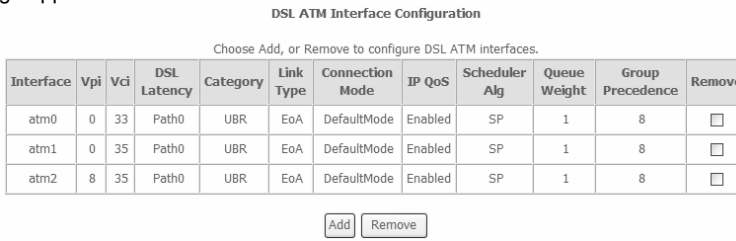


5.2 Advanced Setup

5.2.1 Layer2 Interface

ATM Interface

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



DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove
atm0	0	33	Path0	UBR	EoA	DefaultMode	Enabled	SP	1	8	☐
atm1	0	35	Path0	UBR	EoA	DefaultMode	Enabled	SP	1	8	☐
atm2	8	35	Path0	UBR	EoA	DefaultMode	Enabled	SP	1	8	☐

Add Remove

Figure 6 DSL ATM interface configuration

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

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

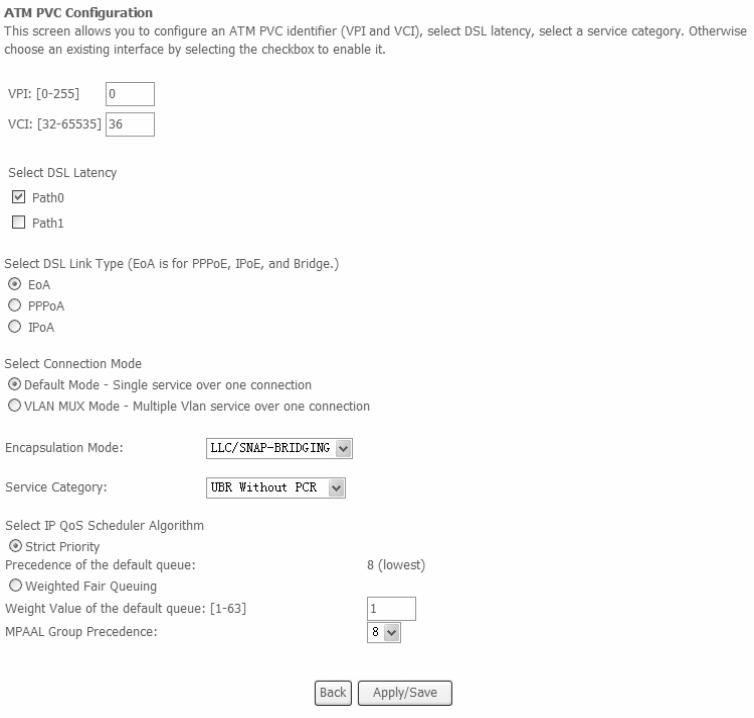


Figure 7 ATM PVC configuration

In this page, you can set the VPI and VCI values, and select the DSL latency, link type (EoA is for PPPoE, IPoE, and Bridge.), connection mode, encapsulation mode, service category, and IP QoS scheduler algorithm.

- **VPI (Virtual Path Identifier)**: The virtual path between two points in an ATM network, and its valid value is from 0 to 255.
- **VCI (Virtual Channel Identifier)**: The virtual channel between two points in an ATM network, ranging from 32 to 65535 (1 to 31 are reserved for known protocols).
- **Select DSL Latency**: You may select **Path0** and **Path1**.

- **Select DSL Link Type**: You may select **EoA** (it is for PPPoE, IPoE, and Bridge), **PPPoA**, or **IPoA**.
- **Select Connection Mode:** You may select the **Default Mode** or the **VLAN MUX Mode**.
- **Encapsulation Mode**: You may select **LLC/SNAP-BRIDGING** or **VC/MUX** in the drop-down list.
- **Service Category:** you may select **UBR Without PCR**, **UBR With PCR**, **CBR**, **Non Realtime VBR** or **Realtime VBR** in the drop-down lsit.
- **Select IP QoS Scheduler Algorithm:** You may select **Strict Priority** and **Weighted Fair Queuing**.

Note:

QoS cannot be set for CBR and Realtime VBR.

After finishing setting, click the **Apply/Save** button to make the settings take effect. See the following figure:

If you want to remove this Interface, please select the **Remove** check box that is corresponding to the selected interface and then click the **Remove** button.

5.2.2 WAN Service

Choose **Advance Setup > WAN Service,** and the following page appears.

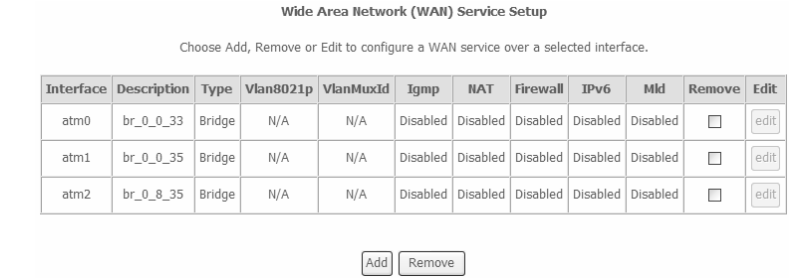


Figure 8 WAN service configuration

In this page, you are allowed to add, remove, or edit a WAN service.

Adding a PPPoE WAN Service

This section describes the steps for adding the pppoe_0_0_36 (PPPoE mode) service.

Step1 In the **Wide Area Network (WAN) Service Setup** page, click the **Add** button to display the following page. (At first, you must add a proper ATM configuration for this WAN service.)

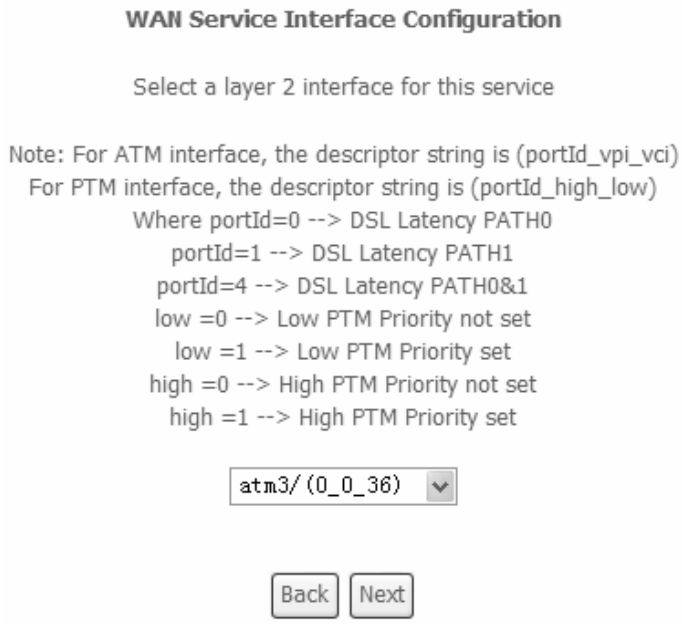


Figure 9 WAN service interface configuration (PPPoE)

Step2 In this page, you can select a ATM Interface for the WAN service. After selecting the ATM interface, click **Next** to display the following page.

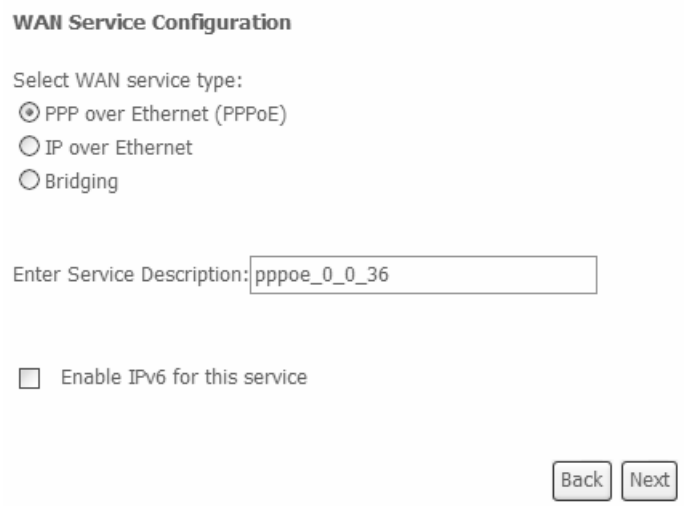


Figure 10 WAN service configuration (PPPoE)

Step3 In this page, select the WAN service type to be **PPP over Ethernet (PPPoE)**. Click **Next** to display the following page.

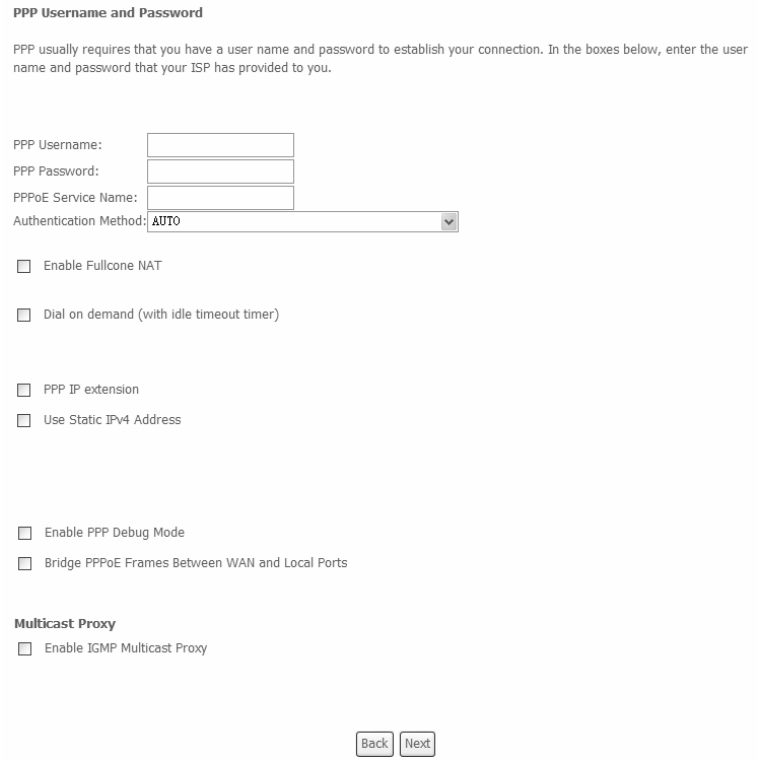


Figure 11 PPP username and password (PPPoE)

Step4 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 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 PPPOE connection. Once it detects the flow (like access to a webpage), the modem restarts the PPPoE dialup. If this function is disabled, the modem performs PPPoE dial-up all the time. The PPPoE connnection does not stop, unless the modem is powered off and DSLAM or uplink equipment is abnormal.
- **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 modem obtains an IP address assigned by an uplink equipment such as BAS, through PPPoE dial-up. If this function is enabled, the modem 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.

Step5 After setting the parameters, click **Next** to display the following page.

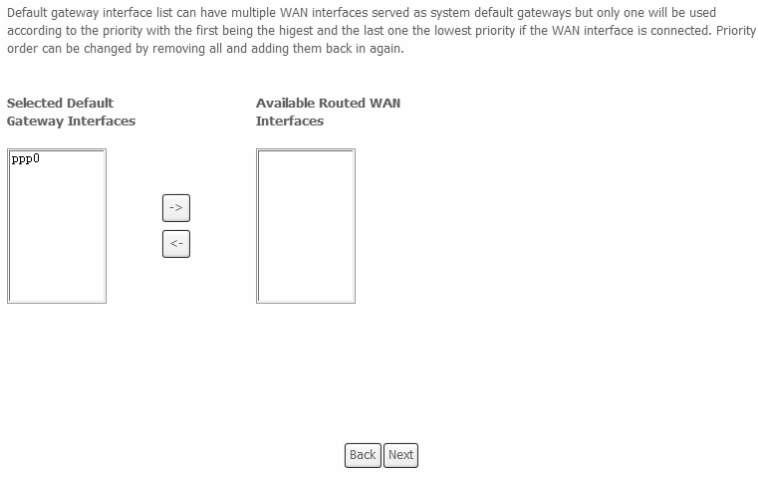


Figure 12 Routing-default gateway (PPPoE)

Step6 In this page, select a preferred WAN interface as the system default gateway and then click **Next** to display the following page.

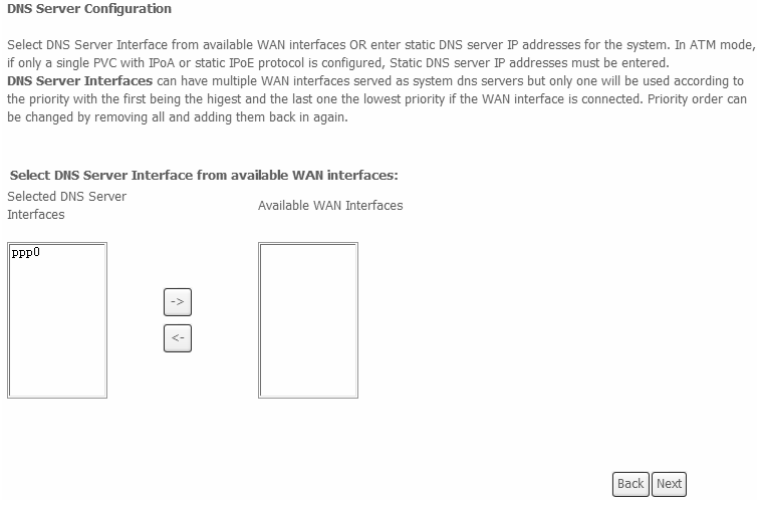


Figure 13 DNS server configuration(PPPoE)

Step7 In this page, you may obtain the DNS server addresses from the selected WAN interface or manually enter the static DNS server addresses. If only a PVC with IPoA or static MER protocol is configured, you must manually enter the static DNS server addresses. Click **Next**, and the following page appears.

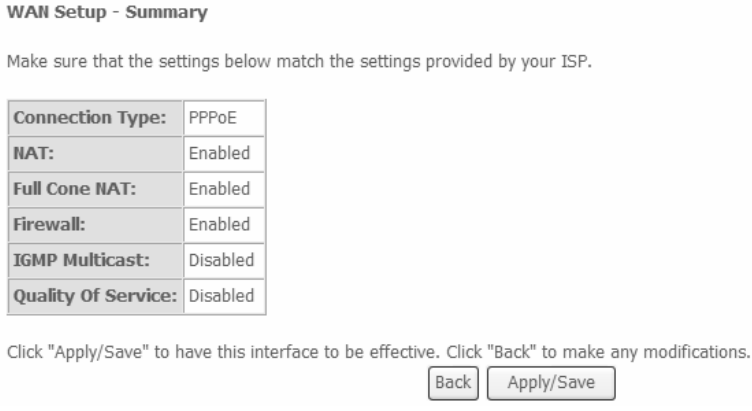


Figure 14 PPPoE summary

Step8 In this page, it displays the information about the PPPoE settngs. Click **Apply/Save** to save and apply the settings, and then the following page appears. You can modify the settings by clicking the **Back** button if necessary.

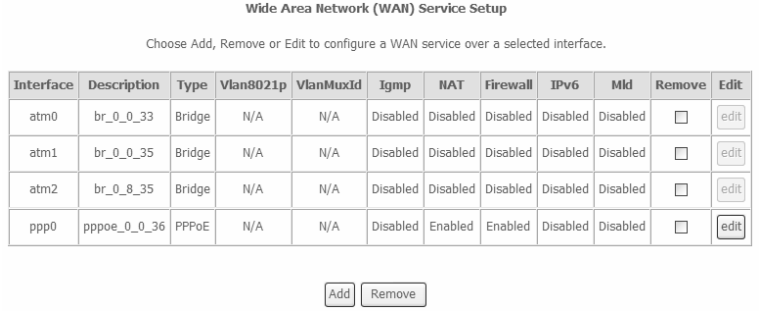


Figure 15 Completing the settings of PPPoE WAN service

Adding a MER (IPoE) WAN service

This section describes the steps for adding the ipoe_0_0_37 (MER mode) service.

Step1 In the **Wide Area Network (WAN) Service Setup** page, click the **Add** button to display the following page. (At first, you must add a ATM configuration for this WAN service.)

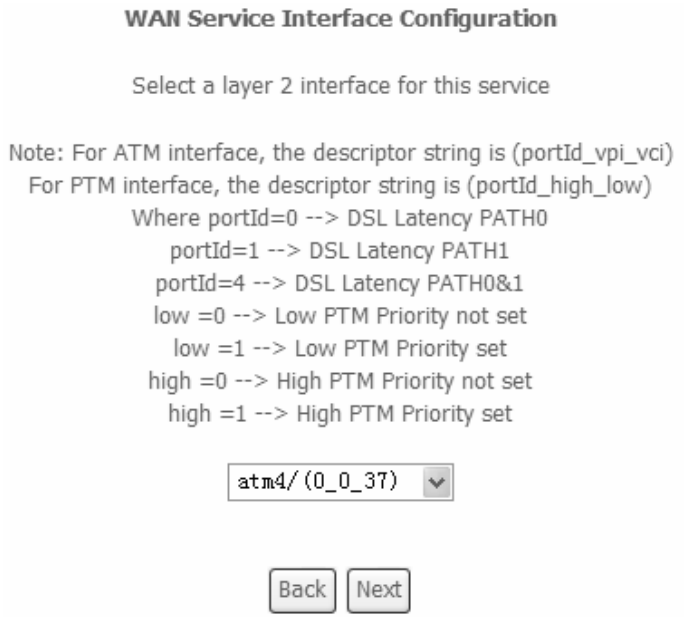


Figure 16 WAN service interface configuration (IPoE)

Step2 Select an ATM Interface, for example, atm1/(0_0_37), and then click **Next** to display the following page.

Figure 17 WAN service configuration (IPoE)

Step3 In this page, select the WAN service type to be IP over Ethernet, and r the service description. After finishing setting, click **Next** to display the following page.

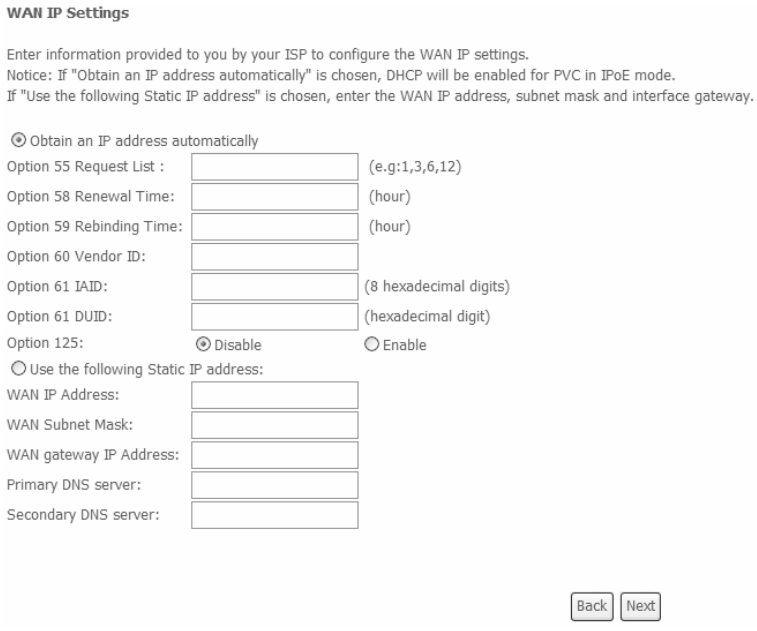


Figure 18 WAN IP settings (IPoE)

Step4 In this page, you may themodify 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 you select **Obtain an IP address automatically**, DHCP will be enabled for PVC in MER mode.*

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

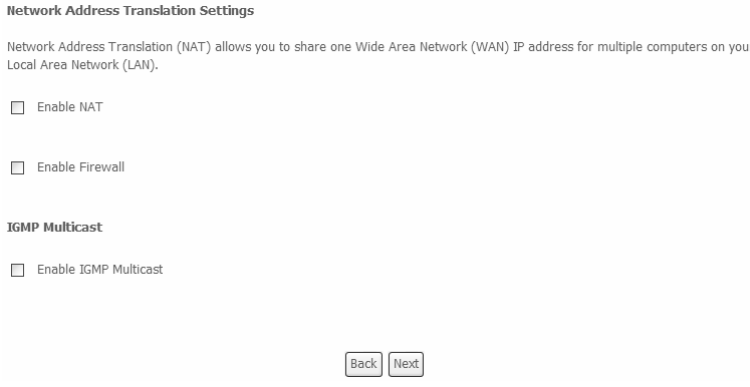


Figure 19 Network address translation settings (IPoE)

Step5 In this page, you can set the network address translation settings,for example, enabling NAT, enabling firewall, and.enabling IGMP multicast. After finishing setting, click **Next** and the following page appears.

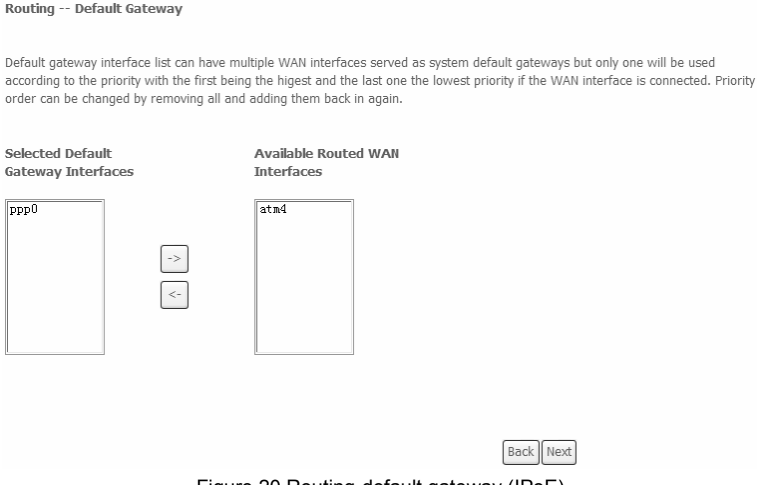


Figure 20 Routing-default gateway (IPoE)

Step6 In this page, select a preferred WAN interface as the system default gateway and then click **Next** to display the following page.

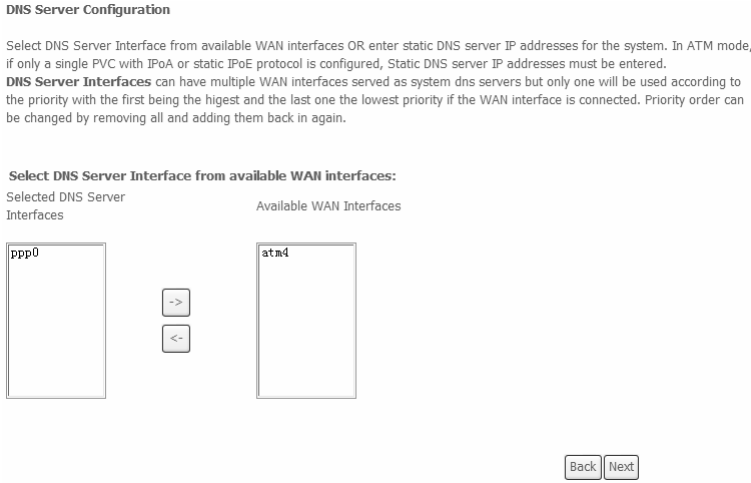


Figure 21 DNS server configuration (IPoE)

Step7 In this page, you may obtain the DNS server addresses from the selected WAN interface or manually enter static DNS server addresses. If only a PVC with IPoA or static MER protocol is configured, you must enter the static DNS server addresses. After finishing setting, click **Next** to display the following page.

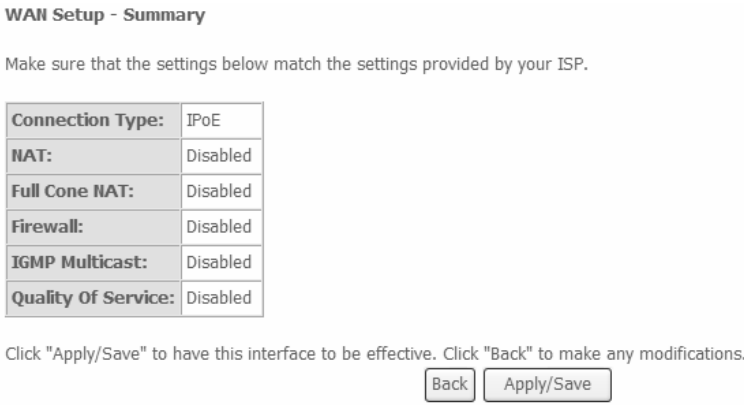


Figure 22 IPoE summary

Step8 In this page, it displays the information about the IPoE settngs.Click **Apply/Save** to save and apply the settings, and then the following page appears. You can modify the settings by clicking the **Back** button if necessary.

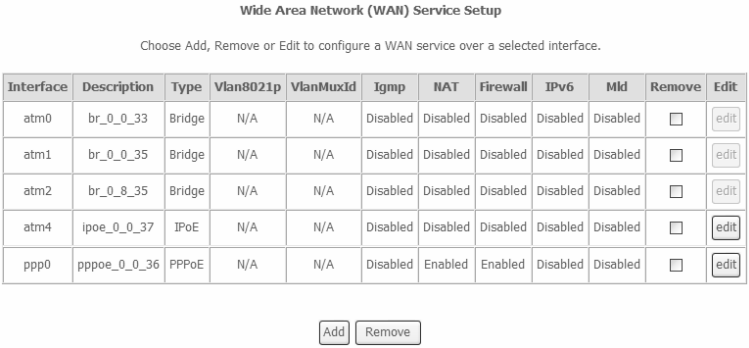


Figure 23 Completing the settings of IPoE WAN service

Adding a PPPoA WAN service

This section describes the steps for adding the pppoa_0_0_38 (PPPoA mode) service.

Step1 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.

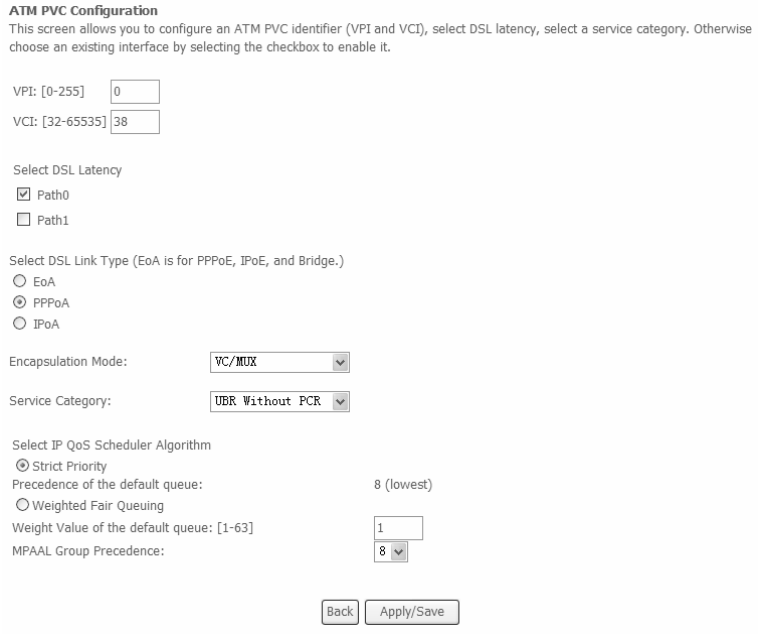
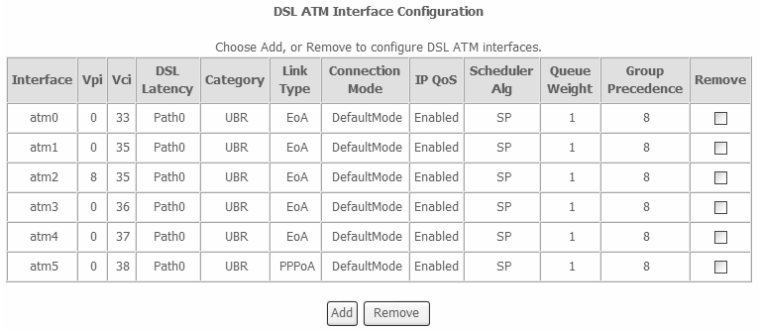


Figure 24 ATM PVC configuration (PPPoA)

Step2 Select the DSL link type to be **PPPoA**, and select the encapsulation mode to be **VC/MUX** (according to the uplink equipment). After finishing setting, click the **Apply/Save** button to apply the setings, and the following page appears.



DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove
atm0	0	33	Path0	UBR	EoA	DefaultMode	Enabled	SP	1	8	☐
atm1	0	35	Path0	UBR	EoA	DefaultMode	Enabled	SP	1	8	☐
atm2	8	35	Path0	UBR	EoA	DefaultMode	Enabled	SP	1	8	☐
atm3	0	36	Path0	UBR	EoA	DefaultMode	Enabled	SP	1	8	☐
atm4	0	37	Path0	UBR	EoA	DefaultMode	Enabled	SP	1	8	☐
atm5	0	38	Path0	UBR	PPPoA	DefaultMode	Enabled	SP	1	8	☐

Add Remove

Figure 25 Adding a DSL ATM interface for PPPoA service

Step3 Choose **WAN Service** and click **Add** to display the following page.

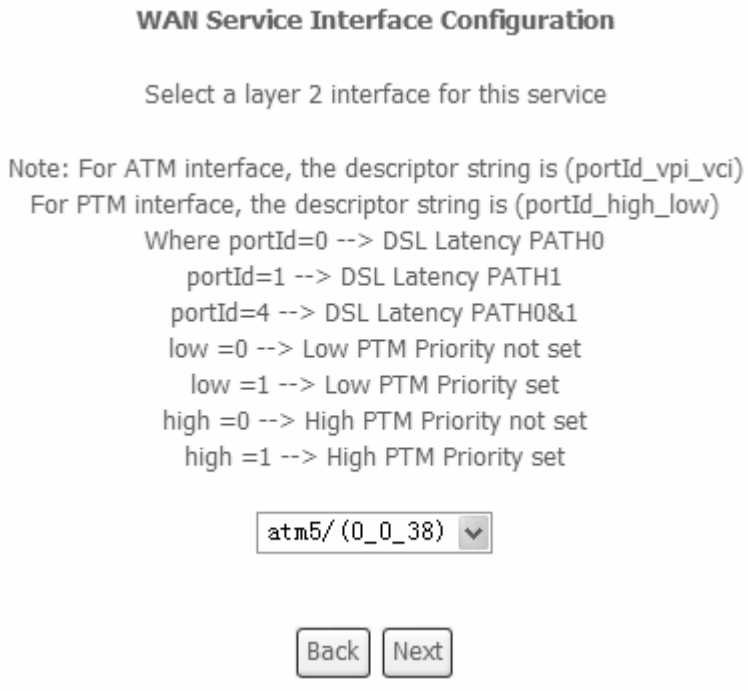


Figure 26 WAN service interface configuration (PPPoA)

Step4 Select the proper interface for the WAN service, and then click **Next** to display the following page.

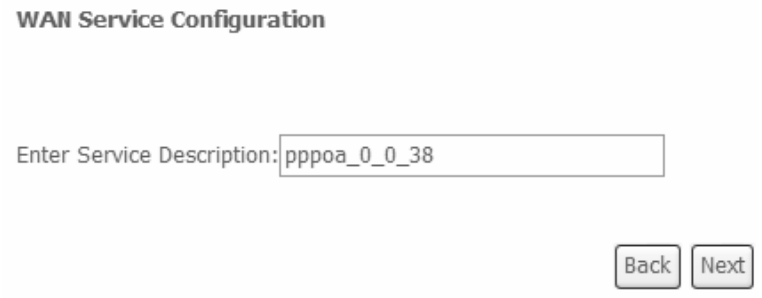


Figure 27 WAN service configuration (PPPoA)

Step5 In this page, you may modify the service description. Click **Next** to display the following page.

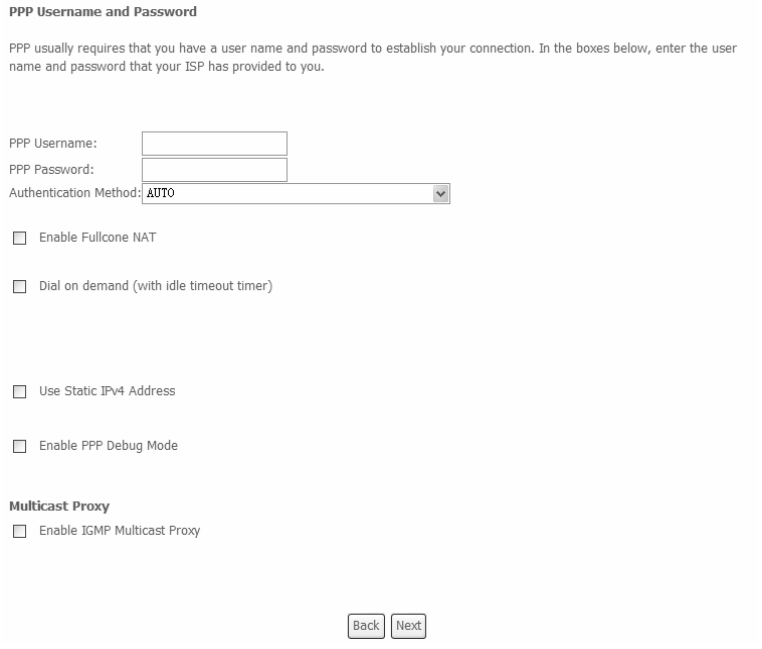


Figure 28 PPP username and password (PPPoA)

Step6 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 finishing setting, click **Next** to display the following page.

Figure 29 Routing-default gateway (PPPoA)

Step7 In this page, select a preferred WAN interface as the system default gateway and then click **Next** to display the following page.

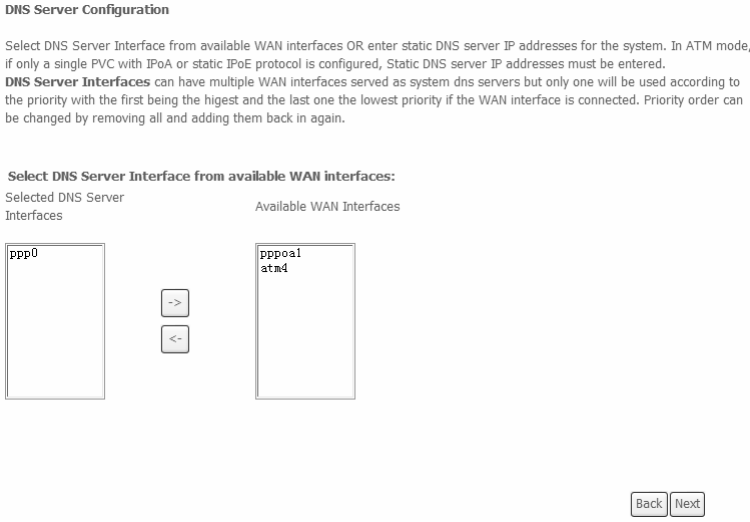


Figure 30 DNS server configuration (PPPoA)

Step8 In this page, you can obtain the DNS server addresses from the selected WAN interface or manually enter the static DNS server addresses. If only a PVC with IPoA or static MER protocol is configured, you must enter the static DNS server addresses. After finishing setting, click **Next** to display the following page.

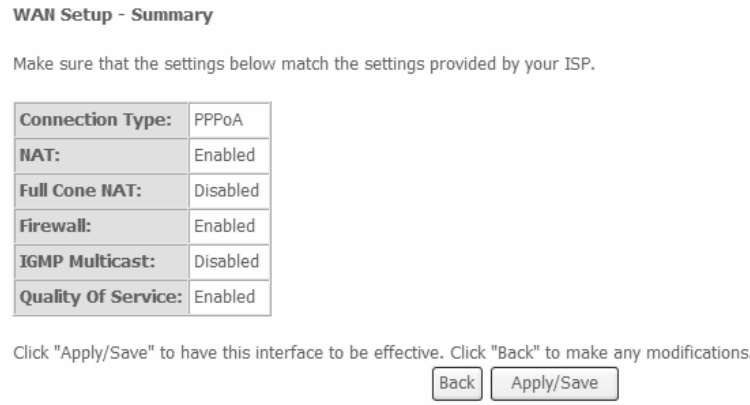


Figure 31 PPPoA summary

Step9 In this page, it displays the information about the PPPoA settngs.Click **Apply/Save** to apply the settings, and then the following page appears. You can modify the settings by clicking the **Back** button if necessary.

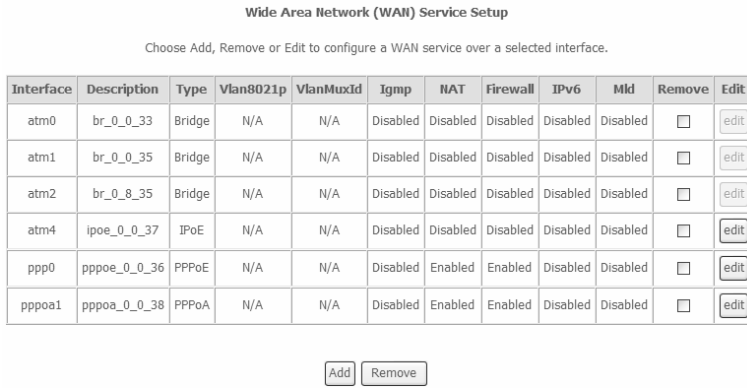


Figure 32 Completing the settings of PPPoA WAN service

Adding an IPoA WAN service

This section describes the steps for adding the ipoa_0_0_39 (IPoA mode).

Step1 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.

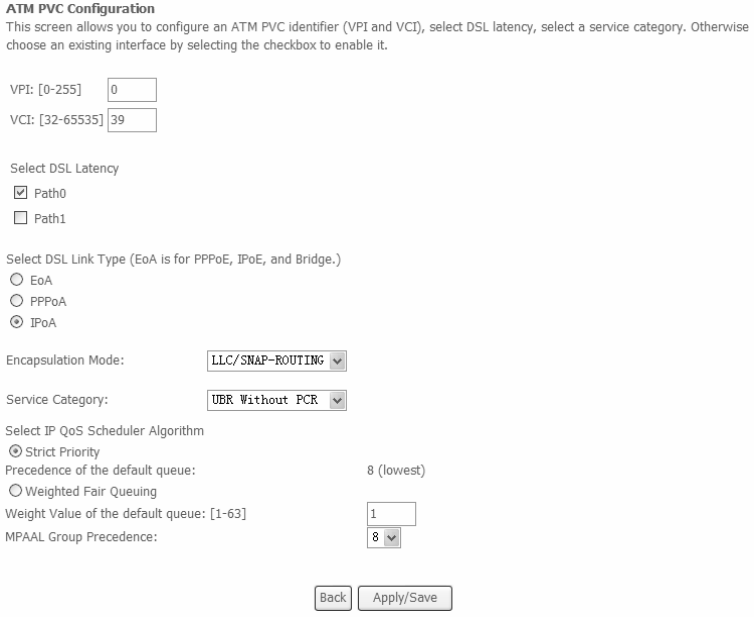
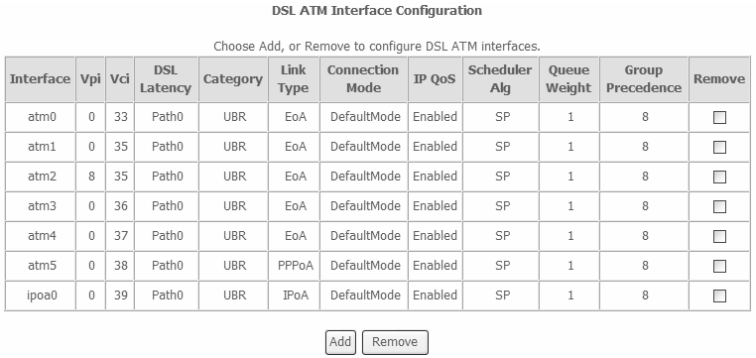


Figure 33 ATM PVC configuration (IPoA)

Step2 Select the DSL link type to be **IPoA**, and select the encapsulation mode to be **LLC/SNAP-ROUTING** (according to the uplink equipment). After finishing setting, click the **Apply/Save** button to display the following page.



DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove
atm0	0	33	Path0	UBR	EoA	DefaultMode	Enabled	SP	1	8	☐
atm1	0	35	Path0	UBR	EoA	DefaultMode	Enabled	SP	1	8	☐
atm2	8	35	Path0	UBR	EoA	DefaultMode	Enabled	SP	1	8	☐
atm3	0	36	Path0	UBR	EoA	DefaultMode	Enabled	SP	1	8	☐
atm4	0	37	Path0	UBR	EoA	DefaultMode	Enabled	SP	1	8	☐
atm5	0	38	Path0	UBR	PPPoA	DefaultMode	Enabled	SP	1	8	☐
ipoa0	0	39	Path0	UBR	IPoA	DefaultMode	Enabled	SP	1	8	☐

Add Remove

Figure 34 Adding a DSL ATM interface for IPoA service

Step3 Choose **WAN Service** and click **Add** to display the following page.

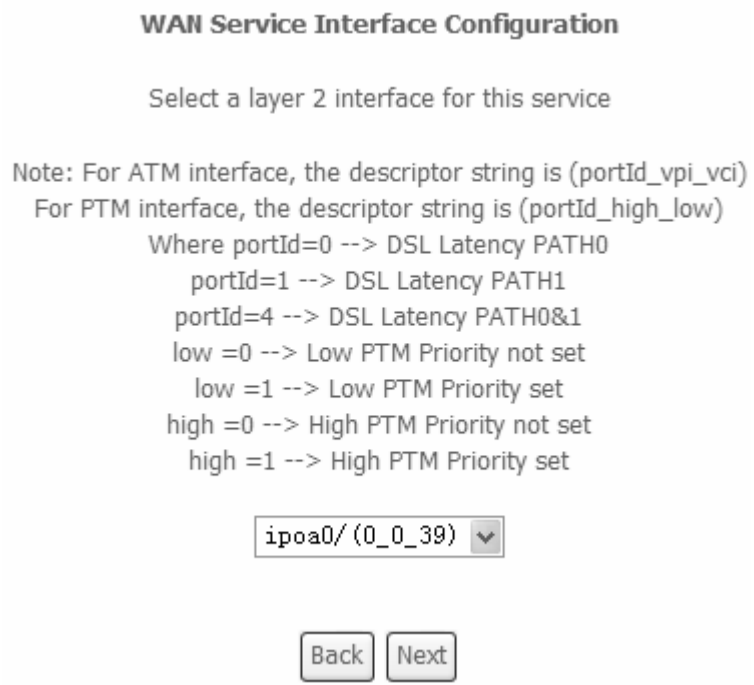


Figure 35 WAN service interface configuration (IPoA)

Step4 Select the proper interface for the WAN service ,and then click **Next** to display the following page.

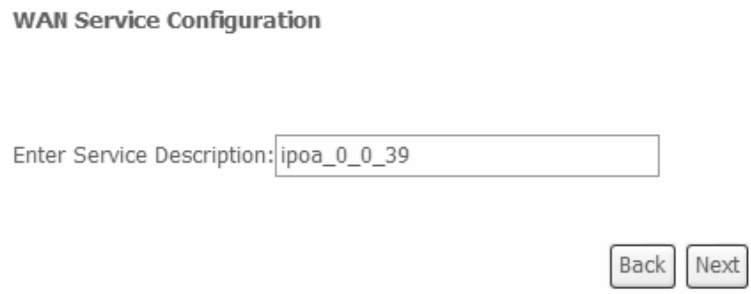


Figure 36 WAN service configuration (IPoA)

Step5 In this page, you may modify the service description. Click **Next** to display the following page.

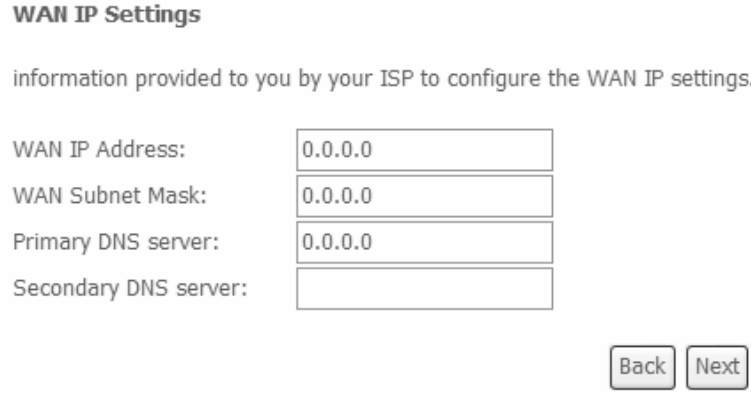


Figure 37 WAN IP settings (IPoA)

Step6 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.

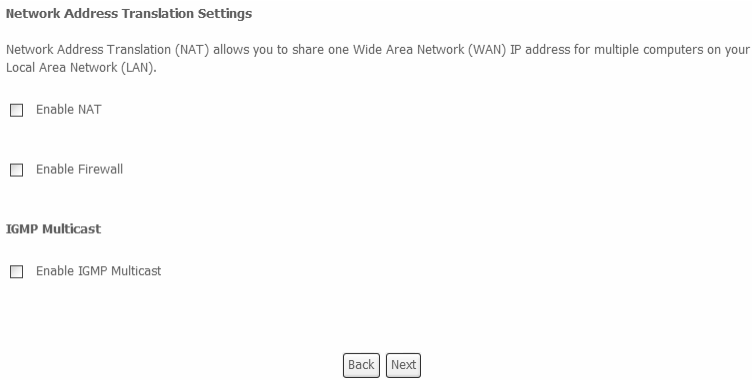


Figure 38 Network address translation settings (IPoA)

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.

Step7 After finishing setting, click **Next** to display the following page.

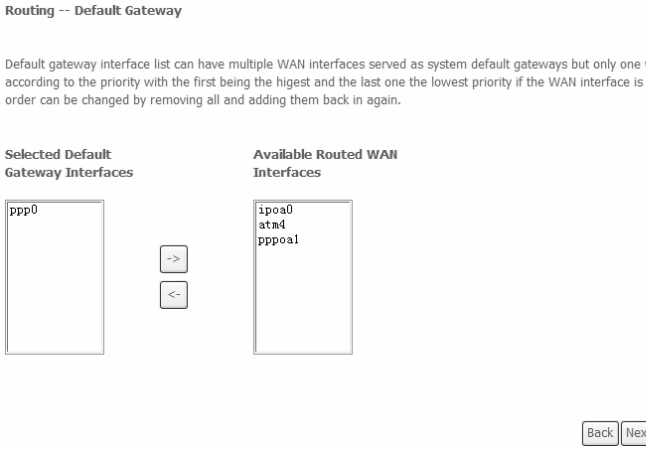


Figure 39 Routing-default gateway (IPoA)

Step8 In this page, select a preferred WAN interface as the system default gateway and then click **Next** to display the following page.

Figure 40 DNS server configuration (IPoA)

Step9 In this page, you should use a static DNS IP address for IPoA mode. Select the proper DNS server interface and enter the primary DNS server and the secondary DNS server. Click **Next** to display the following page.

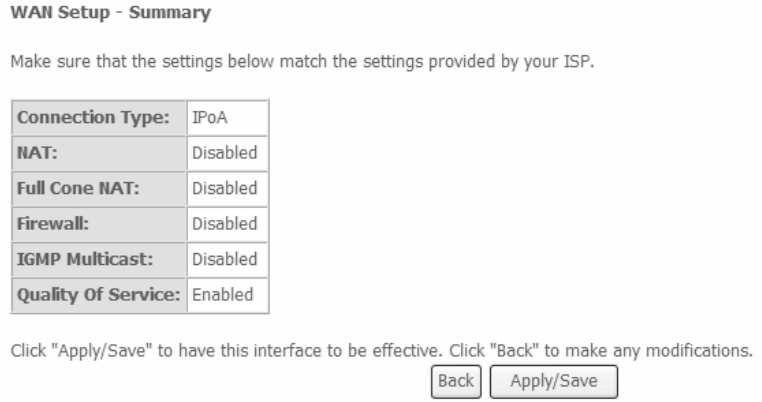


Figure 41 IPoA summary

Step10 In this page, it displays the information about the IPoA settngs. Click **Apply/Save** to save and apply the settings, and then the following page appears. You can modify the settings by clicking the **Back** button if necessary.

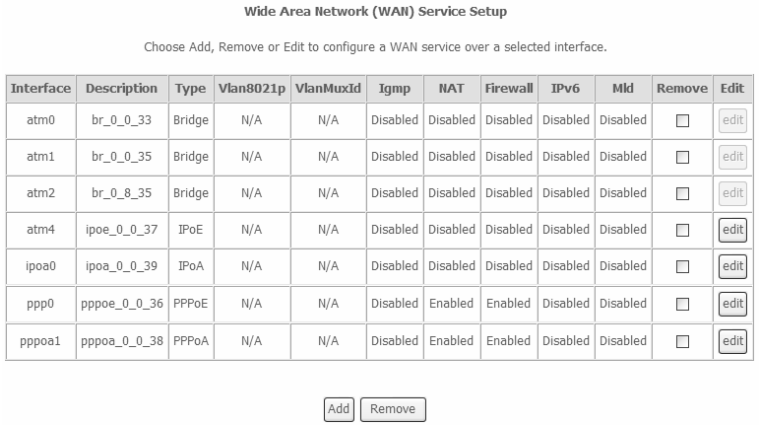


Figure 42 Completing the settings of IPoA WAN service

Adding a Bridge WAN service

This section describes the steps for adding the br_0_0_40(Bridge mode) service.

Step1 In the **Wide Area Network (WAN) Service Setup** page, click the **Add** button to display the following page. (At first, you must add a proper ATM configuration for this WAN service.) Click the **Add** button to display the following page.

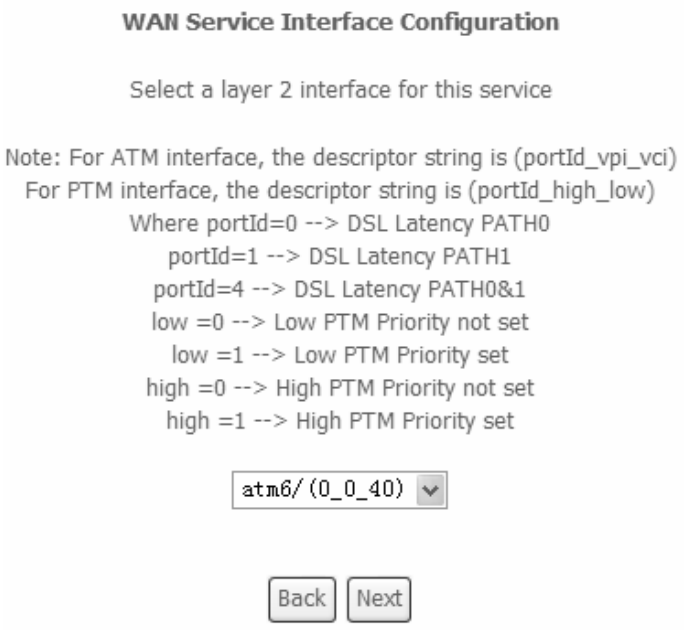


Figure 43 WAN service interface configuration (bridge)

Step2 Select the proper ATM Interface, for example atm6/(0_0_40) and then click **Next** to display the following page.

Figure 44 WAN service configuration (bridge)

Step3 In this page, you can select the WAN service type, and modify the service description. After finishing setting, click **Next** to display the following page.

WAN Setup - Summary

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

Connection Type:	Bridge
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Not Applicable
Quality Of Service:	Enabled

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

Back Apply/Save

Figure 45 Bridge summary

Step4 In this page, it displays the information about the bridge settngs. Click **Apply/Save** to save and apply the settings, and then the following page appears. You can modify the settings by clicking the **Back** button if necessary.

Wide Area Network (WAN) Service Setup

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

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit
atm0	br_0_0_33	Bridge	N/A	N/A	Disabled	Disabled	Disabled	Disabled	Disabled	☐	edit
atm1	br_0_0_35	Bridge	N/A	N/A	Disabled	Disabled	Disabled	Disabled	Disabled	☐	edit
atm2	br_0_8_35	Bridge	N/A	N/A	Disabled	Disabled	Disabled	Disabled	Disabled	☐	edit
atm4	ipoe_0_0_37	IPoE	N/A	N/A	Disabled	Disabled	Disabled	Disabled	Disabled	☐	edit
ipoa0	ipoa_0_0_39	IPoA	N/A	N/A	Disabled	Disabled	Disabled	Disabled	Disabled	☐	edit
atm6	br_0_0_40	Bridge	N/A	N/A	Disabled	Disabled	Disabled	Disabled	Disabled	☐	edit
ppp0	pppoe_0_0_36	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Disabled	Disabled	☐	edit
pppoa1	pppoa_0_0_38	PPPoA	N/A	N/A	Disabled	Enabled	Enabled	Disabled	Disabled	☐	edit

Add Remove

Figure 46 Completing the settings of bridge WAN service

5.2.3 LAN Configuration

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

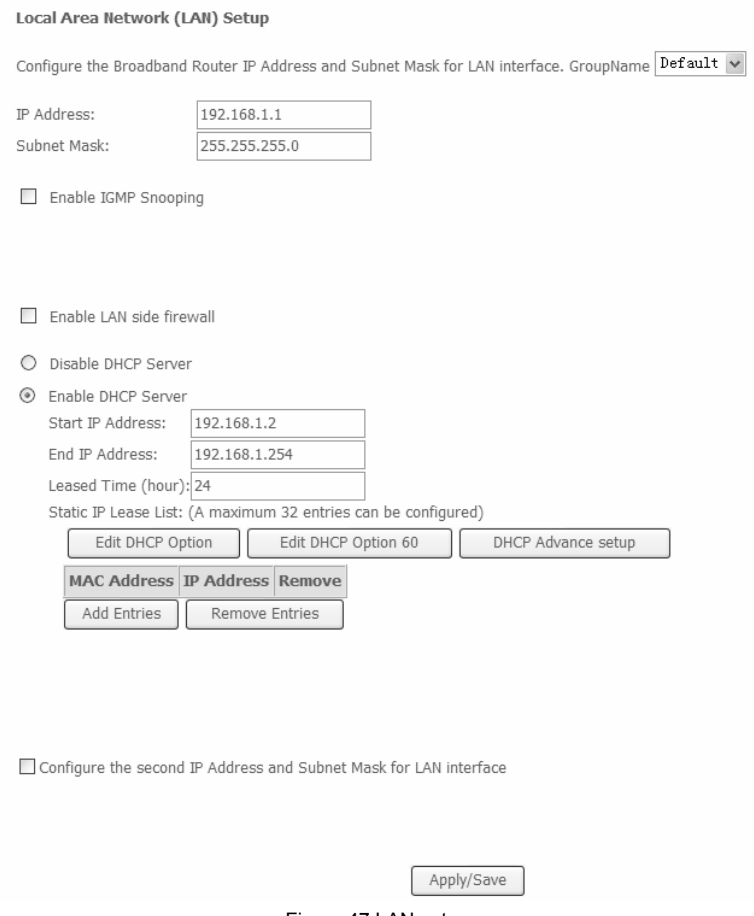


Figure 47 LAN setup

In this page, you can configure an IP address for the DSL router, enable IGMP snooping, enable the LAN side firewall, 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

Figure 48 Configuring the IP address of the DSL router

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

Enabling 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.

Figure 49 Configuring the IGMP snooping

In this page, you can enable the IGMP snooping and select the proper mode for IGMP snooping.

Enabling the LAN Side Firewall

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

Figure 50 Setting the LAN side firewall

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

Configuring the DHCP Server

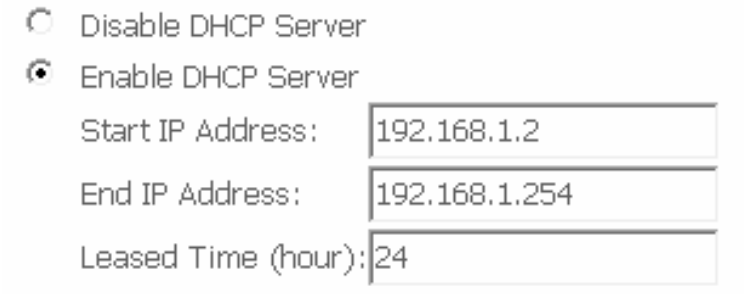


Figure 51 Setting the DHCP server

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.

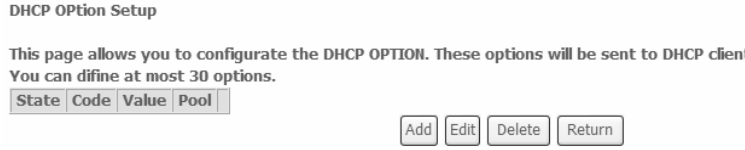


Figure 52 Configuring the DHCP options

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.

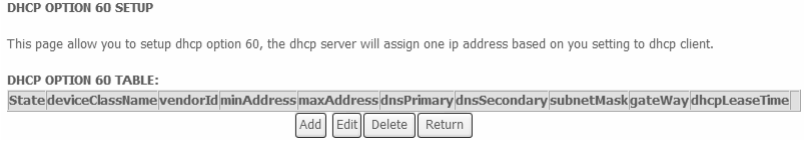


Figure 53 Configuring the DHCP60 options

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

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.

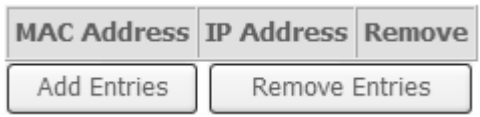


Figure 54 DHCP static lease list

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

Figure 55 Adding an entry of DHCP static IP lease list

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 are allowed to set the second IP address and the subnet mask for a LAN interface.

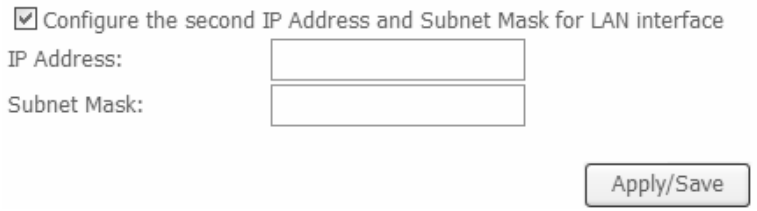
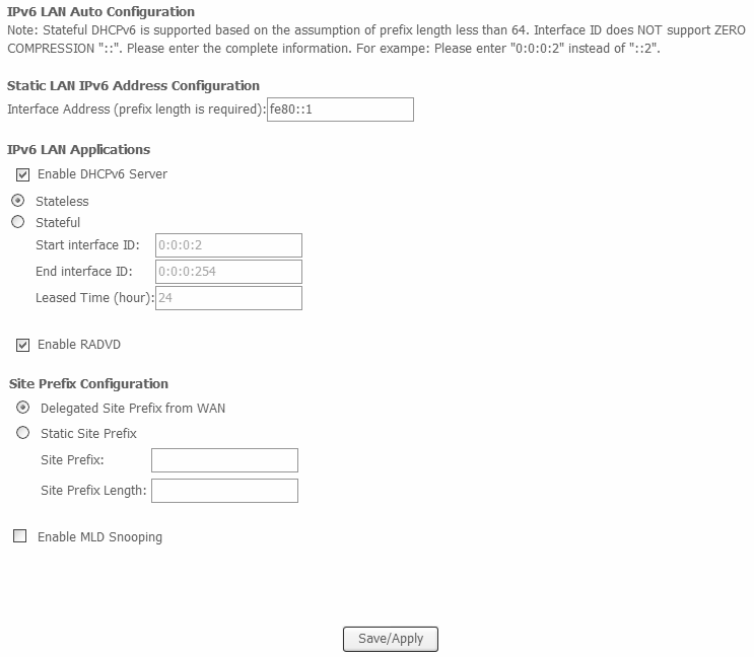


Figure 56 Setting the second IP address and subnet mask

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

5.2.4 IPv6 Auto configuration

Click **Advanced Setup > LAN >IPv6 Autoconfig**, and the following page appears.



In this page, you can set an IP address for the DSL IPv6 router, enable the DHCPv6 server, enable RADVD and enable the MLD snooping function.

- **Enable DHCPv6 Server:** WIDE-DHCPv6 is an open-source implementation of dynamic host configuration protocol for IPv6 (DHCPv6) originally developed by the KAME project. The implementation mainly complies with the following standards: RFC3315, RFC3319, RFC3633, RFC3646, RFC4075, RFC 4272 etc.
- **Enable RADVD:** The router advertisement daemon (RADVD) is run by Linux or BSD systems acting as IPv6 routers. It sends router advertisement messages, specified by RFC2461, to a local Ethernet LAN periodically and when requested by a node sending a router solicitation message. These messages are required for IPv6 stateless auto-configuration.

- **Enable MLD Snooping**: Multicast Listener Discovery Snooping (MLD Snooping) is an IPv6 multicast constraining mechanism that runs on Layer 2 devices to manage and control IPv6 multicast groups. By analyzing received MLD messages, a Layer 2 device running MLD Snooping establishes mappings between ports and multicast MAC addresses and forwards IPv6 multicast data based on these mappings.

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

5.2.5 NAT

Note:
The NAT information is not displayed in the bridge mode.

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.

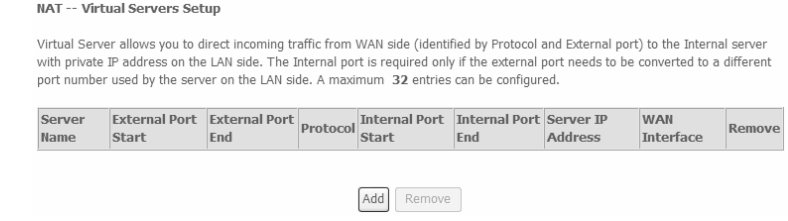


Figure 57 Virtual server setup

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

To add a virtual server, do as follows:

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

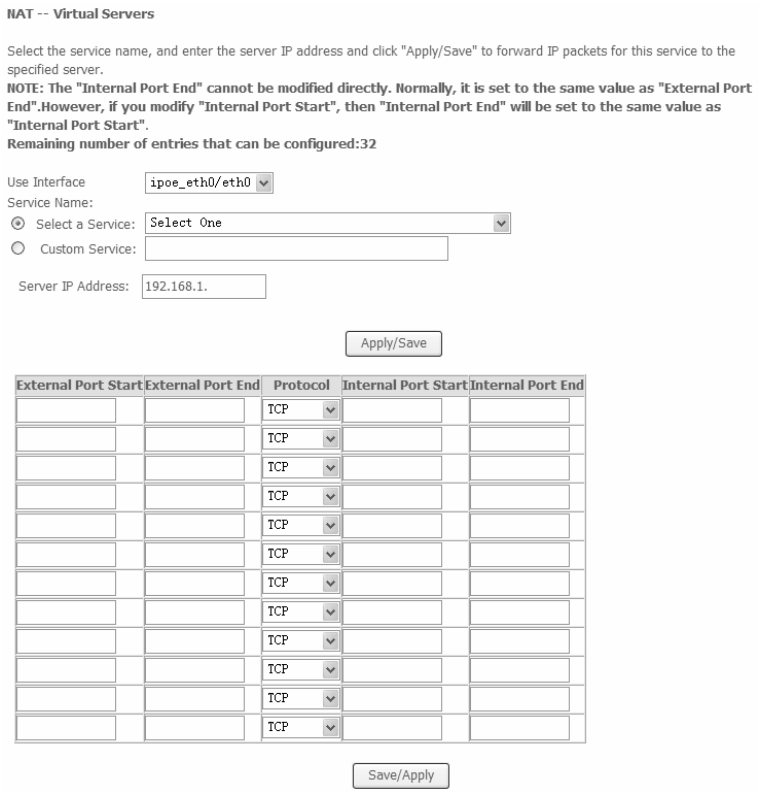


Figure 58 Adding an entry of virtual server

- **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**: 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.

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

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.

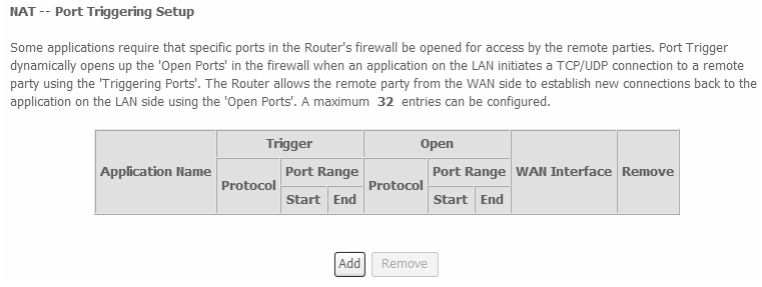


Figure 59 Port triggering setup

In this page, you may add or delete an entry of port triggering.

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

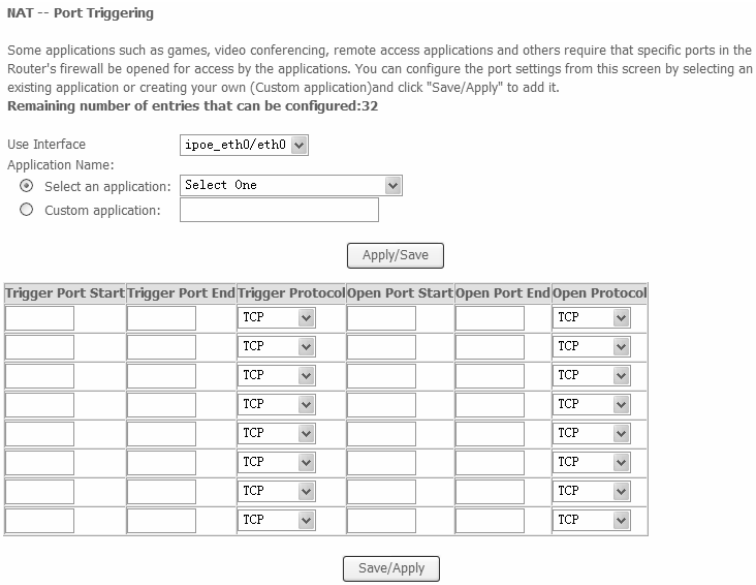


Figure 60 Adding an entry of port triggering

- **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 finishing 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.

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.

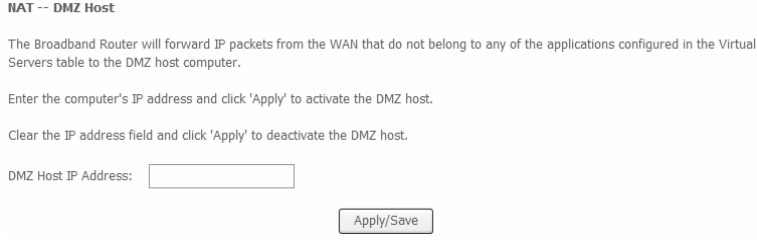


Figure 61 DMZ host

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

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

If you want to clear the DMZ function of the host, please delete the IP address of the host in the field of **DMZ Host IP Address**, and then click the **Apply/Save** button.

Multi NAT

Multi-NAT is the term to describe creating more than one public IP address for your network. Multi-NAT is used in the situation when your ISP provides you with a number of public IP addresses, and you want to use them to provide access from Internet to multiple internal servers. Multi NAT assigns one of the public IPs to the WAN interface of the router; then Multi-NAT is used for the other public IPs, and with them NATed to multiple internal IP addresses.

Click **Advanced Setup** > **NAT** > **Multi NAT**, and the following page appears.

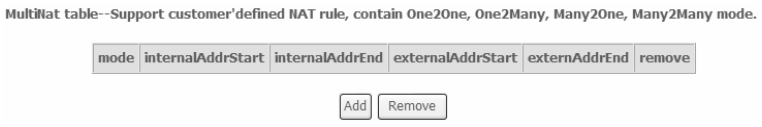


Figure 62 Multi-NAT setup

In this page, you can add or remove a multi-NAT rule.
Click the **Add** button to display the following page.

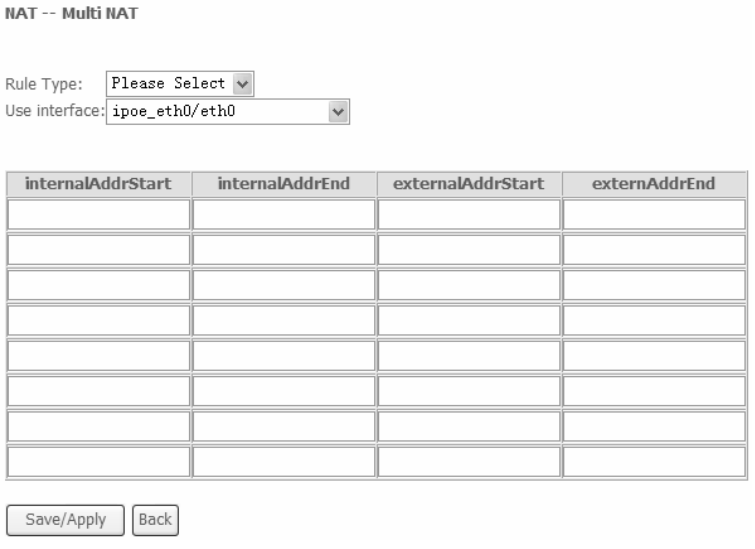


Figure 63 Adding a multi-NAT rule

In this page, please select the proper type; select the proper **Use interface**, and configure the other parameters in this page.
After finishing setting, click **Save/Apply** to apply the settings.

5.3 Wireless

5.3.1 Basic Settings

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

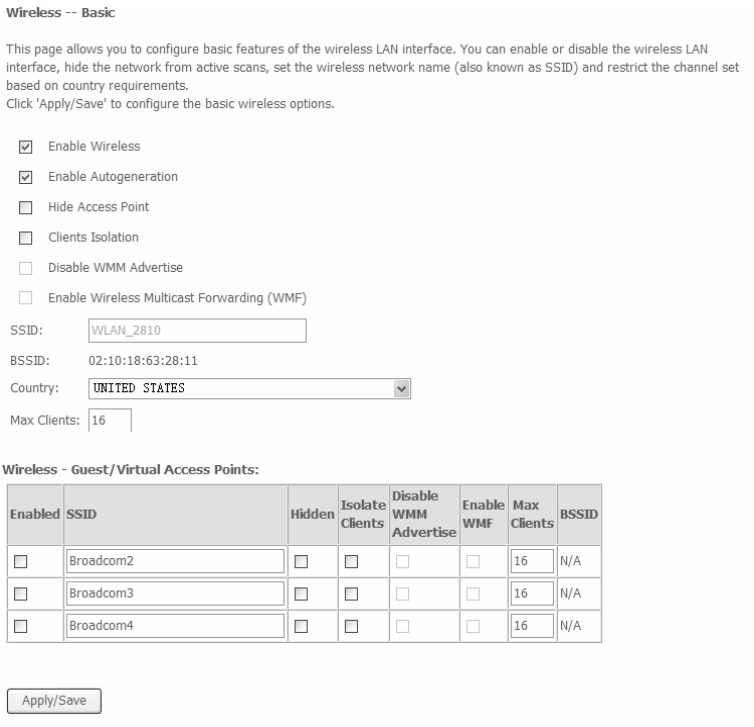


Figure 64 Wireless basic configuration

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

5.3.2 Security

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

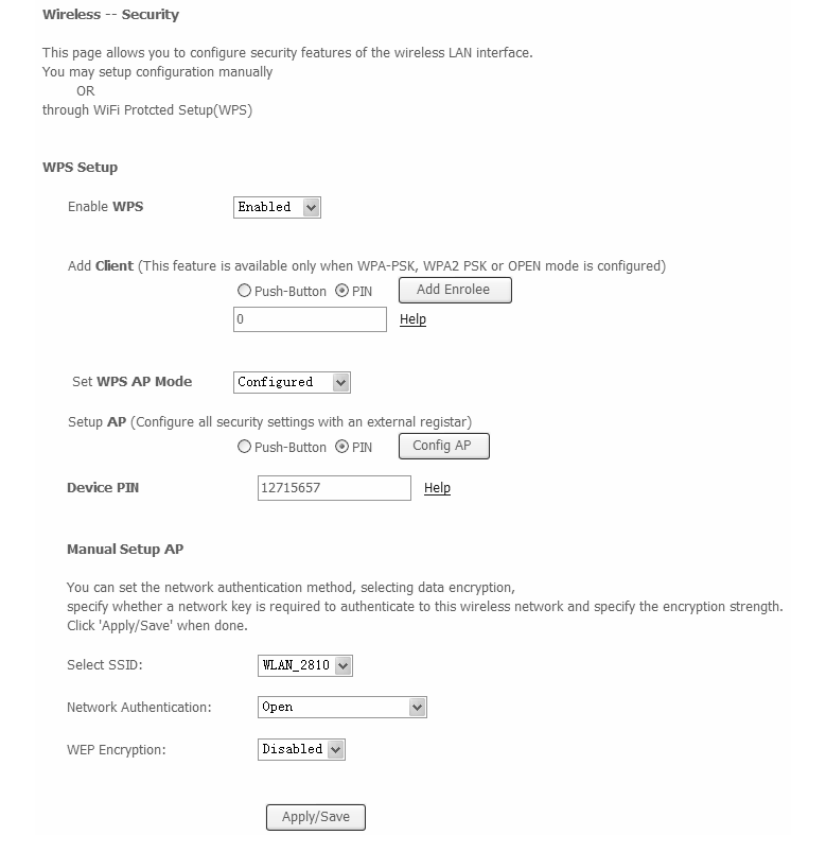


Figure 65 Wireless security configuration

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**

Figure 66 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**

This page provides 9 types of network authentication modes, including Open, Shared, 802.1X, WPA, WPA-PSK, WPA2, WPA2-PSK, Mixed WPA2/WPA, and Mixed WPA2/WPA-PSK.

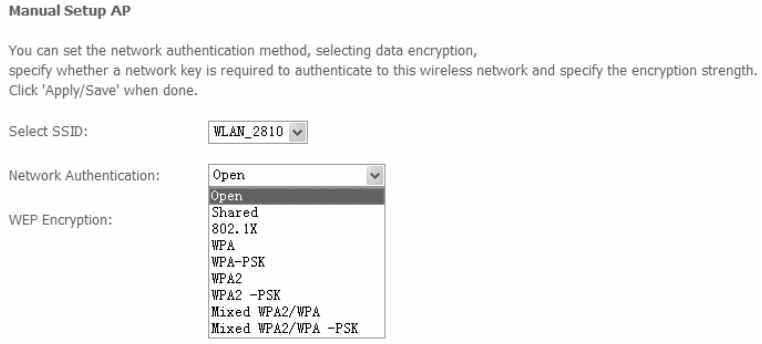


Figure 67 Manual setup AP

5.3.3 MAC Filter

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

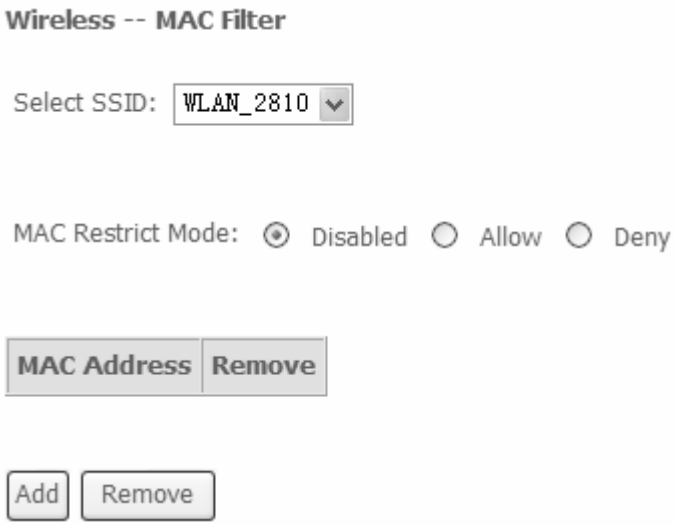


Figure 68 MAC filter configuration

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.

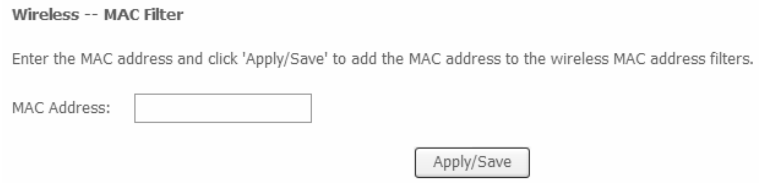


Figure 69 Adding a MAC filter

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.

5.3.4 Wireless Bridge

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

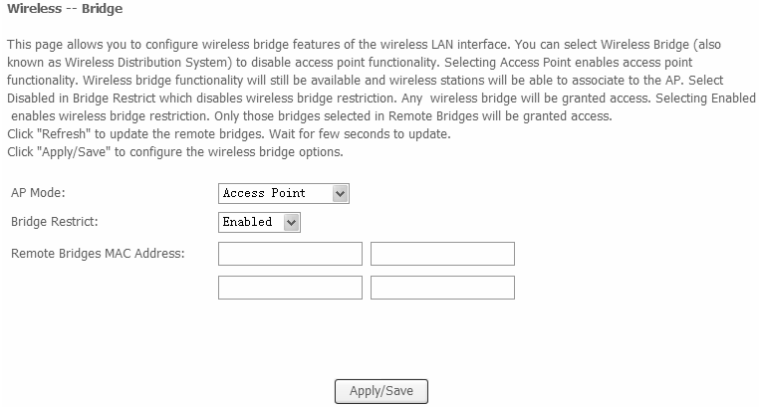


Figure 70 Wireless bridge configuration

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

5.3.5 Advanced Settings

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

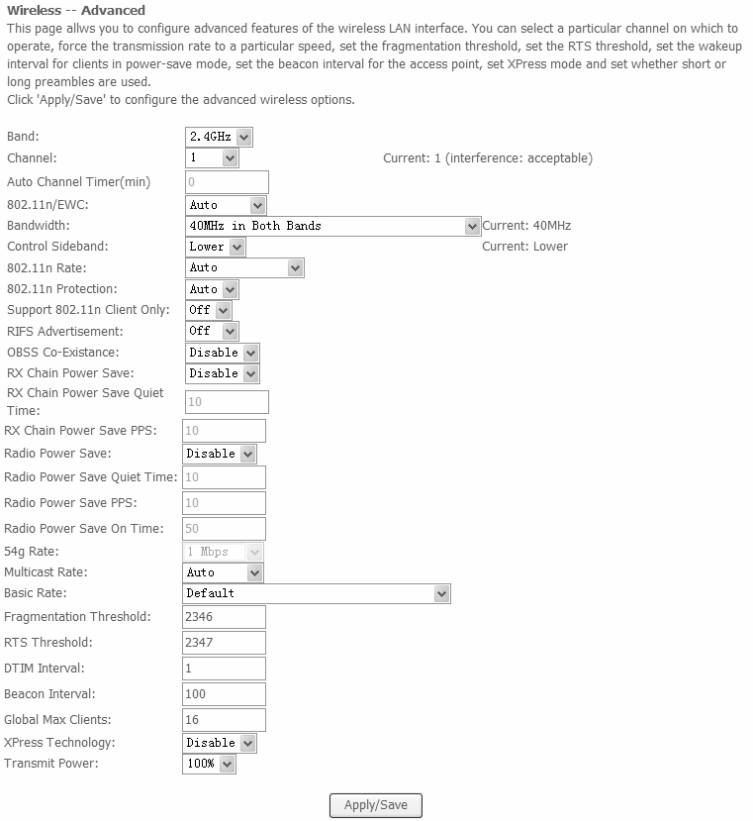


Figure 71 Wireless advanced settings

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.

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 Diagnostics

Choose **Diagnostics**, and the following page appears.

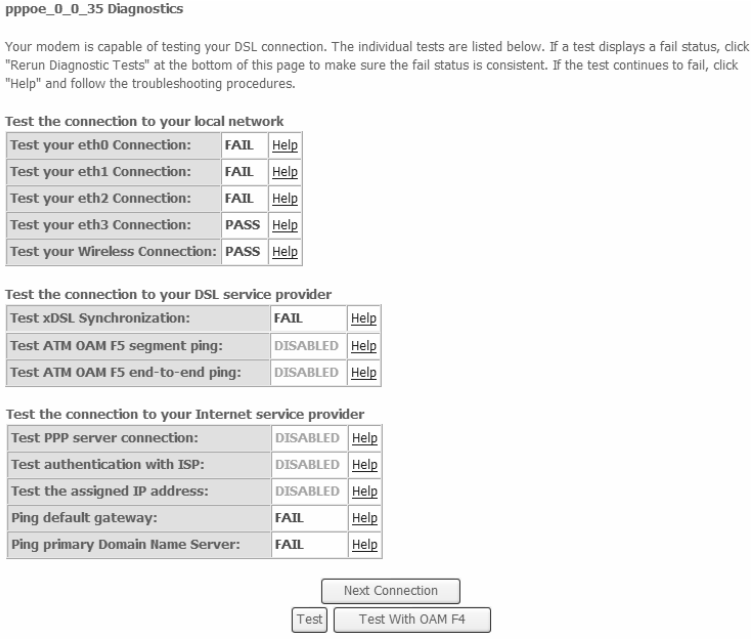


Figure 72 Diagnostics configuration

This page is used to test the connection to your local network, the connection to your DSL service provider, and the connection to your Internet service provider.
You may diagnose the connection by clicking **Test** or **Test with OAMF4**.

5.5 Management

5.5.1 Settings

Backup

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

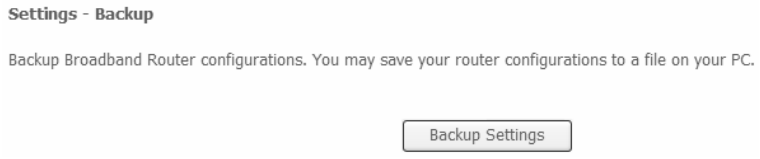


Figure 73 Backup settings

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.

Figure 74 Update settings

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.

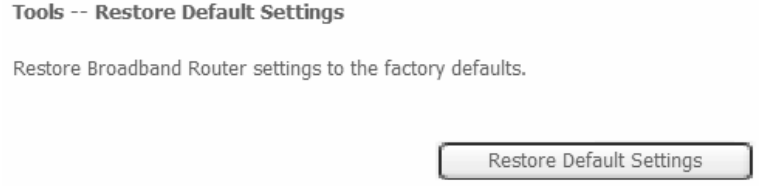


Figure 75 Restoring the default settings

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

5.5.2 TR-69 Client

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

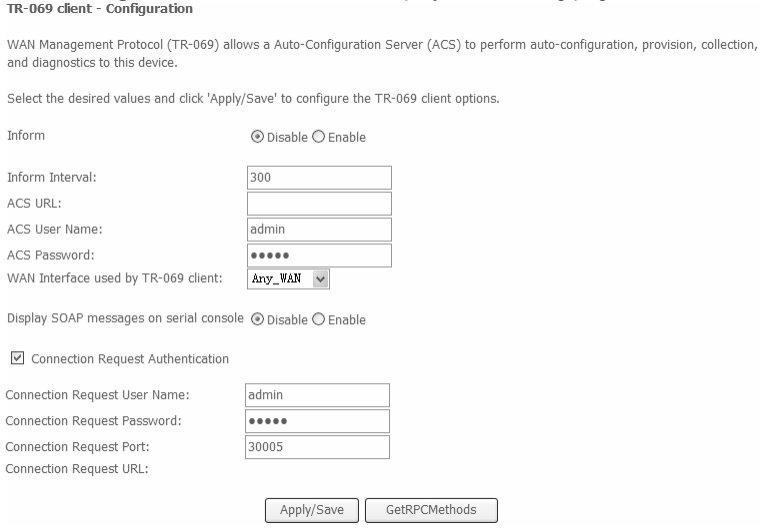


Figure 76 TR-069 client configuration

WAN Management Protocol (TR-069) allows 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 finishing setting, click the **Apply/Save** button to save and apply the settings.

5.5.3 Access Control

Passwords

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

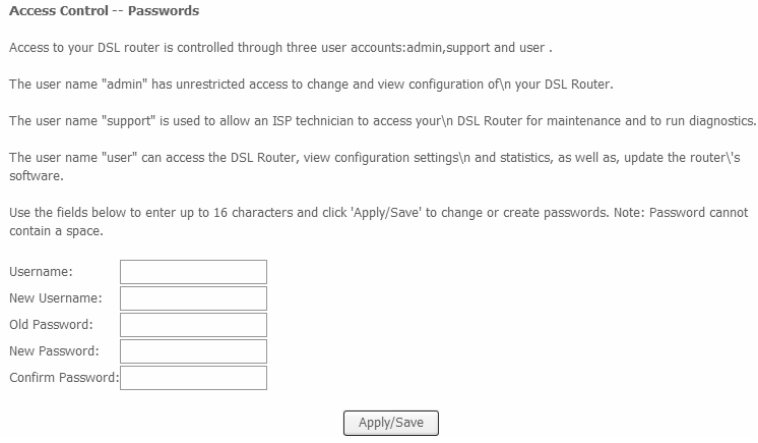


Figure 77 Modifying the password

In the page, you can modify the passwords of different users.
After finishing setting, click the **Apply/Save** button to save and apply the settings.

Services

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

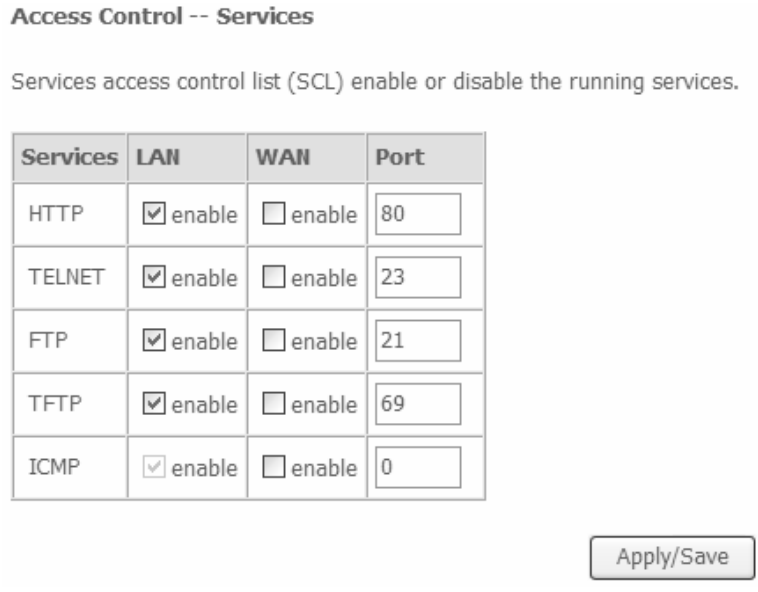


Figure 78 Services control

In this page, you can enable or disable the different types of services.
After finishing setting, click the **Apply/Save** button to save and apply the settings.

Note:
The WAN information is not displayed in the bridge mode.

5.5.4 Update Software

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

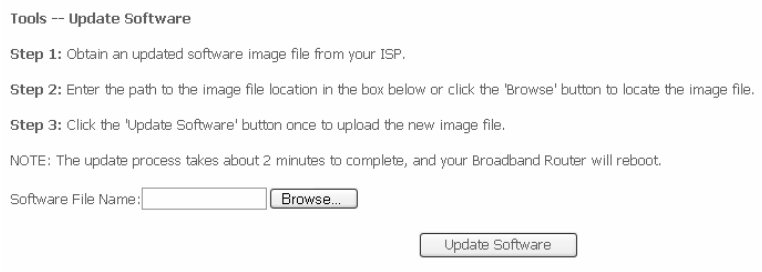


Figure 79 Updating software

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.

5.5.5 Reboot

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

Figure 80 Rebooting the router

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

6 Q&A

(1) **Q**: Why all the indicators are off?

A: Check the following:

- The connection between the power adaptor and the power socket.
- The status of the power switch.

(2) **Q**: Why the **LAN** indicator is off?

A: Check the following:

- The connection between the ADSL router and your computer, hub, or switch.
- The running status of your PC, hub, or switch.

(3) **Q**: Why the **ADSL** indicator is off?

A: Check the connection between the "Line" port of router and the wall jack.

(4) **Q**: Why Internet access fails while the **ADSL** indicator is on?

A: Check whether the VPI, VCI, user name, and password are correctly entered.

(5) **Q**: Why I fail to access the web configuration page of the DSL router?

A: Choose **Start** > **Run** from the desktop, and ping ***192.168.1.1*** (IP address of the DSL router). If the DSL router is not reachable, check the type of the network cable, the connection between the DSL router, and the PC, and the TCP/IP configuration of the PC.

(6) **Q**: How to load the default settings after incorrect configuration?

A: To restore the factory default settings, turn on the device, and press the reset button for about 1 second, and then release it. The default IP address and the subnet mask of the DSL router are **192.168.1.1** and **255.255.255.0**, respectively.

- User/password of super user: **admin**/**admin**
- User/password of common user: **user**/**user**